Context-Based Micro-Training
Enhancing cybersecurity training for end-users
DOCTORAL THESIS

CONTEXT-BASED MICRO-TRAINING

Enhancing cybersecurity training for end-users

Joakim Kävrestad
Informatics
ABSTRACT

This research addresses the human aspect of cybersecurity by developing a method for cybersecurity training of end-users. The reason for addressing that area is that human behaviour is widely regarded as one of the most used attack vectors. Exploiting human behaviour through various social engineering techniques, password guessing, and more is a common practice for attackers. Reports even suggest that human behaviour is exploited in 95% of all cybersecurity attacks.

Human behaviour with regard to cybersecurity has been long discussed in the research. It is commonly suggested that users need support to behave securely. Training is often suggested as the way to improve user behaviour, and there are several different training methods available. The available training methods include instructor-led training, game-based training, eLearning, etc. However, even with the diversity of existing training methods, the effectiveness of such training has been questioned by recent research. Research suggests that existing training does not facilitate knowledge retention and user participation to a high enough degree.

This research aims to address the problems with current training practices by developing a new method for cybersecurity training of end-users. The research used a design science (DS) approach to develop the new method in three increasingly complex design cycles. Principles for cybersecurity training were developed based on previous research and the Technology Acceptance Model and made the theoretical foundation of the research. The result is a theoretically grounded method for cybersecurity training that outlines goals and guidelines for how such training should be implemented. It has been evaluated in several steps with more than 1800 survey participants and 300 participants in various experiments. The evaluations have shown that it can both support users towards secure behaviour and be appreciated by its users.

The main contribution of this research is the method for cybersecurity training, Context-Based Micro-Training (CBMT). CBMT is a theoretical contribution that describes good practices for cybersecurity training for end-users. Practitioners
can adopt it as a guide on how to implement such training or to support procurement decisions. The research also shows the importance of integrating usability into the development of security practices. Users must positively receive both training and the guidelines imposed by training since positive user perception increases user adoption. Finally, the research shows that following security guidelines is difficult. While training is essential, this research suggests that training alone is not enough, and future research should consider the interplay between training and other support mechanisms.
SAMMANFATTNING

Denna forskning adresserar mänskliga aspekter på cybersäkerhet genom att utveckla en metod för cybersäkerhetsträning av användare. Forskningen motiveras med att användarbeteende anses vara en av de attackvektorer som angripare oftast använder. Att använda social manipulation, gissa lösenord och liknande för att utnyttja mänskligt beteende är vanligt. Vissa rapporter hävdar till och med att mänskligt beteende utnyttjas i 95% av alla cyberattacker.


Det huvudsakliga bidraget från denna forskning är metoden för säkerhetsträning, KontextBaserad MikroTräning (CBMT). CBMT är ett teoretiskt bidrag som beskriver mål och riktlinjer för säkerhetsträning av användare. Yrkesverksamma kan använda metoden som en guide för implementation av säkerhetsträning eller som ett stöd vid upphandling av
ACKNOWLEDGEMENTS

Now it is time for the space where I get to briefly reflect on how others helped ensure that this thesis came to be and try to send thanks and credit to those who have supported this work in various ways. But I first need to reflect on the curious way that has led to this moment, the end of the PhD period and the (hopefully successful) start of the journey onwards in academia. I am certainly not following my intended route, which by the way, was to study in Skövde for three years and then earn money in the industry. That was in 2009 and obviously did work out as planned. For that reason, I will not make any more plans but see where opportunities take me in the hope that I can continue working with committed, friendly, fun and brilliant people (you decide what applies to you).

That brings me to the main reasons why “this” happened and my primary source of support on my academic journey. That would be my supervisors, especially Marcus Nohlberg, who has been an inspiration, teacher, supervisor, and great colleague over the past 10+ years. It can truly be said that I would not have considered the opportunity of approaching a research career had I not met you. And I do hope that our work in the outskirts of cybersecurity (the human aspects) will continue with increased force! Similarly, Steven Furnell, who I picked up in Lesbos in 2015, and who showed me that even professors with a high H-index could be friendly, introduced me to wonderful beverages and had me understand British humour. He has also been extremely valuable in the research with insightful comments and an outside perspective. And also, Rose-Mharie Åhfeldt, my third supervisor, for keeping me straight when I sometimes prefer (a bit too much) to take the off-track route.

Research is best made in cooperation, and a special thanks is due to the several persons who have co-authored papers with me during this research. Being able to work with competent and committed colleagues is true bliss. On that note, thanks should also go out to Joeri Van Laere, Ella Kolkowska, and Andreas Jacobsson for insightful comments on earlier stages of the thesis provided as discussion leaders on the research proposal, thesis proposal, and final seminars. And similarly to Jörgen Hansson for the same types of discussions throughout courses during the PhD journey. Many others have been immensely valuable in
the same way. There is unfortunately not room enough to thank everyone, but I will surely take the next round when our routes cross again and thank you in person.

I would argue that the people who help you not work on your PhD are equally as important as those who do. For that reason, I first want to thank my awesome colleagues, especially the “NSA-teachers” Johan, Dennis, Marcus, Thomas and Ali for ensuring timely fika and providing an excellent social climate at work! Of course, my main colleague during the pandemic has been my “better half”, Joanna, who should have a special thanks for being awesome and wonderful in general – you do better work when you are in a good place, and you provide that place at home! But she also had to bear with me while talking about stuff that may not be of interest to her, and while I have been busy or completely away for work more or less frequently, I am thankful. I also want to thank someone who spent lots of time just hanging out with me while writing – and ensuring much-needed walks in-between writing, my dog Milton. A final big thanks to the rest of my family for being available and there for me whenever needed.

Joakim Kävrestad
Stenstorp, 2022
This thesis is a compilation of the following eleven papers published in peer-reviewed academic conferences and journals. The papers are appended to this thesis in full. Note that paper 10 is submitted for publication and currently undergoing review.


CONTENTS

1 INTRODUCTION ................................................................................................................................. 1
  1.1 Problem area .................................................................................................................................. 2
  1.2 Research aim ................................................................................................................................. 6
  1.3 Delimitations ................................................................................................................................. 9
  1.4 Thesis outline ............................................................................................................................... 10

2 BACKGROUND .................................................................................................................................. 15
  2.1 Cybersecurity in brief ..................................................................................................................... 16
  2.2 Human aspects of cybersecurity ..................................................................................................... 18
  2.3 User training and Awareness in the cybersecurity domain ......................................................... 20

3 RESEARCH METHODOLOGY .......................................................................................................... 27
  3.1 Research approach ......................................................................................................................... 29
  3.2 Implementation of design science ................................................................................................ 31
  3.3 Supporting methods ....................................................................................................................... 34
    3.3.1 Structured literature reviews .................................................................................................. 34
    3.3.2 Surveys .................................................................................................................................... 35
    3.3.3 Experiments ............................................................................................................................ 35
    3.3.4 Field notes .............................................................................................................................. 36
  3.4 Sampling and limitations ................................................................................................................ 36
  3.5 Ethical considerations .................................................................................................................... 38
    3.5.1 Respect for individuals .......................................................................................................... 39
    3.5.2 Beneficence ........................................................................................................................... 40
    3.5.3 Equality .................................................................................................................................. 40
    3.5.4 Respect for law and public interest ......................................................................................... 41

4 IMPLEMENTATION AND RESULTS ............................................................................................... 45
4.1 Theoretical framework

4.1.1 Previous research on cybersecurity training

4.1.2 Technology Acceptance Model

4.1.3 Derived principles for cybersecurity training

4.2 Establishment of requirements for evaluation

4.2.1 Requirements for cybersecurity training

4.2.2 Evaluation procedures in the domain

4.2.3 Establishment of a process for evaluation

4.3 DS cycle 1: Exploring the problem space

4.3.1 Method development

4.3.2 Artefact demonstration

4.3.3 Evaluation

4.3.4 Revisiting the principles of cybersecurity training

4.4 DS cycle 2: Proposing a solution

4.4.1 Method development

4.4.2 Artefact demonstration

4.4.3 Evaluation

4.4.4 Revisiting the principles of cybersecurity training

4.5 DS cycle 3: Context-Based Micro-Training

4.5.1 Method development

4.5.2 Artefact demonstration

4.5.3 Evaluation

4.5.4 Revisiting the principles of cybersecurity training

4.6 Context-Based Micro-Training - a summary

5 DISCUSSION

5.1 Main results

5.1.1 Context-Based Micro-Training

5.1.2 Principles underpinning CBMT

5.1.3 Requirements for cybersecurity training

5.1.4 Demographical aspects of this work

5.2 Scientific rigour

5.2.1 Problem relevance

5.2.2 Research Rigour

5.2.3 Design as a search process

5.2.4 Design as an artifact
5.2.5 Design evaluation................................................................. 95
5.2.6 Research contributions.................................................... 96
5.3 Research validity................................................................. 96
5.4 Reflection on included papers ............................................. 97
6 CONCLUSION ......................................................................... 105
  6.1 Revisiting aim and objectives ............................................. 106
  6.2 Contributions to research .................................................. 107
  6.3 Contributions to practice ................................................... 108
  6.4 Limitations and future work ............................................... 109
REFERENCES ............................................................................ 113
PUBLICATIONS IN THE DISSERTATION SERIES ......................... 129
INCLUDED PUBLICATIONS .......................................................... 133
  Paper 1: Online Fraud Defence by Context Based Micro Training .... 135
  Paper 2: Users perception of using CBMT for informationsecurity training. 147
  Paper 3: Using context based micro training to develop OER for the benefit of all ................................................................. 159
  Paper 4: Assisting Users to Create Stronger Passwords Using ContextBased MicroTraining ............................................................. 171
  Paper 5: Can Johnny actually like security training? .................... 187
  Paper 6: Contextbased microtraining: a framework for information security training ........................................................................ 197
  Paper 7: Constructing secure and memorable passwords .............. 211
  Paper 8: Evaluation Strategies for Cybersecurity Training Methods: A Literature Review ......................................................... 231
  Paper 9: Evaluation of Contextual and game-based training for phishing detection ........................................................................ 245
  Paper 10: A taxonomy of SETA methods and linkage to delivery preferences. ................................................................. 263
LIST OF FIGURES

Figure 1 Results, in publications per year, of sample search in Scopus for various cybersecurity-related keywords (search performed 20220325)........... 3
Figure 2 Percentage of papers from search in Figure 1, which concerns the human vector and education (search performed 20220325). ...................... 4
Figure 3 Overview of included publications and related objectives .............. 8
Figure 4 Thesis outline.............................................................................. 11
Figure 5 Outline of the background chapter ........................................... 15
Figure 6 Outline of the chapter research methodology............................ 27
Figure 7 Visualization of research strategy ............................................. 32
Figure 8 Outline of the chapter implementation and results...................... 45
Figure 9 Overview of the research plan. Black boxes show artefact development tasks, grey show demonstrations and white show evaluations ................. 46
Figure 10 Visualisation of the evolvement and role of principles for cybersecurity training ................................................................. 47
Figure 11 Visualization of the position of the establishment of the evaluation requirements in relation to the rest of the research............................. 53
Figure 12 Example visualisation of the evaluation process............................. 55
Figure 13 Visualization of the positioning of DC1 in relation to the rest of the research.................................................................................. 56
Figure 14 Service-side implementation of CBMT ..................................... 59
Figure 15 User-side implementation of CBMT ......................................... 59
Figure 16 Overview of evaluation activities in DC1................................... 61
Figure 17 Visualization of the positioning of DC2 in relation to the rest of the research................................................................................ 62
Figure 18 Implementation of CBMT in DC2 ............................................. 66
Figure 19 Overview of evaluation activities up until DC2.......................... 69
Figure 20 Visualization of the positioning of DC3 in relation to the rest of the research.................................................................................. 71
Figure 21 Model describing the CBMT method ....................................... 74
Figure 22 Model describing the CBMT method in a constructed situation .... 74
Figure 23 WebSec Assistant in the phishing context .................................. 76
Figure 24 WebSec Assistant phishing training ........................................ 76
Figure 25 WebSec Coach phishing warning ............................................. 77
Figure 26 WebSec Coach phishing warning with the option to proceed ........ 77
Figure 27 Overview of evaluation activities up until DC3. .............................................81
Figure 28 Model describing the CBMT method. ...............................................................84
Figure 29 Model describing the CBMT method in a constructed situation. .... 84
Figure 30 Outline of the discussion chapter. .................................................................89
Figure 31 Outline of the conclusion chapter. .................................................................105
LIST OF TABLES

Table 1 External TAM factors relating to the organization a technology is implemented in.................................................................48
Table 2 Social TAM factors relating to the intended user of a technology. ...... 49
Table 3 Technological TAM factors relating to the technology itself................... 50
INTRODUCTION
CHAPTER 1
1 INTRODUCTION

Digitalisation is progressing rapidly, and virtually all aspects of most people's lives have been or will arguably be transformed in a digital sense (OECD, 2019). While the positive effects of digitalisation are undeniable, new challenges emerge, one of which is the rising need for cybersecurity. When people learn to rely on digital services, they increase the risk of digital threats in their personal and professional life and our need for cybersecurity increases. As demonstrated by Sfakianakis et al. (2019), the threat landscape ranges from phishing and spam consistently faced by users to insider threats and cyber-espionage carried out by highly motivated and skilled adversaries targeting large organisations.

The number of cybersecurity incidents continues to grow (Sen, 2018). Sen (2018) reports that 500 million personal data records were stolen in 2018. In 2019, a server belonging to the company ElasticSearch was compromised, leading to the disclosure of 108 million records (Henriques, 2019). 2019 was also the year of the 1177 incident in Sweden. 1177 is a national service for phone-based healthcare advice. The incident involved the disclosure of 2.7 million recorded conversations between caregivers and patients (Andreasson & Blix, 2019). The source of this incident was a misconfigured storage server. Yet another incident in 2019 was when a hacker managed to access information from 100 million customers of the bank Capital One (McLean, 2019). The consequences of those incidents were that the privacy of several hundred million individuals was compromised. Unfortunately, other examples are in plentiful supply.

On the corporate side, security issues can lead to various problems that impact the ability to function normally, including data loss, data breaches, or service unavailability (Pfleeger et al., 2015). Security is undeniably an essential aspect of digitalization that cannot go unheeded. While many traditional cybersecurity efforts have focused on the technical domain, cybersecurity is a social-technical property where insecure user behaviour is crucial (Bulgurcu et al., 2010; Safa & Von Solms, 2016). Threat actors recognize this notion and often exploit user
behaviour, making the need for measures towards secure behaviour emergent (Joinson & van Steen, 2018).

A major attack in recent years was the Petya ransomware. Petya is a ransomware that encrypts data on infected hosts and demands a ransom in order for the victim to receive a decryption key (Aidan et al., 2017). Petya was observed in at least 64 countries and spread using phishing e-mail. It makes one example of a worldwide attack exploiting user behaviour. Other cybersecurity incidents stemming from insecure user behaviour include the compromise of Donald Trumps Twitter account and the compromise of three eBay employees’ credentials, leading to the subsequent compromise of data from 145 million eBay users in 2014 (Kelly, 2014; Tidy, 2020).

The common suggestion for improving user behaviour is through education (Puhakainen & Siponen, 2010). It is hard to overlook the notion that users need to understand the consequences of insecure behaviour and be taught to behave securely (Desman, 2003). Further, there are many distinct suggestions on how to carry out security training from the practitioner and the research community. Different training measures range from lectures to micro training or special-purpose tools such as password strength meters. While there are research examples of individual studies where researchers provide good evidence that specific methods work, several reports suggest that many training programs used in practice are not grounded in empirical evidence of their validity (Al-Daeef et al., 2017; Alshaikh et al., 2018). As such, the need for further research into this area is apparent.

The area of this research is user behaviour related to cybersecurity and, more specifically, how user behaviour can be improved using training. The research meets the need for further research into cybersecurity training by developing a method for cybersecurity training of end-users using a design science research approach. The rest of this section will elaborate on the problem area before the research aim is explicated. The problem area will then be further framed by a presentation of research contributions and delimitations.

1.1 PROBLEM AREA

Cybersecurity is defined in ISO/IEC 27100:2020 (International Organization for Standardization, 2020) as:

safeguarding of people, society, organizations and nations from cyber risks

International Organization for Standardization (2012), in ISO/IEC 27032:2012, further describe cyberspace as:

complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.
As such, cybersecurity includes technical and social actions to minimize risks faced by organizations and individuals, and it is easy to argue that both social and technical measures are necessary to establish a good security level. A part of the social domain is the human attack vector, described as using humans as the entry-point for an attack. This is a well-known practice, and threat actors frequently exploit human behaviour to perform attacks against individuals and organizations (Joinson & van Steen, 2018). Reports from industry and scholars even suggest that the human attack vector is the most regularly used, some suggesting that up to 95% of attacks include human elements (Cybint, 2020; EC-council, 2019; Soare, 2020).

Looking at the number of published academic papers in cybersecurity and closely related domains indexed by Scopus between 2000 and 2020, it is evident that research in those domains is heavily geared towards other areas. This is demonstrated in Figure 1 and Figure 2, where statistics from sample searches are displayed. As described by von Solms and von Solms (2018), cybersecurity and terms for closely related concepts such as computer security and information security are often used interchangeably, and all terms are therefore included in the sample searches.

![Figure 1 Results](attachment:image.png)
While the human aspect of cybersecurity is a critical factor in cybersecurity, Figure 1 and Figure 2 suggest that the domain is not getting as much attention from researchers as it needs. Nevertheless, it is a well-established theme in scientific literature where, for instance, Whitten and Tygar (1999) discussed the usability of security tools already in 1999. More recent literature reveals that human behaviour in relation to cybersecurity is a complex matter affected by many aspects. These include individual factors such as demographics, stress level, and personal traits (Anwar et al., 2017; Chowdhury et al., 2019; Donalds & Osei-Bryson, 2020; Hadlington, 2017; Harrison et al., 2016). Behaviour is also likely to differ based on the individual's situation, such as whether s/he is at home or work (Mashiane & Kritzinger, 2018). While unarguably complex, human behaviour is an area of concern in cybersecurity, and the typical suggestion for how to address this area is by the use of training interventions (Anwar et al., 2017; Bada et al., 2019; Evans et al., 2016; Safa et al., 2015).

Even cybersecurity training has been discussed in the scientific literature for at least 20 years (Siponen, 2000). Training implies providing knowledge; Siponen (2000) describes that users need to be trained on how to act and why and how. That is well in line with how the Protection Motivation Theory (PMT), introduced by Rogers (1975), describes factors that decide how people respond to threats.
Applied to the context of security behaviour, PMT suggests that a user's likeliness to engage in secure behaviour is first affected by how severe and likely the user perceives a particular risk. It is then also affected by the cost, effectiveness, and perceived ability to mitigate that risk (Tsai et al., 2016). The role of security training would be to educate the user on what secure behaviour is, why it is needed and how to engage in it with minimal cost. A central notion is that while knowledge about how to act is influential, it is not enough to make users engage in secure behaviour. This notion is supported by recent research where raising user awareness is suggested as necessary in addition to providing knowledge (Boss et al., 2015; Parsons, 2018; Siponen et al., 2014). Hu et al. (2021) argue that the target audience of cybersecurity training makes an important aspect that should be considered in research. Hu et al. (2021) highlight that such training should be conducted differently depending on if it is targeting Information Technology (IT) specialists or other employees (end-users). This research concerns cybersecurity training for end-users. The term End-users is defined by Cambridge Dictionary (2022a) as "the person or organization that uses something rather than an organization that trades in it". In this research, an end-user is a person using computers in their capacity as an employee or in their private life.

There are several different methods for cybersecurity training of end-users available and described in scientific literature. These include text-based messages, instructor-led sessions, nano-learning, gamified training, and more (Abawajy, 2014; Aldawood & Skinner, 2018). However, those efforts struggle to provide the intended effect; secure enough behaviour (Bada et al., 2019). That is made evident by the continuous attacks successfully exploiting insecure user behaviour. Several reasons for why current practices fail are presented in literature where Bada et al. (2019) suggest that users actually know how to act but still do not act accordingly. The reason might be that following security advice can be too complicated or difficult (Whitten & Tygar, 1999). Other problems described in the literature include the difficulty of making users participate in the training. Many forms of cybersecurity training rely on the user's willingness to participate actively and will only be effective if the users do indeed participate (Gjertsen et al., 2017; Micallef & Arachchilage, 2017).

Consequently, user adoption is a crucial concern for cybersecurity training and pertains to participation in training and the adoption of the behaviour the training intends to promote. User adoption of technology is explained by Technology Acceptance Model (TAM). TAM is a frequently used information systems theory and describes that user adoption is influenced by a user's intention to adopt (Lee et al., 2003). Intention to adopt is, in turn, influenced by the user's perception of usefulness and effort required to use a technology (Davis, 1989). Given the widespread use of TAM in information systems research and its applicability for understanding user adoption of cybersecurity training, it is used in this research as a core theory for understanding user adoption.

Yet another concern regards how well users retain the knowledge they acquire in training and research have demonstrated that, for instance, the effect of lectures wears off after a few months (Lastdrager et al., 2017; Reinheimer et al., 2020). Puhakainen and Siponen (2010) further state that security solutions should be empirically evaluated to ensure that they provide their intended effect. Along
that line, Al-Daeef et al. (2017) and Alshaikh et al. (2018) argue that many current approaches for cybersecurity training are not grounded in empirical evidence of their effectiveness. Consequently, further research into how to conduct cybersecurity training is needed.

The area of this research is methods for cybersecurity training. The term method is defined by Cambridge Dictionary (2022b) as "a particular way of doing something". Further, the concept of methods has received interest from researchers in information systems research, where different definitions can be found (Cronholm & Ågerfalk, 1999). March and Smith (1995) describe a method as "a set of steps used to perform a task". Similarly, Hevner et al. (2004) describe that methods should guide problem-solving. This research does not seek to dwell into, or further, the scholarly discussion on the method concept but adopts the view described by Johannesson and Perjons (2014). A method is seen as a set of guidelines and processes which describes how a problem can be solved and goals be achieved. Subsequently, a method should be problem-oriented and explicate the goals the method seeks to achieve. The way to achieve those goals should be outlined as guidelines and processes.

**1.2 RESEARCH AIM**

To address the problem presented above, this research aims to develop a method that outlines goals and guidelines for cybersecurity training of end-users.

The research adopts a design science approach where an artefact (method for cybersecurity training of end-users) is developed to improve a situation (need for improved user behaviour in regards to cybersecurity). The need for a new method is motivated by the identified shortcomings of existing methods. Design science is an established research methodology in information systems and emphasises the development of artefacts which are grounded in theory and carefully evaluated (Hevner et al., 2004). Three objectives have been developed to clarify the research process:

- **O1**: Establish principles for cybersecurity training methods.
- **O2**: Establish requirements for evaluation of cybersecurity training.
- **O3**: Develop and evaluate a method for cybersecurity training of end-users.

A central principle in design science research is that existing theory should influence the design of new artefacts (Peffers et al., 2007). Previous research has questioned if that is the case with many existing cybersecurity training methods (Abraham & Chengkap-Snith, 2019). The first objective of this research ensures the theoretical grounding of the research by establishing principles for cybersecurity training based on the theoretical background of this work. The principles are developed based on previous research on cybersecurity training and TAM. The principles form the starting point for the remainder of the research and serve as input to the method development. The principles are then
reconsidered in each step of the method development process and refined during the research process.

The second objective responds to the need for empirically evaluated cybersecurity training methods. The need for rigorous evaluation is argued for in scientific literature. Several aspects to evaluate, such as knowledge retention, active participation, increase in awareness, and improved behaviour, are argued for in various publications (Al-Daeeef et al., 2017; Alshaikh et al., 2018; Gjertsen et al., 2017; Lastdrager et al., 2017; Reinheimer et al., 2020). However, no comprehensive evaluation criteria for cybersecurity training efforts have been found, making establishing such criteria necessary. This objective establishes requirements for cybersecurity. The requirements intend to describe what cybersecurity training should facilitate and forms the basis for evaluation.

The third objective is the core objective of this research, where a method for cybersecurity training of end-users will be developed and evaluated in an iterative design science process. The two distinct tasks of development and evaluation could merit two separate objectives. However, those are tightly interconnected in the design science methodology and therefore seen as one objective in this research. The process will start from the principles established in O1. Further, results gathered during the development process will be used to update the principles so that the principles are continuously reconsidered and updated through the research process. The evaluation will analyze how well the method meets the requirements established in O2. This process ensures that the results will be based on theory and evaluated rigorously.

O1 and O2 were explored before O3, and the emphasis of this research has been on O3. Nevertheless, the results from O1 and O2 were revisited in light of the iterative development in O3. As such, most of the included publications relate to O3, as shown in Figure 3 which shows the objective to which each publication mainly relate.
**CONTRIBUTIONS**

This research makes several theoretical and practical contributions where the central contribution is a method for cybersecurity training of end-users. The method developed in the research provides goals that explicate what cybersecurity training should facilitate and guidelines outlining how it should be
implemented. The method is a theoretical contribution that describes how cybersecurity training should be implemented. It is also a practical contribution that organizations can adopt to develop or procure cybersecurity training for their users. A developer can use it to guide the design of cybersecurity training tools, while someone procuring such tools can use it as a frame of reference. As an additional practical contribution, this research provides two freely available implementations of the method that anyone can use free of charge. Some of the implementations are available on GitHub.¹

A further contribution is the principles that the method for cybersecurity training is based on. The principles can be seen as guidelines for how cybersecurity training, intending to support a desired behaviour, should be developed. The principles were first derived from previous research and theory and then refined throughout the research process.

A further contribution is the general requirements and evaluation process that provide insight into how end-user cybersecurity training should be evaluated. Given the complexity of user behaviour in a cybersecurity context, it is expected that cybersecurity training can be evaluated in many ways. It is also expected that different evaluation approaches will evaluate different aspects of cybersecurity training. The results of this research provide an overview of different evaluation approaches, including insight into how the different approaches can contribute. The results can guide future research seeking to evaluate cybersecurity training efforts by providing a reference for such research.

The research also provides subsidiary contributions not directly related to the research aims and objectives. To enable evaluation of the method, implementations of it had to be developed and filled with training material. Research into the usability of cybersecurity practices was needed to ensure the quality of the presented material, and the output of such subsidiary studies make further contributions of this research.

1.3 DELIMITATIONS
Cybersecurity in general, and training within cybersecurity in particular, are interdisciplinary research topics. Delimitations have been made to limit the scope of this research and are presented here to allow the reader to understand the lens through which this research has been viewed.

The chosen topic is influenced by pedagogy and behavioural sciences. Pedagogy provides knowledge about how humans learn (Gergely et al., 2007). While learning plays an undeniable role in training users for whatever purpose, it should be pointed out that the intent of this research is not to do research in the area of pedagogy. Instead, the research can be seen as a consumer of some pedagogic literature to which the research relates. The same can be said about

¹ https://github.com/rr222cy/SecurityAssistantWidget
behavioural sciences, where human behaviour is central (Mrityunjoy, 1995). Theories describing or explaining user behaviour that stem from behavioural sciences are used and related to in this research. However, the research does not seek to expand on or otherwise research them. As such, the tasks and results of this research will focus on outcomes in terms of user preferences and effects on user actions which are common metrics in research on human aspects of cybersecurity.

A third research area related to the work carried out in this research is User Experience Design (UXD). While usability is central to both this research and UXD, the field of UXD puts more emphasis on the experiential qualities of artefacts than this research (Gómez-López et al., 2019; Rajanen et al., 2017). Further, UXD is central to designing artefacts of high experiential quality. The method developed in this research should support the implementation of cybersecurity training for end-users, and the experiential quality of such training is paramount. However, the research is separated from UXD and argues that UXD would be central in using the method rather than its development. The research utilized UXD techniques in artefact demonstration but does not claim to provide results in that domain.

A further limitation is the geographical area in which the research is conducted. Since the research is carried out by a Swedish researcher at a Swedish university, it is natural that participants at various steps in the research are predominantly Swedish. That is especially true for experiments that require the participants' physical presence. While actions were taken to demonstrate the transferability of the results to other contexts, it should be noted that the data gathered is first and foremost representative of Swedish users. However, some efforts have been made to show the transferability of the results to non-Swedish populations.

1.4 THESIS OUTLINE

This thesis contains six chapters, and while the author hopes that the entirety of the text is appealing enough for all readers to read from start to finish, it is possible that some instead focus on the parts that generate the greatest interest. To assist in selecting those exciting parts, Figure 4 shows the structure of this document.
The included chapters are briefly described as follows:

- The INTRODUCTION intends to describe, motivate and frame the aim of this research. It introduces the research area, outlines research aims and objectives, and delimitations.
- The BACKGROUND describes the domain of this research and presents an overview of core literature and theories that the research relies on or relates to.
- The RESEARCH METHODOLOGY outlines the epistemological standpoint of this research, the approach to research and supporting methods. It includes a discussion on ethical considerations related to the research area.
- The IMPLEMENTATION AND RESULTS explain the research process and outline results.
- The DISCUSSION contains a discussion of the results and the papers included in this thesis. The scientific rigour and validity of this research are discussed here.
- The CONCLUSION concludes the thesis by outlining this work’s academic and practical contributions and elaborating on possible directions for future work.
BACKGROUND
CHAPTER 2
2 BACKGROUND

This section seeks to describe the domain of this research and present an overview of core literature and theories that the research relies on or relates to. The chapter outline and relation to the rest of the thesis are shown in Figure 5.

Figure 5 Outline of the background chapter.
2.1 CYBERSECURITY IN BRIEF

Security related to the digital world is named using several different terms which, while they are defined differently, are to a large extent used interchangeably (Bishop, 2003; Craigen et al., 2014; von Solms & von Solms, 2018). Thus, there is a need to clarify the domain of this research and how that domain is perceived in this work. The most common terms are Computer security, IT security, Cybersecurity, and information security. NIST (2020) lists several definitions of the term Computer security, where the commonality is that all refer to the security of machines. In ISO/IEC 27032:2012, International Organization for Standardization for Standardization (2012) describe cybersecurity security as:

preservation of confidentiality, integrity and availability of information in the Cyberspace.

International Organization for Standardization (2012) further describe cyberspace as in ISO/IEC 27023:2012:

complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.

More recently, in ISO/IEC 27100:2020, International Organization for Standardization for Standardization (2020) defined cybersecurity as:

safeguarding of people, society, organizations and nations from cyber risks

The distinction between cybersecurity and information security is that information security concerns all information while cybersecurity is restricted to cyberspace. This research is concerned with training users to behave more securely in cyberspace, thereby minimizing or mitigating cyber risks. Therefore, it is positioned in the cybersecurity domain and adopts the definition provided by International Organization for Standardization (2020).

Improving and maintaining cybersecurity is an ongoing work that should be a part of any organization’s operation. The National Institute of Standards and Technology (NIST) is an American organization under the U.S. Department of Commerce. They develop standards and procedures for cybersecurity that are adopted worldwide. NIST (2018) developed a framework for cybersecurity comprising of the following five main functions:

- Identify where the central goal is to understand the organization’s assets and cybersecurity risks towards those assets.
• *Protect* where the core idea is to develop and implement measures to minimize the impact of or avoid harmful events.
• *Detect* is concerned with ensuring that the organization can identify when harmful events occur.
• *Respond* concerned with the development of routines and practices for response to harmful events.
• *Recover* where plans for restoration and recovery from incidents are developed.

This research concerns *Awareness and training*, which is a part of the *Protection* function. Therefore, the other functions will not be discussed further in the thesis. Similar to how NIST (2018) describe *Awareness and training*, International Organization for Standardization (2013) in ISO/IEC27001:2013 emphasize ensuring competence and awareness as integral parts of information security management.

Knowing how to protect efficiently requires understanding what threats to protect against and what actors are responsible for those threats (NIST, 2018). Over time, the landscape of threat actors has changed to include more sophisticated and well-equipped adversaries (Choo, 2011). The modern cybersecurity landscape includes threat actors who carry out attacks with varying objectives and reasons (Stankovska, 2016). Canadian Centre for Cyber Security (2020) and Kettani and Wainwright (2019) describe that discontent insiders can perform attacks with pre-existing access to the internal network. Further, external threat actors are described by Canadian Centre for Cyber Security (2020) as follows:

• *Nation-states* are states, or state-sponsored, threat actors who perform malicious activities for geopolitical reasons. This threat actor is often very sophisticated and has access to more resources than others. Moreover, they commonly operate over long periods (Bahrami et al., 2019).
• *Cybercriminals* are threat actors performing malicious activities for monetary gain. This is a vast category using versatile methods, including denial of service attacks, intrusions, online fraud, and more (Sabillon et al., 2016). As such, it does include more and less sophisticated adversaries.
• *Hacktivists* perform malicious activities for ideological reasons.
• *Terrorist groups* are motivated by ideological violence.
• *Thrill-seekers* are motivated by the satisfaction of completing an attack and are described by the Canadian Centre for Cyber Security (2020) as the lesser threat of the threat actors (together with terrorist groups and hacktivists). Those threat actors are seen as a lesser threat since their attacks seldom leave a long-lasting effect on cybersystems.

The threat actor needs a path for the attack to launch an attack (Simmons et al., 2014). This path is commonly referred to as the attack vector, and the number of possible attack vectors is high (Hansman & Hunt, 2005; Juliadotter & Choo, 2015; Simmons et al., 2014). Juliadotter and Choo (2015) described that attack vectors can be technological, physical, process-oriented, or human-oriented.
This research is concerned with the human-based attack vectors, which include attacks made possible by, or incidents stemming from, insecure user behaviour and referred to as human aspects of cybersecurity. The remainder of this chapter will, in turn, elaborate on the human aspects of cybersecurity and cybersecurity awareness and training.

2.2 HUMAN ASPECTS OF CYBERSECURITY

The scientific literature unanimously describes that user actions are a common cause of cybersecurity issues (Anwar et al., 2017; Mashiane & Kritzinger, 2018; Zimmermann & Renaud, 2019). However, the human attack vector, or the nature of the human aspects of cybersecurity, is described in the literature with ambiguity. For instance, Simmons et al. (2014) include human aspects in a taxonomy of attack vectors as social engineering. Social engineering is described by Salahdine and Kaabouch (2019) as attacks where individuals and organisations are manipulated in the interest of cyber criminals.

By examining examples of incidents relating to the human aspects of cybersecurity, it becomes evident that the human aspects encompass more than social engineering. Two examples are failure to comply with security policies (Al-Omari et al., 2012) and poor password habits (Florencio & Herley, 2007). Evans et al. (2016) describe that more than half of the worst breaches in 2015 occurred due to unintentional mistakes or errors made by users and discuss human behaviour as an aspect of cybersecurity. Further, Conteh and Schmick (2016) conclude that the vulnerability enabling social engineering is human behaviour. Similarly, Hadlington (2017) lists several actions that constitute risky cybersecurity behaviour.

For this research, the human aspect of cybersecurity is considered to be user behaviour concerning cybersecurity. Following that notion of the human aspect of cybersecurity, it includes both the human attack vector which is considered to be insecure user behaviour enabling threat actors to perform attacks and human behaviour that in other ways lead to cybersecurity incidents. This includes, but is not limited to:

- Insecure password habits such as selecting poor passwords, writing them down, or disclosing them to others.
- Incorrectly responding to phishing by, for instance, opening attachments from unknown senders or clicking on links leading to untrusted web pages.
- Susceptibility to social engineering by, for instance, disclosing sensitive data upon request.

Cybersecurity behaviour is commonly and historically described as one of the major challenges in cybersecurity (De Bruijn & Janssen, 2017; Desman, 2003; Hadlington, 2017). Interestingly, many users heard about cybersecurity, and organizations continue to inform users about desired behaviour (Bada et al., 2019; De Bruijn & Janssen, 2017). Still, users do not exhibit secure behaviour,
which presents a paradox (De Bruijn & Janssen, 2017). Two theories that are commonly used to explain cybersecurity behaviour are Protection Motivation Theory (PMT) and Theory of Planned Behaviour (TPB), both originating from psychological research (Bishop et al., 2020; Loukaka & Rahman, 2017). A third theory frequently used to understand cybersecurity behaviour, originating from information systems research, is Technology Acceptance Model (TAM) (Addae et al., 2019).

PMT was introduced by Rogers (1975) as a framework for understanding fear appeals, messages intended to motivate people towards certain actions by invoking fear. It has then been developed and used for several purposes, including understanding cybersecurity behaviour. PMT describes that a person’s decision to apply a protective behaviour is based on their perception of the threat the behaviour is intended to handle and their perception of the behaviour intended to handle that threat. The perception of the threat is described as a function of the perceived vulnerability to, potential harm of a threat, and potential positive aspects of continued exposure to the threat. The perception of coping behaviour is influenced by a person’s perceived ability to cope with a threat, the perceived efficacy of such behaviour, and its costs (Norman et al., 2015). Applied to the cybersecurity context PMT suggests that a user will select appropriate behaviour if they perceive it as effortless enough, given how the risk of not selecting the appropriate behaviour is perceived.

TPB was first described by Ajzen (1985), and a central notion is that a person’s intention to perform a certain behaviour is a key determinant for actual behaviour. The intention, in turn, is affected by the constructs; attitude, subjective norms, and perceived behavioural control. Attitude refers to a person’s perception of the behaviour in question. Subjective norms highlight social pressure speaking for or against the behaviour. Perceived behavioural control highlights the effect of ease or difficulty of performing a certain action. Extending TPB into the cybersecurity domain, TPB suggests that a user will engage in protective behaviour if the effort to do so is perceived as low enough. However, TPB also suggests that such behaviour is socially situated and highlights the possibility that a user may have a negative attitude towards a certain behaviour for different reasons.

A similar explanation can be found in the Technology Acceptance Model (TAM) developed by Davis (1985). TAM depicts that perceived usefulness and ease of using technology will influence users’ attitudes towards using it (Chuttur, 2009). The attitude will, in turn, lead to a decision on whether or not to use it. Davis (1989) further describes that perceived usefulness means how a person believes that using a particular system would enhance their job performance. On the other hand, perceived ease of use is defined by Davis (1989) as the degree to which a person believes that using a particular system would be free of effort.

This research has chosen to adopt TAM as the theoretical framework for understanding user adoption of technology. There are several reasons for this decision. First, TAM is grounded in information systems which is the area of this research. While PMT and TPB are useful tools, their application in the
cybersecurity domain provides psychological perspectives. This research do not intend to research or advance psychological perspectives of cybersecurity. In contrast, TAM provides an information systems perspective and is a useful theory to apply and relate this research to. Further, TAM is the most widely used theory in the information systems field, making it natural to relate to it in research that considers the use and adoption of an information systems artefact, the method for cybersecurity training developed in this research (Lee et al., 2003; Marangunić & Granić, 2015).

Even with the widespread use of TAM, a common criticism against it is that it provides an overly simplified view of user acceptance (Lee et al., 2003). One reason is that the original constructs of TAM are affected by external factors, which is highlighted in a later representation of TAM by Venkatesh and Davis (1996). Lee et al. (2003) show that the effect of several such factors has been found to impact the constructs of TAM. Understanding external factors relevant to the domain of cybersecurity training of end-users is a key issue in this research and will be elaborated on in the results section of this thesis.

Applying TAM to cybersecurity behaviour, it is reasonable to conclude that two major aspects would influence secure behaviour; the perceived benefit of engaging in secure behaviour and the perceived effort required to do so. The relationship between those aspects is that a user will accept a higher effort if the benefit is perceived as high. On the contrary, a low benefit can be accepted only if the effort is low. Consequently, support systems for cybersecurity behaviour should ideally maximize the perceived usefulness of secure behaviour while minimizing the effort of engaging in such behaviour. That aligns well with Siponen (2000), who argues that users must know what to do, why, and how. Given that a certain behaviour minimizes risk, the what and why would maximize perceived usefulness while how would minimize the effort required.

2.3 USER TRAINING AND AWARENESS IN THE CYBERSECURITY DOMAIN

Since cybersecurity incidents stemming from insecure user behaviour are common and the consequences often severe, the need for supporting users towards a more secure behaviour is apparent. The most commonly suggested approach for providing this support is through various means of knowledge and awareness-increasing interventions – training (Bulgurcu et al., 2010; Desman, 2003; Joinson & van Steen, 2018; Puhakainen & Siponen, 2010). Several different terms are used to describe those training efforts, including security training, Security Education, Training and Awareness (SETA), Security and Awareness Training (SAT), and more. While the terms can arguably be given different meanings, they are used interchangeably in the literature, and clarification of the terminology goes beyond the scope of this research. It is, however, useful to expand on how SETA is described in NIST Special publication 800-50. The three activities of awareness, training and education are described as follows (Wilson & Hash, 2003):

- **Awareness** includes measures intended to put focus on security. The intention is to put attention to and reinforce good security practices.
Training is intended to produce skills and knowledge relevant to a user's role and responsibility. Education intends to integrate different competencies to produce professionals.

Wilson and Hash (2003) also describe a step called Security basics and literacy positioned between awareness and training. This step seeks to teach all IT users the basic skills and knowledge needed to maintain a basic level of security. This research is concerned with all levels except education. It will use the term cybersecurity training as an all-inclusive term for the practice of cybersecurity training and awareness-increasing interventions designed for end-users.

Cybersecurity training aims to make users behave in a desired and secure way (Anwar et al., 2017; Evans et al., 2016; Safa et al., 2015). The fundamental assumption behind the use of training interventions is that users can behave securely only if they know how to and must therefore be informed about how to act. However, studies have shown that knowing how to behave does not always translate into the desired behaviour (Boss et al., 2015; Parsons, 2018; Siponen et al., 2014). That can arguably be explained by TAM, where it is suggested that users will only engage in secure behaviour if it is considered easy enough compared to the risk that the secure behaviour is intended to mitigate. A user is, for instance, only likely to follow guidelines for secure password creation as long as the extra effort of following the guideline is perceived as reasonable in relation to the perceived risk of the password being compromised and the perceived consequence of that. Following that argument, users must be informed about what to do and how and why (Siponen, 2000; Thomson et al., 2006).

The relationship between knowing what to do (Knowledge), why to do it (Attitude), and actually doing it (Behaviour) has been discussed previously in the domain of security awareness (Kruger & Kearney, 2006; Parsons et al., 2014). That is called the KAB model and suggests that knowledge plays a central role in behavioural change. KAB suggests that knowledge is an important driver for change in attitude and that change in attitude drives change in behaviour (Baranowski et al., 2003). KAB was not originally developed for use in cybersecurity, and there is disagreement to be found as to its significance (Baranowski et al., 2003; Bettinghaus, 1986). Still, in the domain of cybersecurity awareness, Parsons et al. (2014) show that knowledge is likely to positively affect attitude, which has a positive effect on behaviour. However, Parsons et al. (2014) stress that training material should be developed to influence awareness rather than providing general knowledge.

There are several different examples of how to conduct cybersecurity training that can be found in practice and scientific literature. Those include, but are not limited to:

- Physical lectures that users attend at a specific point in time (Reinheimer et al., 2020).
- Nano-learning typically includes short video instructions sent to users, often at regular intervals, via e-mail (Junglemap, 2022).
• Plain text such as pamphlets, e-mails, or informative texts online. Those are commonly provided to users via e-mail or websites in an on-demand manner (Stockhardt et al., 2016).

• Gamified training consumed by users on-demand, where games are used to teach (Gokul et al., 2018).

• Interactive training based on interactive media consumed by users on-demand (Van Rensburg et al., 2018).

• Instructive videos or audio recordings consumed by users on-demand (Ayyagari & Figueroa, 2017).

• Simulations where users experience attacks such as phishing and are then informed about the results (Cuchta et al., 2019).

Based on Al-Daeef et al. (2017) and (Aldawood & Skinner, 2018), contemporary methods for cybersecurity training can be grouped as follows:

• Classroom training is traditionally provided as on-site training but can also be provided as an online session. It is characterized by an instructor who provides training to participants at a certain time. It has been shown to effectively provide knowledge to users in several studies where the participants' knowledge is measured after the training session (Lastdrager et al., 2017; Van Rensburg et al., 2018). However, Taneski et al. (2015) suggest that a lecture-based intervention does not change behaviour to a high enough degree. Further, Lastdrager et al. (2017) show that knowledge gained from classroom training is not retained over time. Therefore, it is necessary to repeat the intervention or combine it with a second method for cybersecurity training. Another factor that is a challenge with classroom training is that of scalability (Al-Daeef et al., 2017). Providing classroom training to all members of a large organization can be costly and logistically challenging.

• Broadcast online training is training delivered to users through broadcasts via social media, web pages, or email. A common form of broadcasted online training is nanolearning, where small training modules are sent to users using email (Junglemap, 2022). The training type is intended to require little time from the user and be embedded into the user's workday, which is assumed to increase user participation (Al-Daeef et al., 2017). It has been shown to be appreciated by users when used outside of the cybersecurity context (Bruck et al., 2012). However, Al-Daeef et al. (2017) suggest that recipients of such emails may disregard them because they incorrectly think they already know how to defend themselves. Further, Khan et al. (2011) argue that messages sent using emails are not sufficient to change the recipients' behaviour and may fail to capture the recipients' attention, negatively impacting user participation.

• E-learning, where users are provided access to a digital platform where they can participate in on-demand training delivered in arbitrary format, provides scalable and easy-to-implement cybersecurity training (Hagen & Albrechtsen, 2009; Stockhardt et al., 2016). Both Hagen and Albrechtsen
(2009) and Stockhardt et al. (2016) show short-term effects of e-learning both in terms of knowledge and changed behaviour. However, Khan et al. (2011) argue that e-learning is unlikely to promote a behavioural change, and Stockhardt et al. (2016) found that users prefer classroom training over e-learning.

- **Simulations or contextual training** is described by Aldawood and Skinner (2019) and Al-Daeef et al. (2017) as a method where users are trained during a simulated phishing attack. Commonly, users are sent a false phishing email and provided with training if they act on that email. Cuchta et al. (2019) suggest that simulated attacks effectively increase users' awareness of phishing. The perhaps biggest problem with this type of training is ethical, demonstrated by the angry reactions of subjects in such studies (Jagatic et al., 2007). Further, simulations would arguably need to be repetitive to avoid problems with knowledge retention, similar to classroom training.

- **Gamified training** means that gamification is used to develop training material and is intended to increase user motivation and, thereby, participation (Jayakrishnan et al., 2020). Applying gamification in the design of cybersecurity training has been evaluated in several scientific studies with positive results regarding cybersecurity knowledge and behaviour (Gjertsen et al., 2017; Gokul et al., 2018; Jayakrishnan et al., 2020). However, the results presented by Gjertsen et al. (2017) question if gamification makes users participate in the training to a high enough degree. While users tend to appreciate gamified training, participation in such training may still not be high enough (Gjertsen et al., 2017; Huynh et al., 2018). However, adopting gamification does not exclude using the above-mentioned cybersecurity training methods. One could argue that gamification is a variation of the above methods that could improve participation rates. A similar notion can be deduced from Khan et al. (2011), who argue that games can change attitudes but are not as good at providing knowledge, suggesting that gamification combined with another method could be beneficial.

As argued by Bada et al. (2019) and made evident by the continuous incidents stemming from the human aspect of cybersecurity (Ani et al., 2019; Hatfield, 2018; Zimmermann & Renaud, 2019), cybersecurity training efforts fail to adequately support users to behave securely. Reasons for this, as described in the literature, include:

- Users are informed about how to act but not motivated to act accordingly (Bada et al., 2019).
- Knowledge acquired during training is only retained for a limited time (Reinheimer et al., 2020).
- Users are not actively participating in on-demand training (Gjertsen et al., 2017).
Many training methods are not based in theory, and their effectiveness is not empirically evaluated (Abraham & Chengalur-Smith, 2019; Siponen & Baskerville, 2018).

To conclude, existing research describes that training end-users is the key to promoting secure behaviour. Further, several methods for providing such training are discussed in the literature. While they all have strengths, they also face challenges that make current methods insufficient. The core challenges identified are knowledge retention, that knowledge does not ensure behavioural change and user participation rates. The challenges demonstrate a knowledge gap which is met in this research in two ways. First, this research starts from previous literature and outlines requirements for evaluating cybersecurity training as a response to the fourth challenge. The first three challenges are responded to by researching how they can be avoided or mitigated in the domain of cybersecurity training.
CHAPTER 2 BACKGROUND

RESEARCH METHODOLOGY
CHAPTER 3
3 RESEARCH METHODOLOGY

This chapter describes the research methodology used in this research and related topics. The outline is described in Figure 6.

Figure 6 Outline of the chapter research methodology.

Historically, Information Systems research has demonstrated diversity in what problems to address and how to address them (Benbasat & Weber, 1996). That diversity is demonstrated by the widespread use of various methodological approaches such as action research, case studies, design science, and combinations of those (Baskerville & Wood-Harper, 1998; Bilandzic & Venable,
2011; Galliers & Land, 1987; Hevner et al., 2004; Mumford et al., 1985). On a similar note, Hevner et al. (2004) point out that there has been a debate over the epistemological foundation of Information Systems research, e.g., positivism or interpretivism.

Positivism has been the historically dominant approach (Siponen & Tsohou, 2018). However, interpretivism is gaining more and more attention and is also well-established in the field (Walsham, 2006). Ryan (2018) describes that the two are in direct opposition to each other as positivism assumes that there is one reality that is the same for everyone. Experiments and quantitative research can describe what that reality is. On the other hand, interpretivism argues that reality is more subjective and should be interpreted in the individuals’ context, often using qualitative means. Goles and Hirschheim (2000) suggest pragmatism as a third paradigm that can be described as positioned between positivism and interpretivism.

This research adopts a pragmatic stance, predominantly for its focus on knowledge that is useful in action and the aim to introduce and evaluate interventions in the world (Goldkuhl, 2008, 2012). Kaushik and Walsh (2019) describe that the pragmatic paradigm focuses on solving problems identified in the real world and creating knowledge in the interest of change and improvement. Goles and Hirschheim (2000) describe that pragmatists acknowledge a common reality but believe that the reality is interpreted differently by different persons. Lee and Nickerson (2010) further emphasize that pragmatic research acknowledges knowledge held by people in general, including practitioners for whom the research is relevant. Further, pragmatic research leaves room for and appreciates applied research. This research seeks to develop an intervention (method) intended to improve a problem in the real world. As such, it is natural to adopt a pragmatic stance.

In terms of adopting research methods, the pragmatic paradigm is not constricted to qualitative or quantitative methods but seeks to use “what works best” in a specific situation (Kaushik & Walsh, 2019). That often leads to a mix of different research methods which is useful for exploring the diverse and often complex problems common in the information systems area (Goles & Hirschheim, 2000). The present case, the design of a method, will inherently include two distinct elements of design and evaluation. As Hevner (2007) argued, the design element should rely on state-of-the-art knowledge, and that implies the use of qualitative means for gathering such knowledge. Synthesising existing research in a domain is, for instance, often done using a systematic literature review which is most often qualitative (Kitchenham, 2004). Evaluation of the method should be empirical. Peffers et al. (2007) describe that Evaluation requires the definition of appropriate metrics and the gathering and analysis of appropriate data. That quote seems to imply the use of quantitative evaluation methods and, consequently, the pragmatic paradigm is suitable for a design and evaluation research process. As described in the background section, cybersecurity behaviour is impacted by several individual factors, which directly contradicts the positivist philosophy of one shared environment. Nevertheless, generalising results by gathering empirical data is an important part of this research. Likewise, qualitative analysis is a core part of gathering insights from
previous literature and from continuous interactions during the research. However, a fully interpretivist approach is argued to be limiting in how evaluations can be performed.

The research approach and its application are described throughout the rest of this chapter.

3.1 RESEARCH APPROACH

This research aims to develop and evaluate a method for cybersecurity training of end-users. The ultimate goal of that method is to make end-users behave more securely and, thus, be more resilient to cyber threats. As such, the research is concerned with developing a method that will positively impact the behaviour and, thus, the security posture of its users.

Design science is a well-established research method for information systems research seeking to develop artefacts to solve problems and is the research approach used in this research. Much like pragmatism, design science emphasizes complex problems and the design of interventions to solve those (Lee & Nickerson, 2010). It is described by Johannesson and Perjons (2014) as:

*Design science is the scientific study and creation of artefacts as they are developed and used by people to solve practical problems of general interest.*

The artefact is the central object of study in design science and can be one of four types; construct (vocabulary within a domain), model (describes relationship's among constructs), method (algorithm or guideline), or implementation (realization of an artefact in its environment) (Hevner et al., 2004; March & Smith, 1995; Peffers et al., 2007). Peffers et al. (2007) describe that each should be broadly defined. The artefact developed in this research intends to describe how to perform end-user cybersecurity training and is, therefore, best described as a method.

March and Smith (1995) further describe the central activities in design science as building and evaluation. The building is the construction of the artefact itself, and evaluation is concerned with developing criteria for evaluating the artefact and evaluating it against those criteria. The same notion is discussed by Hevner (2007) and Iivari (2007). They argue for the importance of separating design science in information systems research from the routine practice of developing information systems, where practitioners are commonly concerned with the latter. One such demarcation can be the evaluation activity where a researcher would employ a scientific approach to such evaluations. Iivari (2007) argues that this demarcation alone could lead to a reactive research field concerned with evaluating existing artefacts rather than developing new ones. A second demarcation suggested by Iivari (2007) is to specify a rigorous research method for developing artefacts. Hevner (2007) expanded that by adding rigour and
relevance cycles as additional activities surrounding the design science research. The rigour cycle is intended to ground the design science research in existing research and provide the research with state-of-the-art knowledge and existing artefacts in the research domain. Hevner (2007) stress the importance of building on prior research to guarantee that the design science research is indeed research and not routine design. The relevance cycle intends to establish the intended context of the artefact and evaluate the artefacts’ usefulness in that context. It addresses the fundamental goal of design science; the development of artifacts that improve their environment (Simon, 1996).

Hevner et al. (2004) describe six guidelines for design science research. Those are described by Peffers et al. (2007) as guidelines describing well carried out research. Further, Peffers et al. (2007) present a practical framework for design science which provides a practical guide that this research followed. The guidelines presented by Hevner et al. (2004) have been interpreted as "what" design science seeks to achieve, while the work of Peffers et al. (2007) is interpreted as a guide to "how" it should be achieved. The guidelines presented by Hevner et al. (2004) are used as a basis for discussing the scientific rigour of this research in Section 5.2 Scientific rigour. The framework by Peffers et al. (2007) guided the practical application of the research process.

The remainder of this chapter presents the guidelines introduced by Hevner et al. (2004), describes the practical implementation of design science in this research, supporting methods, and ethical considerations.

The first guideline concerns Problem Relevance and prescribes that design science aims to develop solutions based on technology to address business problems. As such, developed artefacts should contribute to their environment by solving a problem or better a situation. However, the artefact must also be useful in reality and possible to implement in its intended environment. On this note, Hevner et al. (2004) stress the need for instantiation, namely building and demonstrating the artefact.

Research Rigor is the second guideline and requires that rigorous methods are used in both the construction and the development of the artefact (Hevner et al., 2004). The need for empirical methods for artefact evaluation is stressed. Hevner (2007) described that rigour is also achieved by careful use of the existing knowledge base relating to the problem at hand.

The third guideline is Design as a Search Process which describes the design as searching for an effective solution to the problem at hand. The search is described to often be iterative and beginning with a simplified solution to a simplified representation of the problem. The scope of the problem can grow as the design science process continues. Hevner et al. (2004) describe that many information systems design problems are wicked problems where fully determining the domain is impossible or infeasible. It may not be possible to understand why an artefact works in those situations. However, Hevner et al. (2004) argue that the critical outcome is to establish that the artefact works and in which environment it works.
The fourth guideline, *Design as an Artifact*, discusses that the artefact must be effectively represented to enable application in its intended environment. Hevner et al. (2004) also stress that the artefact must be presented in a way that enables comparison and evaluation in regard to other artefacts for the same purpose. On this topic, Friedman (2003) argues that explicit articulation is necessary for allowing the theory to be tested and reflected upon.

*Design Evaluation* is the fifth guideline and depicts that the quality of the artefact must be demonstrated by evaluation. Design is described as an iterative process, and an inherent difficulty of iterative research is knowing when to stop. The artefact is considered complete when it meets the criteria established for it when it solves the problem it is intended to solve (Hevner et al., 2004). Evaluation should be performed using appropriate research methodologies, and that is dependent on the artefact’s nature and intended environment.

The final guideline is *Research Contributions*. It describes that a design science project should result in contributions in the form of the artefact itself, theoretical insight, and/or new methods or metrics to evaluate by.

### 3.2 IMPLEMENTATION OF DESIGN SCIENCE

The literature just discussed presents guidelines and the fundamental theory describing well carried out design science research. The results and process of this research will be discussed in relation to the guidelines presented by Hevner et al. (2004). However, there are several ways in which design science can be implemented. That is demonstrated by several publications suggesting different Design Science Research Methods (DSRM) (Baskerville et al., 2009; Peffers et al., 2007; Sein et al., 2011; Vaishnavi, 2007).

The DSRM applied in this research is outlined by Peffers et al. (2007) and was adopted because of its extensive previous use and for being well-known. It also provides clear, practical rules for implementation. Peffers et al. (2007) describe six activities that can be executed in various orders with varying levels of iterations. For research starting with problems observed in prior literature or reality, as is the case here, it is common to start the process from the first activity and then move forward with varying degrees of iterations. This section describes the activities suggested by Peffers et al. (2007) and explains how they are performed in this research. This research comprised three design cycles (DC), and a conceptual overview of the DSRM, as implemented in this research, is displayed in Figure 7. The six square boxes correspond to the six activities described by Peffers et al. (2007), which are further described below. The black, grey, and white boxes make one DC.
Figure 7 Visualization of research strategy.

The first activity is *Problem identification and motivation* and is concerned with defining the problem space and motivating the research problem. Hevner (2007) argues that identification and use of prior scientific literature is a key factor distinguishing design science, as a scientific method, from design practices performed by developers. This research began with this activity and resulted in this thesis’s introduction and background chapters, outlining the problem, intended solution, and domain.

The second activity, *Define the objectives for a solution*, stresses the need for determining what criteria the artefact should meet, which should be inferred from the problem specification and based on previous knowledge and existing solutions (Peffers et al., 2007). Peffers et al. (2007) also stress the importance of a structured evaluation process. The evaluation approach and requirements of the artefact developed in this research were defined before starting the design process. The purpose is similar to that of establishing inclusion criteria for a literature review before conducting the searches to minimize researcher bias (Wohlin et al., 2012). This phase intended to define objectives for the solution and explicate how the solution should be evaluated. First, principles for how cybersecurity training of end-users should be carried out were inferred from previous research and the Technology Acceptance Model. The principles make the theoretical underpinning of the method for cybersecurity training which is the central topic of this research, and they were refined throughout the research. This phase also included establishing requirements for cybersecurity training of end-users and a process of evaluation for such training. The requirements describe what such methods should achieve and are used in the remainder of this research as requirements for the evaluation of cybersecurity training. Further, a process for how to carry out that evaluation was established.

Artefact development is the core of design science. As Hevner et al. (2004) described, it is usually an iterative process of development, demonstration, and evaluation towards an incrementally more complete artefact. Peffers et al. (2007) describe the three activities of *Design and development, Demonstration, and Evaluation*. In this research, those phases combined are considered to make one design cycle (DC). Given the complex nature common in design science research, it is non-trivial to decide when the research is completed. The research was considered completed when the artefact satisfied the established evaluation criteria. It included three DC with different roles, as follows:
DC 1: Further explore the problem space and articulate a conceptual notion of a method.
DC 2: Propose a complete method based on the results of DC1.
DC 3: Refine the method proposed in DC2.

The Design and development activity is concerned with creating and developing a method for cybersecurity training of end-users. The demonstration activity aims to demonstrate the usefulness of the artefact by demonstrating that it can solve the problem it intends to solve or a subset of the problem. Evaluation is concerned with the empirical evaluation of the effectiveness of the artefact; how well it meets the established requirements.

In the first DC, input to the design and development process was taken from existing literature and used to form principles for cybersecurity training for end-users. The principles were then used as the basis of a conceptual description of the method. The conceptual description was used to develop demonstrators that exemplified how the method could be implemented, which were used for evaluation. Data from the evaluations and subsequent discussions at scientific conferences were used to develop the method further to include goals and guidelines for implementing cybersecurity training in the second DC. The updated method was implemented as a training intervention that educated users of a website on how to create strong passwords. The evaluation measured the intervention's impact on the strength of the passwords created by the user when they registered an account and how much of the provided knowledge they noticed. The evaluation results and subsequent discussion in various forums were used to refine the method in the third DC. In DC three, an instantiation of the method that educated users on password security, online fraud, fake news, and phishing was developed. The evaluation included an experimental evaluation of the implementation and a survey that evaluated potential users' perception of cybersecurity training implemented according to the developed method. This evaluation step suggested that the method satisfied the evaluation requirements making the third DC the final DC in this research.

Several implementations of the method have been developed during the research to experiment and empirically evaluate the method's effectiveness. The implementations further served the purpose of the demonstration activity making the two activities highly connected. On this note, Hevner et al. (2004) argue that design science artefacts should be evaluated based on their usefulness in the environment they are designed for. The task of developing implementations of the designed method was performed to demonstrate the methods' usefulness in practice. Further, the method was evaluated using experiments and other methods as a means of triangulation to improve the validity of the results, as suggested by Lincoln and Guba (1985). While the primary approach to evaluation was quantitative, qualitative data was also gathered and used to inform the artefact design.

The last activity described by Peffers et al. (2007) is Communication which stresses the need to communicate the research results. The results of this research are concluded in this thesis, and intermediary results were
communicated in academic venues throughout the research. The resulting publications are appended to this thesis starting at page 133. A publication plan has been followed where early publications have been published in academic conferences that specifically invite research in the domain of human aspects of cybersecurity. The intention was to allow for the scientific community's input to benefit the research. Later publications have been submitted to more general conferences and journals to maximize the impact and improve the quality of the research.

### 3.3 SUPPORTING METHODS

The core activities in Design Science research are described as artefact development and evaluation (Hevner et al., 2004). While those activities should be based on the state of the art and empirical data, design science literature demonstrates a great degree of freedom regarding which research methods to apply for this purpose (Johannesson & Perjons, 2014; Peffers et al., 2007). This research used a mix of qualitative and quantitative approaches where qualitative approaches were used for artefact development, and quantitative approaches were mainly used for evaluation. Hevner et al. (2004) describe the development process as searching for an incrementally more complete solution to a complex problem. As described by Merriam (2002), a qualitative approach is intended to result in a better understanding of a phenomenon and yield descriptive results. Quantitative research, on the other hand, is commonly used to evaluate hypotheses statistically and, in this research, used to evaluate the performance of the designed method for cybersecurity training (Sukamolson, 2007).

Further, several data collection methods are used throughout this research. How those are used is introduced throughout the rest of this section. More explicit descriptions are provided in the eleven papers appended to this thesis, starting from page 135.

#### 3.3.1 STRUCTURED LITERATURE REVIEWS

Grounding the research in the existing literature is a fundamental part of what distinguishes design science research from routine design (Hevner et al., 2004). This research used Structured Literature Review (SLR) methodology to consult previous research in various stages of the research:

- Before starting the first design cycle to formulate requirements that the developed method should meet and a process for evaluation of cybersecurity training of end-users (Paper 8).
- At the beginning of the research to establish principles for cybersecurity training of end-users.
- Continuously throughout the research to support development of implementations (Papers 7 and 10). Developing instantiations will inherently require educational material to be produced. While that is not a core part of the research, this material's quality and accuracy should be assured. Such material was based on relevant research identified using SLR.

SLRs in this research followed the procedures described by Kitchenham (2004) to ensure unbiased results. This process stresses the importance of a pre-
established protocol for article search, criteria for inclusion and exclusion of articles, and analysis methods. Analysis of included material typically used a thematic approach in an open or closed fashion, as described by Braun and Clarke (2006).

**3.3.2 SURVEYS**

Surveys allow for data collection from large samples in a structured and systematic way (Oates et al., 2022). Surveys were used in the research for two purposes. First, the collection of quantitative data used to evaluate the developed method. Likert scale is a non-parametric question type commonly used to research respondents' opinions and was used as the primary means of evaluating user perceptions (Joshi et al., 2015). Those were combined with evaluations that aimed to gather parametric data and avoid participant self-assessment in order to avoid response bias (DiStefano & Motl, 2006; Van de Mortel, 2008). An example is one survey that used the developed method to present information to the participants and then asked them factual questions about the information just presented to them before their number of correct answers was measured. The participants were then asked about their perception of the presented training (Paper 4).

Gathered data was analyzed using statistical methods. Measures of statistical significance and hypothesis testing were used for this purpose. The main statistical procedures used were the T-test and Analysis of Variance (ANOVA). T-test was used for pairwise analysis, and ANOVA was used for analysing data containing more than two sample groups. Both tests are typically considered robust for parametric data, which is normally distributed. However, some researchers argue that it can be robust even if those data assumptions are violated (Norman, 2010). Statistical analysis performed in this research typically used parametric tests as the primary procedures but complemented with non-parametric alternatives, such as Mann-Whitney U-test, to avoid the debate over what procedure is most appropriate (McKnight & Najab, 2010). That also served as a means of triangulation to increase the validity of the results (Lincoln & Guba, 1985). Additional procedures were used as deemed appropriate and explained in the research papers where they are used.

Further, qualitative data was collected using free text fields, which allowed participants to express their opinions about the method. This data was used for further development of the method and typically analyzed using a thematic approach. Surveys were included in Papers 1, 2, 4, 10, and 11.

**3.3.3 EXPERIMENTS**

Cybersecurity training methods should ultimately be evaluated by their actual effect on cybersecurity behaviour. Experiments were used to evaluate the method in naturalistic environments. Tichy (1998) argues that an experiment offers the opportunity to examine how an intervention works in its intended environment. However, Campbell (1957) demonstrates that field experiments can be affected by many external factors, and care must be taken to ensure the validity of the results. Experiments conducted within this research used an experimental design with several groups. One group of subjects received training
based on the developed method, and one or more other groups acted as control groups that received training using other methods or no training at all. That is a typical experimental design for evaluating the effect of a new intervention which the developed method is an example of (Gui et al., 2015). This setup is intended to minimize historical bias stemming from mere participation in an experiment which is a concern in pre-post test experimental design (Campbell, 1957). Experiments conducted in this research are reported in Papers 3, 4, and 9.

3.3.4 FIELD NOTES

Being developed as part of a research project spanning several years, intermediary results of this research were discussed in several different forums where it received feedback in more or less structured forms. This included feedback following presentations on academic conferences, discussions during poster sessions, and discussions with practitioners in various forms. Phillippi and Lauderdale (2018) argue that this type of less structured data is valuable in qualitative research and was collected in this research and used in the artefact development stage. The collection was made by taking notes during discussions of relevance to this research. Field notes have been used as a data source in previous design science research (Gaspareto & Henriqson, 2020; Tura et al., 2018). In this research, field notes allowed the artefact development to benefit from feedback from academic and professional forums, as described in Paper 6.

3.4 SAMPLING AND LIMITATIONS

This research involves gathering data from human participants, primarily for evaluation and method design. The inclusion of human participants raises the issue of sampling to ensure that the results are as representative as possible. As Fowler Jr (2013) discussed, a probability sample is the best way to ensure that a sample is representative of the population it intends to represent. It does so by ensuring that every member of the population has an equal chance of being included in the sample. However, acquiring a probability sample is often expensive and impractical, leaving room for other sampling techniques (Fowler Jr, 2013). In this research, the intended target group for the results comprises all users in cyberspace. Generating a probability sample of that group is infeasible for surveys and impossible for experiments. Instead, a sampling approach that can generate a strong result within a sample frame and assess those results' transferability to other sampling frames was used, as suggested by Lincoln and Guba (1985). Moreover, it was decided to allow for less rigorous sampling in the early stages while putting more effort into sampling participants in the later stages of the research. The rationale was that initial evaluations served to test initial ideas to identify that the fundamental design options were sound. Later evaluations served to rigorously evaluate the designed method with a high degree of scientific validity.

In contrast to probability sampling, non-probability sampling includes sampling techniques that do not give every member of the population a chance to be included in the sample. In broad terms, non-probability sampling involves selecting participants deemed to be of high value to the research (purposive sampling) or including readily available participants (convenience sampling). The consequence of both approaches is that it is hard to generalize the result
within the sample to the broader population (Etikan et al., 2016). Still, non-probability samples are more practical to acquire and often less expensive. They are useful in several cases, especially in the initial stages of research and when the researcher is interested in gathering data from a specific part of the population.

This research employed all three sampling strategies with different purposes. Early survey-based evaluations had the purpose of initial testing of ideas and used convenience-based sampling. While the results of those evaluations cannot be argued to be representative of the entire population, they provided valuable insights to the research at a low cost. In the later stage of the research, survey-based evaluations employed probability-based sampling within Sweden, Italy and the UK. The rationale was that the results should first be generalizable within Sweden, and then the transferability of those results into other populations was assessed, as Lincoln and Guba (1985) suggested. Experimental evaluations introduced the challenge of proximity since potential participants, by necessity, had to be in reasonable geographic proximity to the researcher. Thus, the sampling technique used for experiments included an element of convenience sampling based on proximity which was combined with purposive sampling. The primary sample frame was students and working people who are not studying or working within IT. The rationale was that students and workers are within the context of organizational IT environments and therefore adhere to security policies. Further, their security behaviour can have an organizational impact making them the primary target of the method that this research developed. Participants with high IT competence were excluded because they were assumed to possess higher than average knowledge in cybersecurity. That could be a confounding variable that would negatively impact the internal validity of the experiments (Henry, 1990). Field notes from discussions with researchers and practitioners in various forums made a central contribution to this research. This is an example of purposeful sampling to gather data from information-rich cases (Palinkas et al., 2015). Details for the different evaluations are outlined in the papers where they are presented.

The sampling strategy is intended to achieve as high-quality data as possible in a feasible way. It does, however, introduce limitations. First, experimental evaluations focused on Swedish users who are working or studying, and the results in that part are generalizable over that population only. Survey-based evaluations are primarily representative of Swedish users, where evaluations took place using probability sampling methods. Further, the results have been compared and evaluated as consistent in Italy, and the United Kingdom (UK) and are therefore generalizable in those contexts. The degree to which the results of this work are general outside of those sample frames is unknown and should be treated as such.

A discussion related to sampling is that of selecting cases for evaluation. In this research, several tools for cybersecurity training of end-users have been developed based on the developed method. Those tools intend to demonstrate the usefulness of the method in practice. However, while the purpose of the method for cybersecurity training of end-users is to be applicable for cybersecurity topics in general, it has not been possible to develop tools for all
possible cybersecurity topics. Instead, topics have been chosen based on two criteria. First, selected topics that supported quantitative evaluation were prioritized. Second, topics that were considered important in the cybersecurity domain were selected. For example, password habits and phishing were selected topics since they make some of the most commonly used vectors of cybersecurity attacks. Further, password quality and user response to phishing can be quantified with relative ease making the topics suitable for quantitative evaluation.

### 3.5 ETHICAL CONSIDERATIONS

AIS Code of Ethics and Professional Conduct demonstrates that all research must adhere to research ethical principles (AIS, 2019). Swedish Research Council (2017) further describe that the area of research ethics, while ill-defined, concerns the relationship between ethics and research as well as ethical standards that researchers should meet. Swedish Research Council (2017) further describe that ethics often contain discussions on what is good and bad and that a code of ethics is a collection of ethical rules agreed upon in a community. On that note, such a code can specify general rules and additional rules for different communities and cases. While this research is naturally subject to general ethical considerations, just as any research would, the nature of the cybersecurity subject, the application of design science, and the use of participatory research methods constitute aspects where particular care must be taken. Those aspects will be discussed next before the ethical principles applied throughout the research are presented.

As discussed by Schrittwieser et al. (2013) and Dittrich et al. (2009), research in the cybersecurity domain poses ethical challenges. One such challenge is the potential misuse of the research output (Schrittwieser et al., 2013). An example could be that research into phishing susceptibility, while important for understanding the topic, can also assist attackers by providing insight into how more effective phishing messages can be constructed. While this argument is reasonable, it would prevent a substantial amount of important research in cybersecurity. As such, this point alone cannot discourage a research project, but it highlights the importance of solid ethical practices.

A second challenge is that the research itself should not harm others, and this challenge can be compared to the domain of penetration testing. There are many examples of studies where researchers send phishing emails to participants in the name of science. That raises an interesting ethical dilemma: Is it ethically sound to measure how many respondents open the mail? Is it then also sound to measure how many who click a link contained in the mail? Would it also be sound to evaluate how many respondents submit account details on the website that the link is leading to, and would it be okay to verify if the account details are actually real by logging in as the participant?

While the last step would constitute a crime (at least under Swedish jurisdiction), drawing the ethical line is difficult (Dittrich et al., 2009). Dittrich and Kenneally (2012) describe that a foundation for ethical research is respect for persons, law, and public interest and should maximize benefit while minimizing harm. In
practice, research in cybersecurity behaviour and awareness is concerned with affecting users' behaviour, which requires consideration. On the one hand, it can be argued that research on user awareness can be more reliable if the full nature of the research is not disclosed to participants. Telling participants that their awareness will be measured will likely make them more aware and introduce bias. On the other hand, performing participatory research without the participant's voluntary participation will fail to meet the respect for persons requirement present in most ethical frameworks (Renaud & Zimmermann, 2018). A more deceptive approach can lead to more reliable and, therefore, beneficial results. This notion introduces a trade-off between respect for persons and research outcomes that will be further discussed later in this section.

While design science research is certainly subject to traditional ethical constraints, Johannesson and Perjons (2014) argue that design science research must also consider ethics in relation to the developed artefact. Further, Myers and Venable (2014) argue that the ethical foundation for design science research is fundamentally different from that of many other disciplines. The key argument is that the artefact is supposed to be used by the public long after the research is finished. The consequence is that ethical principles should be weighted in favour of public interest when there is a conflict between the interests of the public (i.e., benefit) and the interests of participants (i.e., respect for individuals). This notion opens up for more deceptive research approaches, but those should be used with great care on the back of ethical guidelines from other disciplines.

Renaud and Zimmermann (2018) demonstrated that there are several ethical frameworks presented by different bodies. The ethical principles followed in this research are primarily based on Schrittwieser et al. (2013) and Dittrich and Kenneally (2012). They present ethical guidelines for research in Information and Communicating Technology and Information security. They are also influenced by Myers and Venable (2014), who present an ethical framework for design science research. The principles are explained next.

3.5.1 RESPECT FOR INDIVIDUALS
The meaning of this principle is that participants in research should be aware of what they are participating in, the potential risks with participation, and how their personal data is treated. Dittrich and Kenneally (2012) describe that this involves carefully explaining the research process that the participants are involved in, explaining that participation is voluntary and that the participant may leave at any time without negative consequences. That is commonly done using an informed consent form signed by the participant (Myers & Venable, 2014). Schrittwieser et al. (2013) discuss that it can sometimes be hard to follow strict ethical principles while performing valuable cybersecurity research. On that note, Dittrich and Kenneally (2012) describe that obtaining informed consent before a study may not always be possible, and the requirement to obtain informed consent could be lessened if necessary for the research to obtain usable data. However, the requirement of minimizing harm and maintaining the participant’s anonymity would grow in cases where informed consent is not used in advance. This falls in line with the discussion had by Myers and Venable (2014), who stress that different ethical components may conflict with each
other. If one is to be violated or given less importance, another one should be given higher importance.

Some activities in this research do intend to measure awareness. As previously described, evaluation of the developed method involves measuring its impact in experimental and naturalistic environments with human participants. Informing the participants of the full nature of the study will likely introduce bias. During the planning of such activities, the ethical implications of various research designs have been continuously discussed within the supervisor team and with the council for research ethics at the University of Skövde. Three active measures have been taken during this research:

• Participatory research where the full nature of the research could not be disclosed to the participants was not included in the first design cycle. That allowed the method to be more mature and, therefore, arguably more beneficial before it was tested in a way that included disclosing the full nature of the research only after the study.

• In activities where the full nature of the research was not disclosed to participants before a study, actions were taken to fully debrief the participants after the study, for instance, in Paper 4.

• In some activities, the research methodology was designed so that bias stemming from knowing the full extent of the research did not impact the research questions addressed. This was the case in Paper 9, which measures the effect of cybersecurity training in a scenario where the participants are assumed to be more security-aware than usual due to their participation in the experiment.

3.5.2 BENEFICENCE
This principle includes the assessment of possible harm and benefits stemming from the research (Dittrich & Kenneally, 2012). Ideally, a research project should cause no harm but only benefit. Dittrich and Kenneally (2012) stress the need to identify possible causes of harm and plan to minimize those causes. In design science, possible harm could be that the developed artefact is not of high enough quality (Myers & Venable, 2014). That risk was handled in this research by implementing rigorous research methods to evaluate the method that is being developed.

3.5.3 EQUALITY
The equality principle argues that groups of participants should not be excluded for reasons unrelated to the research (Dittrich & Kenneally, 2012). While this principle should not be confused with sampling techniques employed for statistical reasons, the intent is to ensure that all possible participants have an equal chance of participating in the research and thereby be accounted for in the results. On that note, selection bias based on gender and race has been noted in previous research. It can arguably lead to research more suitable for particular groups (Harrison & Thomas, 2009; Holdcroft, 2007). While this research employed various sampling techniques for various purposes, efforts were taken to grant all members of sample groups an equal opportunity to participate in the research for ethical purposes and improved research validity.
3.5.4 RESPECT FOR LAW AND PUBLIC INTEREST

This principle stipulates that research should comply with laws and regulations (Dittrich & Kenneally, 2012). Laws make out a strict boundary that should not be crossed even if the intent is to harm other illegal activities (Schrittwieser et al., 2013). That involves identifying and understanding regulations that may affect the research. By collecting data from participants, this research was affected by General Data Protection Regulation (GDPR). Participants were anonymous, and data subject to GDPR was not collected to the greatest extent possible. However, anonymity was not possible in all experiments within this research. In those cases, GDPR was adhered to in addition to the information requirements stipulated by the respect for persons principle. No personal data has been collected without prior consent from the data subject. As a general rule, collected data was kept to a minimum and discarded as soon as it was no longer needed. Further, this research is subject to Swedish law, where the need for ethical clearance is defined in the Swedish Ethical Review Act (Swedish Research Council, 2017). The need for ethical approval has been continuously discussed within the supervisor team and with the council for research ethics at the University of Skövde. The result has been that ethical approval has not been needed for the activities in this research.

Dittrich and Kenneally (2012) also describe that this principle includes conducting and reporting on research in a way that is in the public's best interest. In part, this includes transparency and well-described research processes, and that is, in this research, argued to be a vital and fundamental part of the research. Methods used, data gathered, and results obtained were continuously reported transparently. This principle can, arguably, be stretched to making research results available to the public, and the consequence of that would be the notion that Open Access (OA) publishing is beneficial. While OA publishing was not possible for all intermediary results in this research, the aim was to publish as much as possible of the research results as OA.
IMPLEMENTATION AND RESULTS
CHAPTER 4
4 IMPLEMENTATION AND RESULTS

This chapter outlines the steps carried out in this research and the results of each step. The outline of the chapter is shown in Figure 8.

The activities described in this chapter are visualized in Figure 9 and outlined in the coming sections. Results from the research have been continuously published in peer-reviewed conferences and journals. The publications are appended to this thesis and referenced throughout this chapter as Paper 1 to Paper 11. The chapter ends with a summary of the method for cybersecurity training of end-users, Context-Based Micro-Training (CBMT), developed in this research. The summary is written as a stand-alone description of CBMT.
CHAPTER 4 IMPLEMENTATION AND RESULTS

4.1 THEORETICAL FRAMEWORK

This section will explicate the theoretical framework that guided this research. It corresponds to the first research objective, Establish principles for cybersecurity training methods. The principles intend to describe how cybersecurity training for end-users should be developed and provides the starting point for the design science process and the development of requirements for cybersecurity training. The principles are derived from previous research describing challenges with existing methods for cybersecurity training and the Technology Acceptance Model (TAM). TAM is selected for two reasons. First, user adoption is a core concept in this research. Any cybersecurity training method aims to make users adopt a secure behaviour. What secure behaviour means is described to users using security training methods, and the users also need to adopt the cybersecurity training provided to them. Second, the subject of this research is information systems, and the research intends to contribute to the information systems domain. Consequently, adopting TAM as the theoretical basis for the research is reasonable since TAM is a widely used information systems model for understanding user adoption of technology.

Challenges identified in previous cybersecurity training research were described in the Section 2 BACKGROUND but will be briefly repeated. Then TAM and its implication for cybersecurity training methods are described. The section will end with explicating principles describing how cybersecurity training should be implemented, and those principles serve as the starting point for the remainder of the research. The principles are then revisited and refined throughout the research process. The role of the principles in this research and how they evolved during the research is visualised in Figure 10.

Figure 9 Overview of the research plan. Black boxes show artefact development tasks, grey show demonstrations and white show evaluations.
4.1.1 PREVIOUS RESEARCH ON CYBERSECURITY TRAINING

Previous research suggests that existing cybersecurity efforts fail to support users toward secure behaviour adequately. Four key reasons for this can be found in the literature. First, Bada et al. (2019) suggest that training is often used to inform users how to act but does not motivate users to implement accordingly. The essence of this issue is that even if users are informed about how to act, they must also adopt the desired behaviour, which is not certain to happen for several reasons. Parsons (2018) suggests that mechanisms that make users "stop and think" before making security decisions can be beneficial. Similarly, Coventry et al. (2014) describe that knowledge alone does not mediate behavioural change, but the behaviour is influenced by other factors such as context, willpower and beliefs. They also suggest that nudging, providing cues when a decision is to be made, can support secure behaviour.

A second issue described in prior research is that of knowledge retention. In essence, knowledge acquired during training is only retained for a limited time (Reinheimer et al., 2020). Recently, Chowdhury and Gkioulos (2021) pointed out that integrating cybersecurity training into daily routines is favourable for knowledge retention, further highlighting this concept's importance. Knowledge retention should be a central concept for methods for cybersecurity training (Al-Daeef et al., 2017). The reason is that users cannot be expected to continuously apply learnt security practices if they do not remember them.

The third key reason why current cybersecurity training methods fail is that users are not participating to a high enough extent. For instance, Gjertsen et al. (2017) highlight that getting users to adopt on-demand training can be challenging. Naturally, the intended effect is lost if users do not adopt cybersecurity training.
4.1.2 TECHNOLOGY ACCEPTANCE MODEL

The Technology Acceptance Model (TAM) is used in this research as a theory by which to understand user adoption. User adoption is a key concept for a method for cybersecurity training of end-users in two ways. First, the method must support user adoption of itself. More concretely, a training method must facilitate user adoption since it cannot train users that do not adopt it. Second, a method for cybersecurity training must support user adoption of the information it is trying to convey.

The original version of TAM includes three constructs that influence a user's decision to adopt technology; Perceived Usefulness (PU), Perceived Ease of Use (PEOU), and Intention to Use (IU) (Davis, 1985). PU and PEOU influence IU, which then influences adoption. Several modifications and extensions to TAM have been proposed. A commonality is the addition of external factors that influence the original constructs, the relationships between those, or the effect of other external factors (Lee et al., 2003). Both Lee et al. (2003) and Venkatesh and Bala (2008) outline external factors presented and evaluated in previous research. Those factors are presented and categorized below, and implications for cybersecurity training are derived. The categorization takes a socio-technical approach and divides the external factors into organizational, social, and technical factors. The factors' relevance for the development of a method for cybersecurity training is discussed for each category.

Organizational factors
Organizational factors refer to factors that relate to the users' environment. Those are described in Table 1.

Table 1 External TAM factors relating to the organization a technology is implemented in.

<table>
<thead>
<tr>
<th>Factor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subjective norm</td>
<td>A user is more likely to use a system if the user believes that people important to the user think that the user should.</td>
</tr>
<tr>
<td>Image</td>
<td>PU will increase if a user perceives that using a system will positively impact social status.</td>
</tr>
<tr>
<td>End-User Support</td>
<td>Promoting favourable beliefs about a system through support will increase PU and PEOU.</td>
</tr>
<tr>
<td>Visibility</td>
<td>A system that is more visible in an organization is more likely to be adopted by users of that organization.</td>
</tr>
<tr>
<td>Management support</td>
<td>A higher degree of support from managers will increase the chance of user adoption.</td>
</tr>
</tbody>
</table>
Facilitating conditions  |  External factors such as availability of time and money can impact user adoption of a system.
---|---
Physical accessibility  |  The degree to which one has physical access to the hardware needed to use a system will impact perceived usefulness and ease of use.

Several factors describe that the organizational culture where technology is implemented plays a significant role in user adoption. While this research does not question that notion, the possible interplay between cybersecurity training and organizational culture is beyond the scope of this research. However, the guidelines *Facilitating conditions* and *Physical accessibility* suggest that providing users with resources will increase user adoption. Resources can include physical and digital resources that enable cybersecurity training. It can also include the available time that enables users to fit such training into their schedules. As such, it is suggested that users can easier adopt a technology that requires less time to use.

**Social factors**

The social factors refer to factors that relate to the user. Those are described in Table 2.

*Table 2 Social TAM factors relating to the intended user of a technology.*

<table>
<thead>
<tr>
<th>Factor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compatibility</td>
<td>A person’s intention to adopt a system is impacted by how that system corresponds to the person’s values, needs and experiences.</td>
</tr>
<tr>
<td>Self-efficacy</td>
<td>PU and PEOU will increase if people believe that they can successfully use a system.</td>
</tr>
<tr>
<td>Personal Innovativeness</td>
<td>A user’s predisposition to trying out new technology will impact IU.</td>
</tr>
<tr>
<td>Computer Playfulness</td>
<td>A predisposition to playfulness can increase PEOU.</td>
</tr>
<tr>
<td>Computer Attitude</td>
<td>A person’s attitude towards a system will influence PU and PEOU.</td>
</tr>
<tr>
<td>Computer Anxiety</td>
<td>In contrast to self-efficacy, anxiety when using a system can have a negative impact on PEOU.</td>
</tr>
</tbody>
</table>
Experience using a system can increase PU and PEOU. However, experience will affect other external factors, and the nature of that experience will determine how.

Several identified social factors show that different personality traits impact a user's decision to adopt technology. Further, the compatibility factor suggests that a user is more likely to adopt cybersecurity training if that training is perceived to meet the user's needs. It can be assumed that a user will be more likely to participate in training if the relevance of the training is obvious. Further, the self-efficacy factor suggests that a user is more likely to engage in secure behaviour if the user is comfortable with how to do that. On that note, the role of training becomes to provide the user with appropriate directions for how to behave in the desired way.

Technical factors
The technical factors refer to the technology itself. Those are described in Table 3.

Table 3 Technological TAM factors relating to the technology itself.

<table>
<thead>
<tr>
<th>Factor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voluntariness</td>
<td>A higher degree of voluntariness will have a positive effect on IU.</td>
</tr>
<tr>
<td>Relative Advantage</td>
<td>A user is more likely to adopt a system perceived as better than other systems for the same purpose.</td>
</tr>
<tr>
<td>Complexity</td>
<td>Perceived difficulty to use will have a negative effect on PU.</td>
</tr>
<tr>
<td>Trialability</td>
<td>A user can be more likely to adopt a system that can be tested before adoption.</td>
</tr>
<tr>
<td>Social Presence</td>
<td>The degree to which a system allows users to transmit social cues. Social presence is described as more important for communication systems.</td>
</tr>
<tr>
<td>Job Relevance</td>
<td>PU is increased if a system is perceived as beneficial for a person's job performance.</td>
</tr>
</tbody>
</table>
Computer Attitude | A person's attitude towards a system or computers in general will influence PU and PEOU.
---|---
Information Accessibility | How one can retrieve wanted information from a system will impact PU and PEOU.
Result demonstrability | PU increases if a user perceives that the results of using a system are easily observed and communicated.
Perceived enjoyment | If a system is perceived as enjoyable to use, the likelihood of user adoption will increase.
System Quality | The likelihood of system adoption will increase if a user perceives that the system performs tasks that match the user's goals well.

This category first suggests that voluntariness will positively influence user adoption. Similarly, the ability to test the technology before its adoption is favourable. The quality of the technology itself is crucial and described in several identified factors. The quality of a technology can be described by how well it responds to a user's needs and how well it can improve the user's task performance. Given the notion that lower complexity will further increase user adoption, it can be concluded that cybersecurity training that is perceived as low effort but provides the user with tools that increase the user's perceived task performance is good. Finally, information accessibility and result demonstrability highlight that cybersecurity training that is perceived as providing observable results and from which information can be easily understood further facilitates user adoption.

4.1.3 DERIVED PRINCIPLES FOR CYBERSECURITY TRAINING

Based on the theoretical basis for this research presented above, five principles that the development of cybersecurity training should follow were developed. The principles were derived from issues with existing methods for cybersecurity training identified in previous literature and the theoretical explanations for user adoption provided by TAM. The principles formed the starting point of the first design cycle, described in Section 4.3 DS cycle 1: Exploring the problem space, and were revisited and updated at the end of each design cycle. The principles and motivations for them are as follows:

- **Cybersecurity training should minimize the effort needed by the user to engage in such training.** The intention is to make users perceive that participation in training requires low effort. It should be interpreted as a call to minimize required time and cognitive complexity. A minimized cognitive complexity means that the users can easily understand how to partake in training.
• Cybersecurity training should be provided to users in relation to situations where it is needed. There are several reasons for this principle. First, previous research has suggested that security nudges can mediate secure behaviour and providing training in close relation to a situation where the training can be applied can be seen as a nudge. Second, providing a user with guidance on how to use a technology (in this case, interpreted as applying secure behaviour) can increase the user’s self-efficacy and reduce anxiety, thereby increasing the likelihood that the user adopts the desired behaviour. Finally, this approach can work as a motivating factor that provides favourable beliefs toward the desired behaviour.

• Cybersecurity training should be repetitive. The rationale for this principle is that repetitive training counteract previously identified problems with knowledge retention. Further, combined with principle two, it allows for integrating cybersecurity training into the user’s daily routine. With principle one, this suggests a shift towards frequent and short cybersecurity training instead of infrequent and long.

• Cybersecurity training should be relevant for the user. Several external TAM factors describe that relevance is a key mediator for user adoption in different ways. Training tailored to the user and their context can be assumed to be more desirable for the user.

• Methods for cybersecurity training should be comparatively evaluated. Several external TAM factors speak of system quality as a mediator for user adoption. A natural extension of that is that such systems should be evaluated so that the quality can be demonstrated. Such evaluation can also demonstrate expected outcomes of cybersecurity training, which meets the goal of result demonstrability. Finally, comparative evaluation ensures that the effect of one method can be compared to that of another and meets the relative advantage factor.

4.2 ESTABLISHMENT OF REQUIREMENTS FOR EVALUATION

The second objective of this research, Establish requirements for evaluation of cybersecurity training, was explored before the beginning of the first design cycle. The progress line visualizes the location of the current task in the overall research process, in Figure 11.

The purpose of this step was to articulate requirements that cybersecurity training should meet and a process for how to evaluate a method against those requirements. The requirements were inferred from the theoretical framework and related literature presented in the Section 2 BACKGROUND. The evaluation process was further informed by a structured literature review which intended to identify the methods used for evaluation in the domain and how they are used.
4.2.1 REQUIREMENTS FOR CYBERSECURITY TRAINING

The theoretical framework and related literature presented in the background sections of this thesis describe prior research in cybersecurity behaviour and the use of training to improve cybersecurity behaviour. Four requirements that cybersecurity training should meet to be successful were inferred from that body of literature. Relevant literature was identified using an SLR (Paper 8), and the requirements are:

- **Support users towards secure behaviour** is the first requirement. For cybersecurity training to be effective, users of it should exhibit a more secure behaviour than users not using the training. Behaving securely would, for instance, include avoiding phishing e-mails, selecting good passwords, adhering to security policies, etc. Improving users’ security behaviour is the primary target of any training effort and is considered the most important of the four requirements. Cybersecurity training cannot be considered effective unless the research can demonstrate that it improves user behaviour regarding cybersecurity.

- Second, cybersecurity training should **increase its users’ knowledge about cybersecurity**. While previous literature describes that providing users with knowledge is not enough, providing knowledge is still a central function of a training effort (Bada et al., 2019; Boss et al., 2015; Siponen, 2000). It is impossible to behave securely unless you know how to do so. Cybersecurity training should therefore be able to provide its users with knowledge in order to be considered effective.

- The third requirement, **be perceived as positive by its users**, is partly based on previous literature arguing for the importance of usability of security functions (Bada et al., 2019; Whitten & Tygar, 1999). It is further inferred from TA, which describes user perception as a key precursor to user adoption. User adoption is, in turn, a given requirement for cybersecurity training to provide its intended effect. As with any function, it can only provide its intended effect
if users adopt it. As such, cybersecurity training must be perceived as positive by its intended users to be considered effective.

- This research seeks to develop a method for cybersecurity training of end-users. For it to have any value, it must be possible to use, leading to the fourth goal; be feasible to implement in practice. This requirement is supported by Hevner et al. (2004), who argue that information systems artefacts should be evaluated based on their usefulness in the environment for which they are designed. As such, the fourth requirement stipulates that cybersecurity training methods must be feasible to implement in practice for the methods to be considered effective.

4.2.2 EVALUATION PROCEDURES IN THE DOMAIN

A Structured Literature Review (SLR) was used to inform this research about how cybersecurity training has been evaluated in previous research (Paper 8). The SLR identified three distinct types of evaluations (Choi & Lee, 2015; Kunz et al., 2016; Reinheimer et al., 2020; Stockhardt et al., 2016; Xiong et al., 2017):

- User perception evaluations with a focus on how potential users perceive training.
- Evaluations measuring if and how much knowledge about a topic that is transferred to potential users.
- Experimental evaluations of how a training method affects potential users’ cybersecurity behaviour. Experimental evaluations were performed using both simulated and naturalistic experiments.

User perception is not discussed in existing literature as a contributor to improved security behaviour. However, as argued by several scholars, user perception is an important factor for user adoption (Bhagavatula et al., 2015; Lee et al., 2003; Whitten & Tygar, 1999). The fact that user adoption is a precursor to whatever a security function tries to achieve is unarguable. User perception evaluations are used to evaluate users’ perception of their skill, or their perception of a training method to which they have been exposed.

Increasing knowledge is considered important and certainly a necessity for promoting secure behaviour. To act securely, a user must know what to do and how (Siponen, 2000). However, research suggests that knowledge alone does not necessarily translate to behaviour (Boss et al., 2015; Parsons, 2018; Siponen et al., 2014). It can be argued that evaluation should primarily focus on behavioural outcomes. That does, however, require experiments that can be hard and expensive to conduct, leaving room for knowledge-based evaluations as well (Vroom & Von Solms, 2004).

In addition to the identified evaluation methods, information systems literature stresses the importance of practically usable results. On this note, a method for implementing cybersecurity training must be feasible to use in practice, meaning that it must support the development of such training.
4.2.3 ESTABLISHMENT OF A PROCESS FOR EVALUATION

Based on the discussion in the section above, some conclusions about how cybersecurity training should be evaluated can be made. First, four different requirements to evaluate such training by were identified: ability to change behaviour, ability to transfer knowledge, how users perceive it, and that it can be implemented in practice. As such, evaluation studies should consider at least one of those requirements. It is, however, reasonable to conclude that a cybersecurity training effort is only fully evaluated once all four aspects have been considered. Further, each requirement can be seen as a scale where any cybersecurity training method will have a more or less favourable result. While evaluating a single method can provide important results, only comparative evaluations can reveal how different methods relate to each other. For a newly developed method to be considered a contribution, it should be proven better than existing methods. That requires comparative evaluations, and an evaluation process should be able to demonstrate if a cybersecurity training method meets the requirements. It should further demonstrate how the method compares to other existing methods.

An evaluation process was established to enable evaluation in regards to the four requirements in an arbitrary number of steps. That is argued to provide more flexibility than a process with a fixed number of steps. Further, it aligns with the design science approach used in this research, where research in one design cycle will reveal what evaluations are needed in upcoming cycles. The intention is that all evaluations relating to one requirement should together showcase that the artefact fulfils that requirement.

An example visualisation of the evaluation process is presented in Figure 12.

![Figure 12 Example visualisation of the evaluation process.](image)

The visualisation is intended to showcase the need for evaluation in relation to the four established requirements. A short description of the results can be added for each evaluation task. The visualisation provides a qualitative representation of evaluation results and activities.

The visualisation also intends to enable the demonstration of how a method for cybersecurity training meets the four requirements by using an unspecified
number of evaluation tasks. Ideally, a cybersecurity training method can be shown to outperform other methods in all four aspects. However, a method that is at least as good as other methods in three aspects but better in one is still an improvement.

In this research, initial evaluations sought to demonstrate the feasibility of a method for cybersecurity training that was "in development". Therefore, early evaluations were focused on knowledge transfer and user perception, while comparative evaluations focusing on behavioural change were in focus in later stages of the research. Implementability was demonstrated by developing tools for cybersecurity training of end-users based on the method developed in this research.

**4.3 DS CYCLE 1: EXPLORING THE PROBLEM SPACE**

The first design cycle further explored the problem space with the intent of formulating a conceptual description of a method for cybersecurity training of end-users. The conceptual description was based on the established principles and additional literature. The actions performed in the first design cycle are further described throughout this section.

**4.3.1 METHOD DEVELOPMENT**

The first step of the method development phase was to develop a conceptual method that follows the principles for cybersecurity training established in the section “Theoretical Framework”. The current step in the research process is visualised in Figure 13.

![Figure 13 Visualization of the positioning of DC1 in relation to the rest of the research.](image-url)
The method development took an iterative approach. A limited method description and implementation were created and evaluated (Paper 1) before the results were compared to further literature, and a more comprehensive conceptual description was developed. Two fundamental points were formulated to describe how cybersecurity training should be delivered:

- It should be presented to users when the user is in a situation where the training is directly relevant.
- It should require active participation from the user.

The first point is based on the principle that training should be provided to users in relation to situations where it is needed. It is based on the pedagogical theory of situated learning, as described by Herrington and Oliver (1995), which also informed the second bullet. The situated learning theory describes that a more meaningful learning process will occur if the learning occurs in an authentic situation (Brown et al., 1989), thereby meeting the principle that cybersecurity training should be relevant for the user. It also becomes repetitive since training is provided to users every time a specific situation is encountered.

Practically, the intention was to deliver training to users when they encounter a risky situation rather than provide users with training at regular intervals, on-demand or during scheduled sessions. Using this approach, users are informed on how to act in a situation they are currently experiencing. That was assumed to make the training more relevant and thereby increase the chance of the users participating. A feeling of relevance was also assumed to make the user perceive the training as more effortless. This approach also limits the problem of knowledge retention since the training is presented every time the user encounters a risky situation. The participation problem is also limited since the training seeks out the user rather than the user having to actively seek out the training. However, the training must be implemented by a service provider or the user. In the case of the service provider, someone hosting an online service could, for instance, develop training on phishing that is presented to users when they open their e-mail or even when they open an email that is classified as potentially malicious. In the case of a user-side implementation, one example could be that antivirus software could be extended to provide the user with training if it identifies different situations such as exposure to phishing, account creation pages, link clicks, etc.

In an early evaluation (Paper 1), which served the purpose of a proof-of-concept study, a simple demonstrator was developed, and 47 participants were recruited to use it. The demonstrator was designed to teach participants about online fraud and presented the participants with a conversation between a buyer and a seller on an online marketplace. They were then asked to rate the trustworthiness of the seller. They received feedback based on their ratings, indicating if their ratings were correct or not. Following the exercises, the participants were asked to rate the trustworthiness of six ads from a Swedish online auction house where three ads were fraudulent and three were legitimate. The results were compared with a control group who performed the rating without prior training and
suggested that the training had a positive effect (Paper 1). The developed method was at this point named Context-Based Micro-Training (CBMT).

The early development focused on when training should be presented to a user but not on how. How to present information was explored next. The material presented in this thesis's background and introduction sections suggests that security is seldom a user's primary goal. Further, usability (or lack thereof) is a likely explanation for why users do not adopt security measures and guidelines to a large enough extent. TAM offers a theoretical explanation and suggests that support systems for cybersecurity should minimize the users' required effort while maximizing the users' perceived benefit. As a result, CBMT was extended to describe that the format of presented information should be short and easy to absorb. That aligns with the first of the principles established in the section “Theoretical Framework”, that cybersecurity training should minimize the effort needed by the user to engage in such training. CBMT is inspired by nanolearning, where training is presented to learners in short sequences (Wang et al., 2014). As McLoughlin and Lee (2008) described, the intention is to make the provided information possible to absorb in a short amount of time. Nanolearning has been evaluated with positive results regarding learner participation and satisfaction in other contexts than security and has been argued to minimize information overload (Bruck et al., 2012).

As an end to the method development phase in the first DC, the method was expressed as four goals that training implemented according to it should aim to facilitate:

- Provide training that users want to make use of, instead of forcing users to participate in the training.
- Require no prior knowledge from the user.
- Include an awareness-increasing mechanism.
- Provide training to the user when the user is in a situation where the training is relevant.

The first two goals intend to ensure training material that users engage with voluntarily and that is presented at a level that does not require any prior knowledge. The intention is to make the material accessible and perceived as more user-friendly. The two last goals describe that training should be presented to users in a situation where the training is directly relevant. This is assumed to further the relevance of the material and thereby further the users' motivation to participate in the training. Presenting training in a relevant situation also serves as an awareness-increasing mechanism which intends to put security at the top of the users' minds when the user encounters a cybersecurity risk. This function requires a component that can detect when a user encounters a risky situation. That component can be placed at a service provider for a single service or at the user's computer and should then be able to detect different risky situations. In the first case, the user would be given training when the user is about to perform a certain action associated with a security risk, such as creating a password or opening an email with an attachment. The process, in this case, is visualised in Figure 14.
Implementing CBMT at the user-side requires that risky situations are detected, and appropriate training is delivered only then. The user should not see the evaluation process. The process is visualised in Figure 15.

4.3.2 ARTEFACT DEMONSTRATION

The demonstration phase aims to show that the artefact can be used for its intended purpose. In this research, that means demonstrating that cybersecurity training for end-users can be developed according to the method CBMT. The demonstration in this DC also enables evaluation since the demonstration took the form of developing demonstrators that were then used to evaluate the method in the evaluation phase.

Two demonstration activities took place in DC 1:

- Development of short videos describing cybersecurity concepts\(^2\) (Paper 2).
- Development of learning material for a university course in data communication\(^3\) (Paper 3).

The demonstrators were not fully functional but demonstrated how learning material could be presented. The functionality of automatically presenting material in appropriate situations was not developed in DC 1. While the demonstrators enabled evaluation and played an important role in further exploring the problem space, their value in demonstrating the ability to implement CBMT fully is limited.

\(^2\) https://www.youtube.com/channel/UC4gDh8JF8Soz7rjaK Pu0ovg
\(^3\) https://www.youtube.com/watch?v=9TDFRgh5lkk&list=PLEjQDf4Fr75qADv9JoUbNaiUmB8zMhw6V
4.3.3 EVALUATION

Two evaluation activities took place in DC 1:

- Knowledge-based evaluation where CBMT was used to develop learning material for a technical first-cycle university course in data communication. This evaluation intended to evaluate if learning material based on CBMT could be used to teach material previously taught using traditional classroom lectures. The participating students’ exam results were compared to exam results from previous students, and the students were given a survey on their perception of the training material. Twenty-eight students participated in this evaluation (Paper 3).

- Perception evaluation as a survey where participants were shown short videos about cybersecurity concepts before being asked about their perception of the training type. The participants were also asked if they preferred the CBMT training over training delivered as text, lecture, or on-demand video. One hundred ninety-eight participants completed the survey (Paper 2).

The knowledge-based evaluation took place in a university course given by the author of this thesis. It was a course in data communication that was purposefully selected because it intended to teach the students practical skills in network administration. This evaluation intended to evaluate if learning material based on CBMT could be at least as effective as traditional lectures in teaching the course material. The study was preceded by a pilot where students from a previous year were taught about a networking concept that was new to them. The reason for performing the pilot was that the usability of CBMT was unknown, and directly using it in a course without prior testing was considered unethical. If the material was proven to be sub-par, it could harm the students learning and thereby cause harm.

The evaluation of the student scores revealed that the students who used CBMT-based learning material performed at the same level as students from previous years when traditional lectures were used. In numbers, 90% of the included 28 students passed the theoretical test at the end of the course, compared to 88% the previous year (Paper 3). The evaluation was conducted using publicly accessible statistics. Given the high number of passing students, this was seen as a positive evaluation for CBMT, which was further emphasized by assessing the students’ perception of the learning material. 26 of the 28 participants reported that they preferred the CBM-based material over traditional lectures. They also reported that the material encouraged them to do practical exercises included in the learning material and that the material motivated them in their studies. This study sought to evaluate if CBMT-based material could be used to teach learners and found that it could. The students also received it positively, as shown by the survey in Paper 3.

The perception evaluation, presented in detail in Paper 2, presented the participants with three short videos covering different cybersecurity concepts. Each video included a practical aspect where the participants were asked to perform some action based on the material presented in the video. After watching the videos, the participants were presented with Likert scales that
measured their perception of the videos, CBMT in general, and asked them to compare CBMT to training delivered as text, as a lecture or in an on-demand video. The results showed that the participants were positive toward CBMT-based cybersecurity training and preferred CBMT-based training over the other training types to a large extent. It should, however, be noted that the comparative results were reached when the participants were asked about their preference just after being subjected to CBMT-based training, and the risk of bias is obvious. The results, in this regard, were interpreted as an indication rather than a highly significant result. An overview of the evaluation results in DC1 in relation to the requirements for cybersecurity training is presented in Figure 16, which also references the published papers detailing the evaluations.

Figure 16 Overview of evaluation activities in DC1.

As per the research strategy, the evaluations in this DC were published in scientific conferences to enable discussion of the work with other researchers. The content of these discussions was collected as field notes and used as input to the second DC. The discussions raised two questions that were taken as input to the research. The first question was how to implement the method in practice. While that concern was already included in the research process as a requirement, it highlighted the importance of expressing how it is intended to be implemented. The second raised question was expressed as a concern about how users would perceive it in reality. A comparison to the previous assistant in office word, Clippy, was made. It was further discussed that making the training enforcing could result in users not liking it, deterring users from using it.

4.3.4 REVISITING THE PRINCIPLES OF CYBERSECURITY TRAINING

The evaluations performed in this DC were positive towards CBMT, as described in this DC. They can be seen as confirming the principles established in Section 4.1 Theoretical framework. However, the field notes collected at discussions at scientific conferences raised two questions. The first, how to implement the methods in practice, was considered part of the methods development process and further addressed in DC2. However, the second question raised concerns about how users would perceive training presented in the users’ workflow. Consequently, the description of one principle was slightly updated, as shown in

---

4 https://en.wikipedia.org/wiki/Office_Assistant
the quote below, and the perspective adopted as important for further research. The other four principles remained unchanged.

**Cybersecurity training should be provided to users in relation to situations where it is needed.** There are several reasons for this principle. First, previous research has suggested that security nudges can mediate secure behaviour and providing training in close relation to a situation where the training can be applied can be seen as a nudge. Second, providing a user with guidance on how to use a technology (in this case, interpreted as applying secure behaviour) can increase the users’ self-efficacy and reduce anxiety, thereby increasing the likelihood that the user adopts the desired behaviour. Finally, this approach can work as a motivating factor that provides favourable beliefs toward the desired behaviour.

*However, care must be taken to ensure that the implementation of this principle is not perceived as too enforcing as that could lower usability.*

### 4.4 DS CYCLE 2: PROPOSING A SOLUTION

The second DC intended to extend the goals from DC 1 with practical guidelines for implementing cybersecurity training for end-users. The overall process was to continue the method development and then validate that it could be used to support implementation by employing an external company to develop an instantiation. The implementation was then used to further evaluate the method’s ability to improve the cybersecurity behaviour of end-users in an experiment (Paper 4). User perception was also evaluated using the same implementation (Paper 5). How this DC is positioned in the overall research process is visualized in Figure 17.

![Figure 17 Visualization of the positioning of DC2 in relation to the rest of the research.](image-url)
An additional task during this DC was to explore how password guidelines could be expressed to support the user in creating secure and easy-to-remember passwords. The outcome of this activity is documented in Paper 7, and the reasons for it were:

- Since the evaluation tasks trained users in a naturalistic environment, it was considered important to ensure that the information provided to users was empirically evaluated. Providing sub-par information would risk harming the participants, which presents an ethical obstacle.
- Literature suggests that guidelines presented to users should in themselves be usable (See Section 2 BACKGROUND). This insight is a call to research the usability of presented information.

4.4.1 METHOD DEVELOPMENT

The method development phase in the second DC extended the method based on the input from the discussions after presenting the work from DC1 at scientific conferences. At the end of DC 1, the method was the following goals that express what training according to CBMT should facilitate:

- Provide training that users want to use instead of forcing users to participate in the training.
- Require no prior knowledge from the user.
- Include an awareness-increasing mechanism.
- Provide training to the user when the user is in a situation where the training is relevant.

The conference discussions emphasized a need to express how training developed according to the method should be implemented. They further emphasized the importance of being positively perceived by users. First, the composition of the method was modified to include goals that express what training should aim to facilitate and guidelines that provide practical directions for how it should be implemented.

The literature presented in Section 2 BACKGROUND shows that security is not a top priority for most users. As such, requiring too much time from the users risks limiting user participation. The notion of minimizing the effort needed by users to partake in training is one of the principles established as part of the theoretical framework for this research. Resource use, in terms of time, was not addressed in the goals developed in the first DC. Be short and easy to absorb was added as a goal to highlight the importance of minimizing the time required by users. At the same time, the fourth guideline from DC 1 was considered to be more of a practical guideline than a goal. It was rephrased as a guideline that read Delivered to users when it is relevant to their current situation.

The next three guidelines are intended to clarify the principles underpinning CBMT: it should be related to practice, relevant to the user, and delivered in short sequences. A final guideline was added as a response to the discussion on user perception and the importance of not being to enforcing. The guideline,
therefore, highlights that a user must be able to opt-out of receiving training. The five guidelines expressed in DC 2 were:

- Delivered to users when it is relevant to their current situation.
- Delivered in short sequences.
- Relevant to the users' current situation.
- Include a practical element.
- Must be possible to opt-out.

Those goals and guidelines represented the method for cybersecurity training of end-users and were used in the artefact demonstration step discussed next.

4.4.2 ARTEFACT DEMONSTRATION

The artefact demonstration phase in this DC served two purposes. First, it demonstrated the possibility of implementing cybersecurity training for end-user following the method central to the research, CBMT. Second, it enabled evaluation.

The artefact demonstration was carried out by contracting a software development company to develop a tool for cybersecurity training of end-users. The tool was developed as a script that can be implemented by the owner of a web page and holds the following capabilities:

- It follows the goals and guidelines specified by CBMT.
- It should be possible to implement on a web page with minimal effort.
- It should be able to detect when a user is about to create a password on that web page.

As previously described, CBMT can be implemented by a service provider or user-side. This step demonstrates a service provider implementation where the service provider assumes the responsibility for implementing the training. The benefit is that the training will be provided to the user without needing action from the user or an organization managing the users' devices. The drawback is that users will not be provided with training unless they use a service that offers it. One can argue that risky situations are more likely to occur when using services delivered by providers less concerned with security, which contradicts service provider implementations. Nevertheless, it can also be argued that the ease they offer users makes them worthwhile. Furthermore, the skills a user gains from training from a security-aware provider are surely beneficial when using other providers.

The selected context for the implementation was password guidelines, and there were two reasons for selecting that context. First, passwords and password management remains one of the main challenges within human aspects of cybersecurity. Poor password quality, password reuse and so on are common causes of incidents. Second, passwords can be used to quantify behaviour with relative ease. Examining the quality of created passwords allows for collecting
empirical data that can be used to evaluate the effect of a measure, in this case, the provided training.

The implementation was developed by the company Xenolith AB\(^5\). The component that evaluated when the user needed training was designed to activate when a user visited a sub-page containing an account registration form. It detects such a form by looking for multiple occurrences of fields for typing passwords since that is the typical layout of an account registration form. Then, when a user clicks or tabs into the password field, training is provided. The resulting training is showcased in Figure 18.

The training is a dialogue that first describes the essential password creation tips in three sentences. The user can then choose to continue to get deeper information. The user is then invited to take a short quiz on the presented information. The dialogue ends with a box where the user can create a password accompanied by a strength meter.

The password guidelines presented to the users emphasized long and easy-to-remember passwords. The concrete tip provided to the users was to use a password that included four words and did not include personal information, names or social security numbers. This tip was based on research activities which suggested that those guidelines would result in users selecting stronger passwords as compared to guidelines emphasizing password complexity (Paper 7).

\(^5\) https://www.xenolith.se/
Figure 18 Implementation of CBMT in DC2.
4.4.3 EVALUATION

The evaluation activities in DC2 were performed to evaluate if CBMT could meet all the four requirements previously established, namely:

- It must support users towards secure behaviour.
- It must increase its users’ knowledge about cybersecurity.
- It must be perceived as positive by its users.
- It must be feasible to implement in practice.

The artefact demonstration presented above shows that a working implementation of CBMT can be developed in four months with a budget of under 12 300 euros. Provided that the implementation provides its intended effect, that is argued to demonstrate that the method is feasible to implement in practice. Two further evaluations took place in DC2 to evaluate how well the implementation met the other requirements:

- The effect on password behaviour was evaluated by implementing the implementation on the website of a local Internet Service Provider (ISP). The service provider measured the strength of newly created passwords, and anonymous metrics were shared with the research team. This evaluation included 303 participants, and is appended to the thesis as Paper 4.
- The second evaluation, Paper 5, evaluated user perception of the implementation by letting two experts in User Experience Design (UXD) perform a usability analysis of the implementation. The usability analysis was performed without influence from the author of this thesis, and their report was used as qualitative data to evaluate the CBMT method.

The effect on actual behaviour was evaluated in a naturalistic experiment where the implementation was provided to 124 users who were about to register an account on the web page of a local ISP. 50% of the users who registered an account during the data collection period received training, while the other 50% did not and acted as a control group. Two metrics assessed the strength of the created passwords:

- Length in characters.
- A strength score was computed using the algorithm zxcvbn (Wheeler, 2016).

It should be duly noted that the ISP calculated the metrics immediately before the password was stored securely. The only data shared with the researchers was the password metrics and what group (control or experiment) the metrics belonged to.

The collected data revealed that users subjected to the training created longer and stronger passwords than users who were not. The median length of passwords was 11 in the group who received CBMT training and 9.5 in the control group. The median strength score was 3 (out of 4) in the CBMT group and 2 in

6 https://studentnatet.se/
the control group. The between-group differences were statistically significant (Paper 4). Thus, the experiment shows that CBMT can positively affect security behaviour and is a positive evaluation for CBMT in terms of requirement 1.

The survey-based evaluation, also presented in Paper 4, included 179 participants and was done as a follow-up to the experiment intended to assess how much of the provided information users noticed. The survey was not anonymized. Instead, participants were invited to a survey about their security behaviour and told that they should register with an e-mail address and create a password. They were informed that they would get personalised feedback with their results compared to the results of the other survey participants. The general survey was only there to give the participants what they were promised. The true purpose of the survey was to measure how much of the password guidelines presented to the participants during registration they actually noticed.

Three different registration pages were created, with three different ways of presenting password guidelines. In addition to presenting guidelines using the developed implementation, the other ways of presenting the same information were with a text-box and a link to a text-box. The participants then received five questions about the just-presented information, a free-text field where they were asked to provide their opinion on the format in which they received information and a survey with general questions about security behaviour. The survey ended with a de-briefing page where the study's intent was explained, and the participants were provided with information on how to get their individual feedback. Note that no passwords were stored or assessed during this part of the study. This evaluation showed that users presented with password guidelines using CBMT noticed the information to a higher degree than users who were presented with the same information in plain text or with a link to plain text. Therefore, it is a positive evaluation of CBMT in terms of requirement two. The free-text field answers from several of the participants in the CBMT group revealed that they took note of the presented information but opted not to follow it. Their motivation was that they used some other method to create their passwords. None of these respondents expressed any negative perception of the training, but several were positive, even if it didn’t change their behaviour (Paper 4). While this data set is too small to draw any certain conclusions, it suggests that CBMT can be accepted by users even if they are already familiar with the presented information.

The second evaluation, presented in Paper 5, took the form of a usability analysis performed by two UXD experts, independently from the author of this thesis. The analysis focused on the developed implementation and was carried out as an expert analysis complemented by a one-participant usability test. It was completed in the spring of 2020, and the ongoing Covid pandemic prohibited usability tests with more participants. The expert analysis followed the procedure outlined by Wilson (2013) and resulted in a report with factors that hindered or enabled usability. The results were then compared to the CBMT goals and guidelines. The evaluation suggested that CBMT could indeed be used to develop cybersecurity training that can be positively received by end-users and serves as a positive evaluation of CBMT in regards to requirement 3. The evaluation also identified 22 factors that could hinder usability. A vast majority
of those spoke to the implementation itself rather than the CBMT method since they identified spelling errors, design problems etc. However, the evaluation also highlighted that the user could be caught by surprise by inputting training into the users' workflow. This can be seen as intrusive and can hinder usability. This insight was brought to the development phase of DC3.

An overview of the evaluation activities in this DC and how they respond to the established requirements for cybersecurity training is shown in Figure 19. Figure 19 also shows previous evaluation activities, and references published papers detailing the evaluations.

![Figure 19 Overview of evaluation activities up until DC2.](image)

The evaluations were published in scientific conferences to enable input from the scientific community. Discussions following such presentations were documented as field notes and used as input to the research. Because of the Covid pandemic that was ongoing at the time, the conferences were held online, making discussions harder. Still, the intrusive nature of CBMT was further discussed. The summary of the discussions was that the awareness-increasing mechanism is important for security and does imply an element of interruption. Further, the interruption cannot be seen as enforcing because that will have too much of a negative effect on usability.

**4.4.4 REVISITING THE PRINCIPLES OF CYBERSECURITY TRAINING**

Following the evaluation part of DC2, the principles for cybersecurity training were revisited. The intrusive nature of CBMT was a recurring theme during DC2 and was discussed during the evaluation activities and subsequent presentations at scientific conferences. Evaluation results and field notes from discussions at
scientific conferences describe that interrupting the user’s workflow, which is a core functionality of CBMT, can hinder usability. At the same time, data collected also supports that interrupting a user’s workflow to provide security-related information can positively influence security behaviour. Further, evaluations have not found that included participants perceive the interrupting function as a problem - that possible problem is rather derived from feedback from the scientific community. It appears that some degree of interruption can be accepted by users as long as the benefit of that interruption is high enough. That falls well in line with how TAM describes user adoption as a function of perceived ease of use and usefulness. This discussion was raised in DC1 with a subsequent update to the principle stating that Cybersecurity training should be provided to users in relation to situations where it is needed. The research in this DC confirms the update from DC1, outlined in Section 4.3.4 Revisiting the principles of cybersecurity training.

A second theoretical aspect, highlighted by the activities in DC2, was that the effectiveness of cybersecurity training is impacted by the information presented to users and how that information is presented. In essence, the research around password guidelines suggests that users are more prone to adopt a suggested behaviour if that behaviour is in itself perceived as easy. That relates to the principle Cybersecurity training should minimize the effort needed by the user to engage in such training. It considers the effort needed to engage with cybersecurity training, but the importance of the presented material is not clearly described. The description of this principle was updated to reflect the importance of considering the usability of the information presented by security training, as shown in the quote below, with the addition marked italic. The importance of the presented material was further researched in the upcoming DC.

**Cybersecurity training should minimize the effort needed by the user to engage in such training.** The intention is to make users perceive that participation in training requires low effort. It should be interpreted as a call to minimize required time and cognitive complexity. A minimized cognitive complexity means that the users can easily understand how to partake in training. Further, cybersecurity training will be more effective if the material presented to a user is perceived as easy to use. As one example, a user is more likely to adopt a password guideline emphasizing long passwords based on words than password guidelines suggesting passwords based on long and complex random strings.

### 4.5 DS CYCLE 3: CONTEXT-BASED MICRO-TRAINING

While a method was proposed and evaluated with positive results in DC2, the evaluation also identified an area that requires further research: the degree to which the user's workflow is interrupted by the training. The interrupting function is a core component of CBMT and provides an awareness-increasing mechanism. Nevertheless, users may refrain from using the training completely.
if it poses a serious usability problem. The first goal of DC3 was to address this concern further and refine the method in general. The second goal of DC3 was to further the evaluation of CBMT using more rigorous studies than in DC1 and DC2. DC1 provided initial positive evaluations, and DC2 provided additional positive evaluations, even on user behaviour. Several of those evaluations were also comparative and showed that CBMT performed better than other options for cybersecurity training. However, some gaps still need to be filled:

- There are two modes in which CBMT can be implemented; service provider level or user level. Only the service provider level has so far been demonstrated and evaluated. Demonstrating and evaluating a user-level implementation is needed to evaluate the CBMT method fully.
- The evaluations have so far, mostly, focused on Swedish users. Evaluating CBMT in a larger context is needed to show that the results in this research are transferable to other populations.
- The evaluation regarding security behaviour only focused on password guidelines, which is one single risky situation. Phishing is another risky situation that has been discussed in a large number of previous studies on security behaviour. Evaluating the effect of CBMT in a phishing context is thereby relevant and adds comparability with previous work.

In addition to refining the method, DC3 seeks to fill the three described gaps. An additional task in DC3 was to research usability in the cybersecurity domain in general to identify the usability aspects that are most important for users. There were two reasons for this task. First, it enables the results gathered in this research to be discussed outside of the cybersecurity training domain. Second, it provided valuable input to the artefact demonstration step in the third DC, where the implementation is supposed to be installed by end-users. The current step of the research process is visualized in Figure 20.

![Figure 20 Visualization of the positioning of DC3 in relation to the rest of the research.](image-url)
4.5.1 METHOD DEVELOPMENT

The method development phase, which is described in Paper 6, refined the method based on three sources of input:

- Output from the evaluations in DC2 and field notes from conference discussions where the evaluations were presented.
- Insights gained from the demonstration and evaluation phases in DC2.
- Field notes from discussions at a poster session at SWITS, a collaboration group for Swedish researchers within cybersecurity. This poster session was attended to gather additional feedback from the research community.

The main contribution to method development from the evaluations performed in DC2 was that the training delivered according to CBMT should not be too intrusive. Yet, the intrusive nature of the training is important since it works as an awareness-increasing mechanism. While this factor has been continuously present during the research, it is noticeable that no empirical data has suggested that the presented training has been too intrusive. Further, the value of the awareness-increasing mechanism is well supported by previous research and emphasized by CBMT’s demonstrated ability to improve cybersecurity behaviour in the password context (Paper 4). However, while it is clear that the mechanism should remain, the evaluations suggest that it must be implemented with care to minimize any possible annoyance. A further result from the survey-based part of Paper 4 was that while participants using CBMT noticed the presented information to a higher degree than participants in the other groups, most users did not notice all the presented information. That was interpreted as most participants not spending that much time on the training and that they only noticed the information that stood out. Consequently, it is beneficial to highlight the most important information so that the user’s attention is put to the most crucial points presented.

During the development phase in DC2, it was noticed that the guideline *Delivered to users when it is relevant to their current situation* could be interpreted as a hard requirement only to provide training in naturally occurring situations. Following that interpretation, CBMT would not be possible to use in training exercises, simulated situations or education since those all include constructed situations. While the awareness-increasing nature of CBMT provides the most effect in naturally occurring situations, CBMT is intended for use even in constructed situations, as demonstrated in the evaluation phase of DC1. The contextual nature of the provided training is argued to make the training more meaningful even in constructed situations.

The development phase in DC2 further suggested that the guideline *include a practical element* was cumbersome. A strict interpretation would be that the presented training needs to provide a practical element. While that can be the case, the main idea of CBMT is rather that it should precede a practical element that is naturally occurring. In the case of password guidelines, the training is provided, but the user is then left to continue with the password creation after the training. The practical element is, in this case, the creation of the new password, and that does not have to be contained within the training.
CBMT was also presented at a poster session at the 19th Seminar of the Swedish IT Security Network (SWITS) to stimulate discussions (Kävrestad, 2019). Several seminar participants were positive about the CBMT method, and the discussion revolved around the nature of the material presented to users. CBMT does not intend to specify in what format information is presented, but the discussion suggested a need to highlight that the information is easy for users to follow. That is in line with the expressed goal stating that cybersecurity training should require no prior knowledge from the user but adding a guideline pointing in the same direction was argued to emphasize the need to carefully develop the material so that it is easy for users to comply with. This aspect was further emphasized by the research around password guidelines conducted in DC2. On this topic, it was made evident that a central reason why users do not comply with password creation guidelines is that they are too complex.

The CBMT method was updated according to the insights presented above. One goal and two guidelines were added, and two guidelines were modified. The resulting goals and guidelines are presented below (modifications in DC3 are written in italic). The goals and guidelines make the method for cybersecurity training of end-users developed in this research. The CBMT method was published at a scientific conference in the state presented in this section (Paper 6). Following the presentation of the method, the remainder of this section will discuss it in more detail.

**Goals:**
- Provide training that users want to make use of, instead of forcing users to participate in the training.
- Include an awareness-increasing mechanism.
- Require no prior knowledge from the user.
- Be short and easy to absorb.
- Should minimize annoyance for all users, especially users already familiar with the subject.

**Guidelines:**
- Delivered to users when it is relevant to their current situation. The situation can be constructed or natural.
- Delivered in short sequences.
- Relevant to the users' current situation.
- Include or directly relate to a practical element.
- The information presented must in itself be easy to understand.
- The most crucial points of the information should be highlighted.
- Must be possible to opt-out or skip.

The processes required by a tool designed to provide cybersecurity training to end-users according to the CBMT method are visualized in Figure 21. When a user enters a situation, the tool should evaluate if that situation is risky or not. If
the situation is risky, the tool needs to evaluate what type of situation it is. In practice, those processes can be one and the same. For instance, a function that identifies a password creation field will identify the risky situation while identifying the situation type. Once the situation type has been determined, the tool should make the user aware of the situation and suggest training. Should the user want training, training is presented in a concise and accessible manner.

Figure 21 Model describing the CBMT method.

If CBMT is used in a constructed environment, for instance, as part of a training exercise, the responsibility of identifying a situation is removed. The process then presents the user with information when they start a task and lets the user continue with the task afterwards. Used in this way, the goals and guidelines of CBMT can be followed in several situations. One example could be in a gamified environment where a user explores cybersecurity in a game where s/he is tasked with handling different cybersecurity situations. When such a situation is encountered, the option of having training can be presented to the user, and the content can be aligned with CBMT.

Further, as shown in DC1, CBMT can be used to develop learning material for practical curriculum delivered to students. In such a case, a student would be tasked with a practical assignment and provided with learning material before starting it. If a more complex assignment is to be completed, several CBMT-based modules should be developed so that each module includes a short sequence of information. The processes become simplified, as demonstrated in Figure 22.

Figure 22 Model describing the CBMT method in a constructed situation.

4.5.2 ARTEFACT DEMONSTRATION

The artefact demonstration phase serves two purposes in this DC. First, it enables experimental evaluation of the effect that CBMT can have on cybersecurity behaviour. Second, it demonstrates that CBMT is feasible to implement in practice. A software development company again completed the
artefact demonstration in a joint project. Since the implementation in DC2 was implemented to be provided by the service provider, this demonstration was developed to demonstrate CBMT-based training implemented as a tool at the user's computer.

The tool was developed as a web browser plug-in with the following capabilities:

- It follows the goals and guidelines specified by CBMT.
- It should be a tool that users install in their web browser.
- It should detect when a user is about to create a password or is in a situation with an elevated risk of exposure to fraud, phishing or fake news.
- Once such a situation is detected, it should provide the user with training relevant to the particular situation.

To support the development in this phase, additional research into the usability of cybersecurity functions designed to be used by end-users was conducted. The rationale was that providing users with a tool they are expected to run on their own device calls for further understanding of how they perceive the provided training and cybersecurity tools in general. Tasks related to installation and possible maintenance of the tool should be considered and be positively received by the users. This research was carried out as a survey with over 1400 respondents to identify which usability aspects were most important for users (Paper 11). Thus, the result could guide the implementation so that efforts were put into the most important areas.

The tool was designed to be installed as a plug-in for a web browser and does not require any user configuration to work. It is activated at different events that signify an elevated risk of exposure to fraud, phishing or fake news and when a user is about to create a password. The risks were selected because they are frequently faced by users in their daily use of digital devices. The tool is published and free to use under the name WebSec Coach and is available for Firefox and Google Chrome. The remainder of this section will exemplify how the tool works for the phishing situation. It works similarly in the other situations.

The phishing module is activated when a user opens an inbox and is displayed as a tooltip in the upper right corner of the screen. This is demonstrated in Figure 23. The user can still control the inbox and allow the tooltip to remain. The other options are to close the tooltip or click a link for more information. Choosing to receive more information takes the user to a guide with six text-based slides that provide the user with additional information and tips on how to detect phishing. The training slides are developed following guidelines for accessible web content\(^7\) and include a text-to-speech function. One slide from the training is displayed in Figure 24.

\(^7\) https://www.w3.org/TR/WCAG21/
Figure 23 WebSec Assistant in the phishing context.

Figure 24 WebSec Assistant phishing training.
The tool will also warn the user if the user is about to enter a web page known for use in phishing. The intention is to provide the user with an additional warning if the user is about to visit a known malicious website. This warning is deliberately designed to be more verbose than the tooltip. It is displayed in Figure 25.

![Figure 25 WebSec Coach phishing warning.](image)

The user can click advanced and select to proceed to the website. The user can also add an exception for the particular website. This functionality increases awareness by forcing users to confirm visits to potentially harmful websites, as demonstrated in Figure 26.

![Figure 26 WebSec Coach phishing warning with the option to proceed.](image)
The functionality for fake news, online fraud and passwords are similar to the functionality for phishing. The tool was developed in a project funded by The Swedish Post and Telecom Authority.

4.5.3 EVALUATION

The evaluations in DC3 were performed to evaluate CBMT in regards to all four requirements established for cybersecurity training, namely:

- It must support users towards secure behaviour.
- It must increase its users' knowledge about cybersecurity.
- It must be perceived as positive by its users.
- It must be feasible to implement in practice.

All criteria were evaluated with positive results in DC2, focusing on one cybersecurity risk (passwords) and a limited population (Swedish users). The evaluations in this DC seek to further the generalizability of the results produced in this thesis as follows:

- User perception of CBMT was comparatively evaluated in two steps. First, a survey was used to identify user preferences concerning cybersecurity training. Then, existing cybersecurity training methods were identified using an SLR. Lastly, the steps were combined by analyzing all identified methods with regard to user preferences. The results outline how different cybersecurity training methods respond to user preferences. The survey included participants from Sweden, Italy and the UK. Thus, the survey evaluates user perception of CBMT comparatively and adds to the generalizability of the results (Paper 10).

- The second evaluation, presented in Paper 9, was a simulated experiment where participants were split into three groups. One group was a control group, and the other groups were subjected to training on phishing detection in two different ways: using the implementation developed and playing a game. They were then provided with an inbox that contained legitimate and fraudulent e-mails and asked to delete all fraudulent e-mails. During the experiment, an eye tracker was used to track where on the screen they were looking, and they were asked to "think aloud". That allowed the researcher to record how they made decisions about the e-mails.

The artefact demonstration presented above shows that a working implementation of CBMT can be developed in 18 months with a budget of 95 000 euros. While the needed budget for an implementation project depends on several factors, the figures are reported here to showcase an example. Provided that the implementation provides its intended effect, it is argued to demonstrate that the method is indeed feasible to implement in practice.

User perception evaluation

The user perception evaluation, presented in detail in Paper 10, in this step was survey-based to allow for the generation of a large sample. The survey intended to generate a main sample of Swedish respondents for comparability with
evaluations from DC1 and DC2 and smaller samples from Italy and the UK. The rationale was that by comparing the results to nations relatively close to Sweden, the possibility of generalising the results within Europe would be measured. Further generalisation of the results was left for future work. The participants were recruited using a web panel where the number of participants could be pre-decided. It was decided to aim for 800 respondents from Sweden and 300 each from Italy and the UK. A stratified sampling approach was used where the population within each nation was divided into subgroups based on gender, age, and geographical region. Equal proportions of each subgroup were recruited for the survey using simple random sampling. The web panel provider Webropol carried out the practical sampling.

The survey asked the participants about their preferences on various aspects of cybersecurity training without subjecting them to any such training. The rationale was to let the results describe how participants prefer to participate in cybersecurity training without risking bias by introducing them to a specific method. The survey results were related to existing cybersecurity training methods identified using an SLR. The evaluation showed that contextual training, such as CBMT, is the training method with the highest potential to be positively received by users.

The survey results showed that participants in all answer groups positively perceived CBMT even if the results differed between the different nations (Paper 10). It could be identified that Swedish and British respondents were equally positive while respondents from Italy, while positive, were less positive. The analysis further concluded that none of the demographic factors gender, age, or IT competence impacted the participants’ perception of CBMT. This evaluation concluded that the perception of CBMT was positive in Sweden, Italy and the UK regardless of the respondents’ age, gender och IT competence. As such, it serves the purpose of showing that CBMT meets requirement 3. It further suggests that the results are general over different European nations and demographic groups.

Experimental evaluation
The experimental evaluation, fully described in Paper 9, took place in a simulated environment where 41 participants were subjected to training using CBMT or asked to play a game. Participants who agreed to participate in the study received information about the study, including how their data would be handled when their participation was discussed. All participants signed a written informed consent form prior to the experiment. Participants in the CBMT group received the training during the experiment to mimic the natural behaviour of CBMT. Participants in the game group were asked to play a game before arriving for the experiment to mimic the behaviour of gamified training delivered on-demand. They were then asked to assume a persona and delete phishing emails in an inbox belonging to that persona. The experiment also included a control group that did not receive any training before the task. Two sets of variables were collected. First, the participants’ behaviour was monitored using an eye tracker. That allowed for the collection of variables that reflected how well the participants adopted the behaviour suggested by the training; examining links, sender addresses, attached files and language used in the e-mails. Second, a score was calculated based on the participants’ performance and reflected the number of emails the participants correctly identified as phishing or legitimate.
The collected data show that participants who received training using CBMT scored higher than participants in the control group or who played a game. The data also showed that some of the participants in the game group neglected to play the game. That highlights the difficulty of getting users to participate in training that requires active participation. When comparing the complete game and control groups, no meaningful difference could be found between those in terms of behaviour. However, disregarding those in the game group who did not play the game showed that the game had a positive effect on behaviour, albeit a lower effect than CBMT. As for the score variable, participants in the CBMT group had higher scores than participants in the other two groups. No difference between the control group and participants that played the game could be observed. This evaluation shows that CBMT can positively influence cybersecurity behaviour – and to a greater extent than gamified training delivered to users on-demand (Paper 9).

A second interesting observation from this experiment was that while the experiment showcased positive effects of training, few participants accurately identified all included phishing emails. Considering the experimental setup, where participants were encouraged to participate in training and then asked to identify phishing, it can be assumed that the participants’ awareness of phishing was high. Still, only 7.7% of the participants correctly identified all emails correctly. Only participants in the CBMT group identified all emails correctly and made up 21.4% of the CBMT group. Further, 38.5% of the participants examined both links, sender addresses and attached files throughout the experiment. The proportions in the different groups were 9.1% in the control group, 57.1% in the CBMT group, and 42.9% in the game group. Those numbers further the notion that training is effective but question if training alone is enough. On the contrary, the collected data show that most of the participants failed with at least one email, even when their awareness can be assumed to be high. That shows that identifying phishing emails accurately is difficult and suggests that, while training is important, other defence mechanisms should also be considered.

To summarize the evaluation activities in DC3, a tool was developed based on CBMT and showcased the implementability of the CBMT method. A large scale survey shows that CBMT can be positively received by users in Sweden, Italy and the UK (Paper 10). An experiment shows that CBMT can improve cybersecurity behaviour and do so better than gamified training delivered on-demand (paper 9). An overview of the evaluation activities in this DC and how they respond to the established requirements for cybersecurity training is shown in Figure 27. Figure 27 also shows previous evaluation activities, and references published papers detailing the evaluations.
CHAPTER 4 IMPLEMENTATION AND RESULTS

At this point, CBMT has been comparatively evaluated with positive results regarding three of the four established requirements:

- It must support users towards secure behaviour (Paper 9).
- It must increase its users' knowledge about cybersecurity (Papers 3 and 4).
- It must be perceived as positive by its users (Paper 2, 3, and 10).

The fourth requirement, it must be feasible to implement in practice, has not been evaluated comparatively. Such evaluation would require implementations of several cybersecurity training methods and has not been feasible during this research. However, two implementations have been built during the research, which is argued to demonstrate that CBMT is feasible to implement in practice.

4.5.4 REVISITING THE PRINCIPLES OF CYBERSECURITY TRAINING

Following the evaluation phase in DC3, the principles for cybersecurity training was revisited. The principles were derived from previous research on cybersecurity training methods and the Technology Acceptance Model before the first design cycle. They have since been revisited and updated following the activities in DC1 and DC2. No further modifications were made following DC3. At the end of this research, the principles are expressed as follows:
• **Cybersecurity training should minimize the effort needed by the user to engage in such training.** The intention is to make users perceive that participation in training requires low effort. It should be interpreted as a call to minimize required time and cognitive complexity. A minimized cognitive complexity means that the users can easily understand how to partake in training. Further, cybersecurity training will be more effective if the material presented to a user is perceived as easy to use. As one example, a user is more likely to adopt a password guideline emphasizing long passwords based on words than password guidelines suggesting passwords based on long and complex random strings.

• **Cybersecurity training should be provided to users in relation to situations where it is needed.** There are several reasons for this principle. First, previous research has suggested that security nudges can mediate secure behaviour and providing training in close relation to a situation where the training can be applied can be seen as a nudge. Second, providing a user with guidance on how to use a technology (in this case, interpreted as applying secure behaviour) can increase the user’s self-efficacy and reduce anxiety, thereby increasing the likelihood that the user adopts the desired behaviour. Finally, this approach can work as a motivating factor that provides favourable beliefs toward the desired behaviour. However, care must be taken to ensure that the implementation of this principle is not perceived as too enforcing as that could lower usability.

• **Cybersecurity training should be repetitive.** The rationale for this principle is that repetitive training counteract previously identified problems with knowledge retention. Further, combined with the principle above, it allows for the integration of cybersecurity training into the users’ daily routine.

• **Cybersecurity training should be relevant for the user.** Several external TAM factors describe that relevance is a key mediator for user adoption in different ways. Training tailored to the user and their context can be assumed to be more desirable for the user.

• **Methods for cybersecurity training should be comparatively evaluated.** Several external TAM factors speak of system quality as a mediator for user adoption. A natural extension of that is that such systems should be evaluated so that the quality can be demonstrated. Such evaluation can also enable the demonstration of expected outcomes of cybersecurity training, which meets the goal of result demonstrability. Finally, comparative evaluation ensures that the effect of one method can be compared to that of another and meets the relative advantage factor.

### 4.6 CONTEXT-BASED MICRO-TRAINING - A SUMMARY

Context-Based Micro-Training (CBMT) is a method for cybersecurity training of end-users and the core result of this research. This section is intended to describe CBMT and can be read separately from the rest of the thesis. It also serves the purpose of demonstrating the CBMT method in full.

CBMT outlines how effective end-user cybersecurity training should be implemented by providing goals and guidelines for such implementation. The
goals describe *what* cybersecurity training of end-users should aim to achieve, while the guidelines express *how*. The goals and guidelines are as follows:

**Goals:**
- Provide training that users want to make use of, instead of forcing users to participate in the training.
- Include an awareness-increasing mechanism.
- Require no prior knowledge from the user.
- Be short and easy to absorb.
- Should minimize annoyance for all users, especially users already familiar with the subject.

**Guidelines:**
- Delivered to users when it is relevant to their current situation. The situation can be constructed or natural.
- Delivered in short sequences.
- Relevant to the users’ current situation.
- Include or directly relate to a practical element.
- The information presented must in itself be easy to understand.
- The most crucial points of the information should be highlighted.
- Must be possible to opt-out or skip.

CBMT is based on previous research on cybersecurity training and the Technology Acceptance Model. It is also influenced by situated learning which describes that learning is more meaningful if it occurs in an authentic situation (Brown et al., 1989; Herrington & Oliver, 1995). Providing a meaningful learning experience is crucial, especially for adult learners (Knowles, 1984). It does so by presenting training to a user when they are in a situation where the training is directly relevant. That approach intends to make the training more meaningful. It also makes the training re-occurring by nature and provides an awareness-increasing mechanism. By providing users with training in a risky situation, the user is made more aware of that risk.

Figure 28 outlines the processes that a tool designed according to CBMT should include. When a user enters a situation, the tool should evaluate if that situation is risky or not. If the situation is risky, the tool needs to evaluate what type of situation it is. CBMT does not specify how the evaluation should happen, but examples of possible evaluation techniques include pattern matching and content analysis. Pattern matching could detect when a user is opening a suspicious email, and content analysis could detect when a user visits an account registration form.

In practice, the two evaluation processes can be one and the same. For instance, a function that identifies a password creation field will identify the risky situation while identifying the situation type. Once the situation type has been
determined, the tool should make the user aware of the situation and suggest training. Should the user want training, training is presented in a short and accessible manner.

![Diagram](image)

**Figure 28 Model describing the CBMT method.**

CBMT can also be used in a constructed environment, for instance, as part of a training exercise. The process then becomes to present the user with information when they start a task and then let the user continue with the task afterwards. Used in this way, the goals and guidelines of CBMT can be followed in several situations. One example could be in a gamified environment where a user explores cybersecurity and is tasked with handling different cybersecurity situations. When such a situation is encountered, the option of having training can be presented to the user, and the content can be aligned with CBMT.

Further, CBMT can be used to develop learning material for practical curriculum delivered to students. In such a case, a student would be tasked with a practical assignment and provided with learning material before starting it. If a more complex assignment is to be completed, several CBMT-based modules should be developed so that each module includes a short sequence of information. The processes become simplified, as demonstrated in Figure 29

![Diagram](image)

**Figure 29 Model describing the CBMT method in a constructed situation.**

In addition, CBMT can be implemented as part of a single service or as a tool installed on the user’s device. A single service implementation is implemented by a service provider and provides users of their service with training. Examples of such implementations are providing password guidelines using CBMT on an account registration page or training on phishing when a user opens a mailbox containing e-mails flagged as possible phishing. The benefit of implementing CBMT for a service is that no tool needs to be installed on the users’ computers. Rather, training will be provided to all service users. Not requiring the user to
install is likely to lead to a higher degree of user adoption. The downside is that training will naturally only appear in services where it has been implemented. It is not likely that it will be implemented at sites less concerned about security or even fraud.

CBMT can be implemented as a tool on the user's computer to overcome that problem. While that requires that the tool is installed by the user, or an organization maintaining the user's computer, it ensures that training is delivered regardless of what service providers the user uses.
DISCUSSION
CHAPTER 5
5 DISCUSSION

This section will, in turn, describe the main results of this research and how they relate to previous literature. The chapter ends with a reflection on the papers supporting this thesis. The outline of the chapter is shown in Figure 30.

Figure 30 Outline of the discussion chapter.
5.1 MAIN RESULTS
The central result of this research is the method for cybersecurity training of end-users named Context-Based Micro-Training (CBMT). The development of CBMT has been guided by and supported by several studies that provide additional theoretical insight at a more detailed level. CBMT is based on principles for cybersecurity training derived from previous research and the Technology Acceptance Model (TAM). Those principles and the evaluation requirements used in this research make further research results. While the results of this research have been described in the publications supporting this thesis, the main results are outlined in this section and related to relevant theories and literature.

5.1.1 CONTEXT-BASED MICRO-TRAINING
CBMT makes the core result of this research and describes how cybersecurity training for end-users can be implemented. The core points of CBMT can be described as follows:

- Training should be presented to users when they are in a risky situation. The training thereby includes an awareness-increasing mechanism that supports secure behaviour.
- The material should be presented in short sequences and be easy to absorb. That ensures that the user is not required to spend a lot of time and energy on the provided training and intends to improve user participation rates.
- The presented material should preferably reflect guidelines developed with usability in mind. Guidelines that are easy to follow are more likely to be adopted by users.

CBMT is based on previous research and has been developed and evaluated in three increasingly complex design cycles. It is described in Section 4.6 Context-Based Micro-Training - a summary.

5.1.2 PRINCIPLES UNDERPINNING CBMT
CBMT has been developed based on five principles for cybersecurity training. The principles were derived from previous research on cybersecurity training and the Technology Acceptance Model (TAM). The principles have then been discussed and revised throughout the research process and make a theoretical contribution that outlines how end-user cybersecurity training should be developed. The principles are described in full in the Section 4.5.4 Revisiting the principles of cybersecurity training. The three leading keywords for the principles are usability, usefulness and relevance. This research argues that usability is crucial for user adoption of both cybersecurity training and secure behaviour. Usefulness and relevance are important precursors for users' perception of usability.

Indeed, usability became a large part of the research at several levels. First, usability concerning how training is delivered was integral to the method development from the beginning. Second, the presented material's usability
became an important component of the research. Several parts of the research suggest that users are interested in being secure, but they prefer to spend as little time and effort as possible on security (Paper 11). Consequently, training interventions should present the most important information to users in an easy-to-digest format. Further, the material presented must in itself be easy to follow. To support that claim, research into usable password guidelines was performed (Paper 7).

This research found strong evidence that usability is a key factor in why users do not follow traditional password creation guidelines emphasising password complexity, unique passwords for different accounts, and regular password changes. The research further questioned the need for complexity requirements and attempted to find a way to design password guidelines that combined computational security with usability. The result, presented in Paper 7, was that passwords of at least four words would support both memorability and computational security.

Lack of, or perceived lack of usability, has been found to prohibit user adoption in several other contexts, including e-mail encryption and multi-factor authentication (Bhagavatula et al., 2015; Reynolds et al., 2018; Whitten & Tygar, 1999). While training intends to support users using such features, this research argues that training alone is insufficient. While training can teach users about security practices, the practices must be perceived as easy enough to use, or the risk that users will simply neglect them is great.

Repetition and interruption are also important concepts covered by the principles. Repetition suggests that cybersecurity training should be repetitive, and the intent is to counteract the knowledge retention problem identified in previous research. Interruption suggests that cybersecurity training should be inserted into the user's workflow when the user encounters a situation with elevated cybersecurity risk. The interruption concept has been extensively discussed during this research. On the one hand, it is undeniable that such interruption does increase the user's awareness, which improves cybersecurity behaviour. That is demonstrated several times in the evaluation activities in this research. On the other hand, such interruption can present a usability problem, which would conflict with the need for usability. Still, this research does show that interruptive training can be implemented without sacrificing usability. No evaluations with potential users show usability issues with CBMT. Rather, the possible risks with interruptions have been described in expert evaluations and discussions with researchers. In conclusion, interruptive training must be implemented with usability in mind, and CBMT can be implemented with a high degree of usability (Paper 5).

5.1.3 REQUIREMENTS FOR CYBERSECURITY TRAINING
The evaluation requirements used in this research was designed by reviewing previous research evaluating cybersecurity training efforts. It is, in itself, a contribution from this research that can be used by other researchers seeking to research cybersecurity training methods (Paper 8). It describes four...
requirements that a method for cybersecurity training of end-users should meet, namely:

- It must support users towards secure behaviour.
- It must increase its users' knowledge about cybersecurity.
- It must be perceived as positive by its users.
- It must be feasible to implement in practice.

Requirement one is the key requirement since any training method must support users towards secure behaviour. The second key requirement is argued to be number three, which speaks of user perception. User perception is argued to be an important precursor to user adoption. User adoption is, in turn, necessary for the training to be able to provide its intended effect. Requirement two is mainly argued to complement one, and the rationale is that users cannot behave securely if they do not know how. However, previous research has suggested that knowledge does not necessarily translate to behaviour, which makes bullet two insufficient on its own. Further, requirement four emphasizes the need for demonstrating the possibility of implementing the method in practice and makes a crucial aspect for methods that intend to support implementations. The requirements are developed with such a method in mind but can also be used to evaluate actual implementations. The need for requirement number four is then removed, but the role of the other requirements remains the same.

The requirements are intended to facilitate evaluation by expressing what cybersecurity training should be evaluated by. However, it is evident that each requirement can be seen as a scale where any cybersecurity training method will have a more or less positive result. While evaluating a single method can provide important results, only comparative evaluations can reveal how different methods relate to each other. For a newly developed method to be considered a contribution, it should be proven to be better than existing methods. That requires comparative evaluations, and the evaluation process suggests that evaluations should demonstrate if a cybersecurity training method meets the requirements and if it does so better than existing methods.

5.1.4 DEMOGRAPHICAL ASPECTS OF THIS WORK

Possible differences between demographic groups have been considered throughout this research for two reasons. First, testing for demographic differences is argued to be an important step in assessing the generalizability of the results. To exemplify, an average result could hide significant between-group differences. If group A were to have an average score of five, and group B would have an average score of 1, the combined average would be 3, and the results would not be accurate for any of the groups. Further, finding a result for a large population without finding significant differences between sub-groups in that population would suggest that the results are indeed general for the population as a whole. A second reason for controlling for demographic differences was that previous research suggests that cybersecurity behaviour is a complex matter influenced by demographic differences. The demographic aspects continuously tested were age, perceived gender, IT competence and nation of residence (in
later stages). They were selected based on their previous use in cybersecurity research (Anwar et al., 2017; Debb et al., 2020; Dodel & Mesch, 2019; Lee & Kim, 2020; Siponen, 2000).

The results in this domain are a bit conflicted, and demographic differences were found, mainly for the nation of residence and IT competence (Paper 10). It is hardly surprising that IT competence impacts how a user will perceive cybersecurity training or usability in the domain. First, one can assume that an IT professional is more accepting and willing to put efforts into security since s/he is more aware of the consequences and perhaps also genuinely interested in cybersecurity. Security practices may also be perceived as easier to comply with for someone who works in IT since the configuration of password managers, encryption software, and such is not new to her. An effect of the nation of residence is also expected, not least considering previous research providing similar insights (Ameen et al., 2021; Onumo et al., 2017).

More unexpected was that age and perceived gender seemed to have little or no influence in the studies in this research (Papers 10 and 11). The effect of age and perceived gender has been evaluated regarding the perception of cybersecurity training and usability in the cybersecurity domain but has not been found to have any large impact. Several previous publications have studied the effect of gender on various cybersecurity aspects. For instance, Anwar et al. (2017) and Ifinedo (2012) suggest that female users intend to follow security policies more than male users. However, other studies have found that male users tend to create better passwords than female users (Fernandez-Aleman et al., 2015; Gratian et al., 2018). It is a bit unexpected that this research suggests that there are few or no differences in perception of usability or cybersecurity training, which can suggest two things. First, the context of this study is different from the other mentioned studies, and it may simply be that the differences identified in previous work do not impact the perception of training or usability. A second explanation can be that previously identified differences are not caused by gender but by other factors that have not been accounted for in previous work. However, the correct answer to that question is beyond the scope of this research.

5.2 SCIENTIFIC RIGOUR
This research adopted guidelines for well-carried-out design science research presented by Hevner et al. (2004). This section will discuss how the research responds to each of the six guidelines presented by Hevner et al. (2004).

5.2.1 PROBLEM RELEVANCE
The problem relevance guideline states that design science should, in information systems research, aim to develop solutions to relevant business problems. Hevner et al. (2004) stress that relevance is in part shown by demonstrating that the problem itself is relevant and important and that the developed artefact can solve that problem. Implementation of the artefact is crucial for demonstrating relevance.
There is no question that cybersecurity behaviour is a key security problem. Insecure user behaviour is the root cause of many, or even most, cybersecurity incidents in organizations making cybersecurity behaviour an emerging organizational problem. The artefact developed in this research provides a solution to that problem by outlining how end-user training should be implemented to support users to behave securely. The artefact is based on previous literature and aims to use strengths identified with previous artefacts for the same purpose while avoiding problems identified in previous literature. The implementability of the artefact is demonstrated by two different types of implementations, and the effect is shown through iterative evaluations, as concluded in Section 4.5.3 Evaluation. Thus, the developed artefact meets the problem relevance guideline by providing a proven solution to a relevant problem.

5.2.2 RESEARCH RIGOUR

The second guideline requires that rigorous methods are used in both the construction and the evaluation of the artefact. Hevner et al. (2004) describe that rigour must be assessed by considering the applicability and generalizability of the developed artefact. This research is argued to fulfil this requirement. It does so since it uses well-established scientific methods for both artefact development and evaluation. The overall research strategy has been to evaluate the developed artefact using empirical methods continuously. The scope of the evaluations has been growing, with initial evaluations using non-probabilistic sampling with the intent of acting as proofs-of-concept. Later evaluations included larger samples drawn with rigorous sampling methods to provide reliable evaluations. Likewise, the applicability of the artefact has been demonstrated by the implementation of the artefact in its intended environments.

Each individual research activity has relied on different research methods. Naturally, methodological considerations have been made in each of those activities. They are motivated and accounted for in Papers 1 to 11 supporting this thesis.

5.2.3 DESIGN AS A SEARCH PROCESS

Hevner et al. (2004) describe the search process as an iterative search for an artefact that meets its established criteria. The process often begins with a simplified version of the problem and explores the problem space with increased complexity through several design cycles. Hevner et al. (2004) argue that an artefact can be complete when it can be demonstrated to show that it solves its intended problem. The problem at hand in this research is end-user behaviour in the cybersecurity domain. The developed artefact has been shown to improve the behaviour of its users (Papers 4 and 9). It has further been evaluated in terms of user perception with positive results. That was demonstrated by first developing requirements that the artefact should meet and then evaluating the method against those requirements. The design process began with a simplified version of the problem, resulting in a brief conceptual description of a method. It was developed towards a more and more complete method through three design cycles.
5.2.4 DESIGN AS AN ARTIFACT
The design of an artefact is central to design science, and the artefact developed in this research makes the main contribution. Hevner et al. (2004) describe that the artefact should be represented to enable implementation and comparison with other artefacts for the same purpose. The artefact developed in this thesis is a method that is described in text and models. The description is intended to reflect the different theories that underpin the method so that it can be accurately compared with other artefacts for the same purpose. This allows the method to be both fully and partially tested and reflected upon, as discussed by Friedman (2003). One can, for instance, test any guidelines individually or all at once.

The purpose of the developed method is to support the implementation of cybersecurity training for end-users. It was used to support two implementations during the research, demonstrating that it fulfils its intended purpose.

5.2.5 DESIGN EVALUATION
Hevner et al. (2004) describe that the designed artefact should be evaluated using appropriate scientific methods. Peffers et al. (2007) further describe that evaluation seeks to measure if the artefact meets the criteria established for it. The nature of design science is such that it seeks to develop artefacts to solve problems or better situations. It is imperative to define the criteria for such a solution before or early in the research process. This research defined four requirements that the developed artifact should meet in order to be considered successful.

Hevner et al. (2004) describe that the research must show that the artefact works in its intended environment. That was demonstrated by using the CBMT method to develop two tools for end-user cybersecurity training. The evaluation employed established scientific methods to evaluate if CBMT could meet the criteria established at the beginning of the research. Further, there were several methods for cybersecurity training of end-users in existence before this research started. For the CBMT method to claim originality, it cannot only meet the criteria established for successful cybersecurity training of end-users. It must also be able to do so better than previous comparative methods. As a rule, evaluations compared CBMT to other commonly used methods in various evaluations. Since various previous methods exist, it was not deemed possible to include all methods in all evaluations. Instead, each comparative evaluation included CBMT and the most commonly used alternatives for the scenario considered in the evaluation. For instance, in DC2, CBMT was evaluated as a means of providing users with password guidelines. In this case, the most commonly used alternatives were to provide the guidelines as plain text or as a link to plain text (Paper 4).

Both Hevner et al. (2004) and Peffers et al. (2007) describe that evaluation processes should rely on established scientific methods. This research utilized several different methods for data collection for evaluation purposes, but the mainly used methods have been experiments and surveys. The gathered data has been quantitative and the reason for that has been that quantitative data allows for comparative analysis using statistical procedures.
5.2.6 RESEARCH CONTRIBUTIONS

Hevner et al. (2004) describe that design science research should result in contributions in the form of the artefact itself, theoretical insights and/or new methods to evaluate by. The results of this research are outlined above, and the contributions comprise the method itself, requirements for evaluation of cybersecurity training, and theoretical insights.

5.3 RESEARCH VALIDITY

Research validity is described by Oates et al. (2022) as including that appropriate processes have been used, that findings come from data and that the findings answer research questions. Oates et al. (2022) further state that different research communities have different interpretations of the validity concept, making it important for this research to view validity from a design scientist’s viewpoint. On that note, recent work in design science methodology argues that scientific validity is often second to the utility and efficacy of the artefact (Larsen et al., 2020; Lukyanenko et al., 2014). Actually, the word validity only appears once in the publication outlining the guidelines by Hevner et al. (2004), and that is in an example. Further, Peffers et al. (2007) argue for using an established research framework to ensure validity in design science research. Indeed, the framework described by Peffers et al. (2007) was used in this thesis.

While this research used an established framework to guide the research, that does not in itself guarantee the validity of the research. Larsen et al. (2020) present a framework for validity in design science research. That framework should ideally guide the research design but is used here to support a discussion on the validity of this research. The reason for the post-research application of this validity framework is that the framework was not published until 2020, and this research started well before that. Larsen et al. (2020) suggest a framework to support the discussion of validity in design science in three steps:

- **Design antecedent validity** deals with the input to the design process.
- **Development and use context validity** deals with the artefact itself and speaks of its suitability for its intended environment and how well it is represented.
- **Design outcome validity** deals with how the designed artefact meets established criteria and compares to other artefacts for the same purpose.

In terms of **Design antecedent validity**, this research has ensured the quality of input to the design process by relying on prior scientific work. The body of scientific literature has been consulted in initial artefact development and the development of evaluation requirements and processes. While the completeness of included reviews is for others to judge, literature has been consulted in a structured way that has been clearly described in publications supporting this thesis. These publications are appended to this thesis from page 133 and onward. Input to the design has further been gathered as a part of the different evaluation studies. The participants in those evaluations are possible future users. By allowing possible future users to influence the artefact design, the method's
suitability for its intended context is argued to increase. Further, the evaluations have been presented and discussed at scientific conferences. Input from those discussions has been collected as field notes and used as input into the research process.

*Development and use context validity* cover two concepts. First, it discusses the artefact’s suitability for its intended environment. In this case, the developed method intends to support the implementation of cybersecurity training for end-users. It can be used in two ways: to develop training implemented as a user-side tool or as a service provider implementation tied to a single service. One implementation of each type has been developed during the research, showcasing the artefact’s suitability in its intended environment. Second, the quality of the representation of the artefact is discussed. On that note, the quality of representation should perhaps be best judged by others. Yet, the demonstration activities have been performed by developers at a software development company, and that does, to some extent, also demonstrate that the representation is good enough to support the intended audience of it.

*Design outcome validity* mainly addresses the evaluation process. This research employed a structured and transparent evaluation protocol that emphasized comparison with other artefacts with similar purposes. Evaluations are grounded on previous research to ensure purposeful evaluation metrics.

### 5.4 REFLECTION ON INCLUDED PAPERS

This thesis is a compilation of eleven papers published in peer-reviewed academic conferences and journals. The papers are appended in full, starting on page 133. As an end to this discussion chapter, this section provides a presentation and discussion on the included papers.

Paper 1, *Online Fraud Defence by Context Based Micro Training*, evaluates if a CBMT demonstrator can support users in identifying online fraud and finds positive results when compared to a control group. This evaluation was carried out as a survey-based evaluation distributed using social media. This was the first academic paper published by the author of this thesis, and it is considered a pilot evaluation of the CBMT concept. In retrospect, the sampling and statistical procedures do not allow for strong conclusions. However, the study did show that the initial idea of CBMT was pursuable. The thesis author was the principal author of this paper and took the initiative to the study. The thesis author performed the study design and data analysis with guidance from the main supervisor. The thesis author further wrote the majority of the paper.

Paper 2, *Users perception of using CBMT for information security training*, was also a survey-based evaluation that evaluated participants’ perception of CBMT compared to classroom lectures, written information and longer videos online. The evaluation found that the participants preferred CBMT over the other options. Being a quantitative survey, this paper can be compared to Paper 1. On the topic of statistical analysis, Paper 2 uses inferential statistics rather than only descriptive, making the results more reliable. Sampling and risk of bias can also
be discussed in this publication. The sampling strategy was again to use social media, which is in line with the sampling strategy of this research. Bias stemming from the research design is, however, a likely negative aspect of this publication. In this case, participants were presented with CBMT-based training before being asked to rate CBMT in relation to other training methods. A likely effect is that confirmation bias comes into play and that the results should be seen as an indication rather than anything else. This paper was a joint effort between the three authors. The third author and the author of this thesis initiated the study. The study design and data collection were primarily completed by the second author. Data analysis and writing were primarily performed by the thesis author.

Paper 3, *Using Context Based MicroTraining to develop OER for the benefit of all*, present an evaluation where CBMT was used to produce learning material for a technical university course. The learning material was used by students attending the course. The results were derived by comparing the students' test results to test results from students taking the course in another format, using traditional lectures as primary learning material. This research intended to evaluate CBMT's ability to transfer knowledge to users, and it did successfully demonstrate that ability. Combined with Paper 2, this paper formed the evaluation tasks in the first DC, and they are argued to show that the fundamental idea of CBMT is sound and worthy of continued research. The thesis author was the principal author of this paper and took the initiative to the study. The thesis author further wrote the majority of the paper.

Paper 4, *Assisting Users to Create Stronger Passwords Using ContextBased MicroTraining*, reports on an experimental evaluation of CBMT. In this evaluation, CBMT was used to teach password guidelines to users of a website belonging to a local ISP. Length and strength of newly created passwords were measured and compared to a control group. The experiment showed that users of CBMT created longer and stronger passwords than users in the control group. Note that the metrics were automatically computed at the time of password creation and that only the metrics were shared with the researchers. The actual passwords, or any other user data, were never shared by the ISP. This evaluation used a fully functional implementation of CBMT and showcases both CBMT's effect on password behaviour and the implementability of CBMT. The password guidelines presented to users in this study resulted from the research presented in Paper 7. The thesis author was the principal author of this paper and took the initiative to the study. The thesis author performed the study design and data analysis with guidance from the main supervisor. The thesis author further wrote the majority of the paper.

Paper 5, *Can Johnny actually like security training?*, presents the result of a usability evaluation of the CBMT implementation used in Paper 4. Two usability experts analyzed the implementation, and the report written by the usability experts was analyzed qualitatively. This evaluation was completed to respond to the usability needs identified in the first design cycle. The evaluation suggested that users can positively receive CBMT but that its interruptive nature can pose a usability problem. An interesting reflection is that this study identified possible
usability problems that were not identified in other evaluations during this research. That suggests that including outside experts, in addition to users, will reinforce user perception evaluations. A possible reason could be that experts tasked with evaluating software spend significantly more time evaluating compared to users given the same task. One could also assume that experts will be more prone to identify problems since they will specifically look for anything that could be a problem. As the first author, the thesis author initiated this study, analysed the results of the usability study in relation to CBMT and wrote the majority of the paper, guided by author four. Authors two and three performed the usability analysis.

Paper 6, *ContextBased MicroTraining: A Framework for Information Security Training*, presents a summary of the research up until the end of method development in DC3. The main value of this publication is that it allowed for community feedback on CBMT and its development. The thesis author was the principal author of this paper and took the initiative to the study. The thesis author performed the study design and data analysis with guidance from the main supervisor. The thesis author further wrote the majority of the paper.

Paper 7, *Constructing secure and memorable passwords*, reports on research which intended to identify how password guidelines could support both computational security and the creation of memorable guidelines. The research was carried out in two steps. First, a literature review was used to identify password creation strategies that supported the creation of memorable passwords. This included using passphrases, passwords with several unrelated words and more. In the second step, optimal ways to attack different types of passwords were researched using expert interviews. Finally, the time to attack password created using the different strategies was computed. The result was that using at least four words as a password would result in passwords that are both memorable and computationally secure. The second contribution of this paper was the insight that users are more likely to adopt security guidelines if they are easier to use. This paper was a joint effort between the thesis author and authors two and three under guidance from author four. The thesis author initiated the study. The first three authors shared data collection, analysis and writing equally.

Paper 8, *Evaluation Strategies for Cybersecurity Training Methods: A Literature Review*, reports on a literature review that analyzed how cybersecurity training had been evaluated in previous research. It was used to guide the development of requirements and evaluation process for cybersecurity training used in this research. The thesis author was the principal author of this paper and took the initiative to the study. The thesis author performed the study design and data analysis with guidance from the main supervisor. The thesis author further wrote the majority of the paper.

Paper 9, *Evaluation of Contextual and Game-Based Training for Phishing Detection*, reports on an evaluation of CBMTs effect on behaviour in the third design cycle. This evaluation took place in a simulated environment. Compared to Paper 4, which reports on an experiment in a natural environment, a
simulated experiment allowed for close monitoring of participants and thereby a collection of more variables. However, it also means that participation bias can be assumed to impact the results. The experiment measured the participants’ ability to identify phishing and, given the participation bias, is argued to measure the participants’ best possible ability to identify phishing. It also compares CBMT to gamified training and shows that CBMT can improve users’ ability to detect phishing better than gamified training. This study also shows that even with training, detecting phishing is hard. A majority of the participants incorrectly identified at least one malicious email as legitimate. As a result, the paper concludes that training, while important, is not enough to ensure secure user behaviour. The CBMT training used in this evaluation was developed as a web browser plug-in that could identify and train users on phishing, online fraud, password security, and fake news. The browser plug-in development was guided by research into the usability of security tools, reported in Paper 11. The thesis author was the principal author of this paper and took the initiative to the study. The thesis author performed the study design and data analysis with guidance from authors three, four and six. Authors two and five developed the software used in the experiment. The thesis author wrote the majority of the paper.

Paper 10, *A Taxonomy of SETA Methods and Linkage to Delivery Preferences*, reports on a comparative evaluation of user perception of different cybersecurity training methods. The paper is currently under review. This evaluation contains one SLR used to identify and classify cybersecurity training methods discussed in scientific literature and a survey that identified how users prefer to partake in cybersecurity training. The survey respondents were not introduced to CBMT, or any other training methods, to minimize possible bias. The survey results were discussed in relation to the identified training methods and suggested that contextual training had the highest potential to be positively received by users. The survey used a stratified sampling method to recruit 800 respondents from Sweden and another 300 from the UK and Italy, respectively. The intention was to generate results representative of Swedish users first and then evaluate if those results could be transferred to Italian and British respondents. The result in this regard was that the results could indeed be transferred even if some national differences were identified. This study used a better sampling technique and a larger sample than previous surveys. This study was partly guided by the research plan where it was decided to use convenience sampling in the early research stages and more robust sampling in later stages. The reason was partly financial, and it can be mentioned that the cost for acquiring this sample was about 10 000 EUR while sampling using social media is free of charge. A second distinct difference that can be observed is that this survey goes to great lengths to ensure that the evaluation is not biased. This follows discussions had when publishing previous evaluations (especially Papers 1 and 2). In those evaluations, participants were presented with CBMT-based training and then asked about it. The risk of that bias was mitigated in Paper 10 by not describing any specific cybersecurity training method to the respondents. The thesis author was the principal author of this paper and took the initiative to the study. The thesis author performed the study design and data analysis with guidance from supervisors. The thesis author further wrote the majority of the paper.
Paper 11, *What Parts of Usable Security Are Most Important to Users?*, intends to provide insight into how users rate different usability aspects in the security domain. The rationale for this paper was twofold. First, the research provided input to the demonstration phase in DC3. Second, usability in the security domain is an integral part of this entire research, and this paper provides additional support for how users perceive security tools and features, which includes training methods. The research was carried out as a survey with 1452 participants. The results showed that minimizing resource consumption was prioritized by users. This includes time as well as costs and device performance. The thesis author was the principal author of this paper and took the initiative to the study. The thesis author performed the study design and data analysis with guidance from supervisors. The thesis author further wrote the majority of the paper.
CONCLUSION
CHAPTER 6
6 CONCLUSION

This chapter presents the conclusions drawn from this research related to the aim and objectives expressed in Section 1.2 Research aim. Contributions to academia and practice are then discussed before the thesis concludes with an outline of limitations and future work. The outline of the chapter is shown in Figure 31.

Figure 31 Outline of the conclusion chapter.
6.1 REVISITING AIM AND OBJECTIVES

The aim addressed in this thesis was *To develop a method that outlines goals and guidelines for cybersecurity training of end-users.*

The aim has been addressed by developing a method for cybersecurity training of end-users using a design science research methodology. The research contained three design cycles (DC), each with three phases: Method development, artefact demonstration and evaluation. The first method development phase drafted a conceptual notion of the method based on principles derived from previous literature on cybersecurity training and the Technology Acceptance Model (TAM). The second and third development phases continued and refined the method based on output from the evaluation phases of the previous DC. The artefact demonstration phases intended to demonstrate that the method worked for its intended purpose by using it to develop tools for cybersecurity training. Demonstrators were developed in DC1, while DC2 and DC3 developed fully functional tools for cybersecurity training used in the evaluation steps. The evaluation steps evaluated that the method could support users towards more secure behaviour, provide users with cybersecurity knowledge and that its intended users could positively receive it. Early evaluations were considered proof-of-concept studies with limited populations and implementations of the method. In contrast, later evaluations used fully functional implementations and larger samples acquired with more robust sampling methods. The final method has been evaluated with more than 1800 survey participants and 300 participants in various experiments.

Three objectives were established for this research with the intent of clarifying the research process:

- O1: Establish principles for cybersecurity training methods.
- O2: Establish requirements for evaluation of cybersecurity training.
- O3: Develop and evaluate a method for cybersecurity training of end-users.

The purpose of the first objective was to establish a theoretical reference for the rest of the research process. The Technology Acceptance Model (TAM) was adopted as a fundamental theory for this research. The rationale was first that user acceptance is a core concept for cybersecurity training of end-users. Users need to adopt both the training provided to them and adopt the behaviour suggested by that training. TAM explains user adoption of technology and makes it a good fit for this research topic. Second, TAM is a widely used model in information systems research, which is the area where this research is positioned. Previous research on cybersecurity training was also made part of the theoretical framework for this research and, together with TAM, formed the basis for five principles for cybersecurity training. Those principles were then reviewed throughout the research. They are presented in full in Section 4.5.4 Revisiting the principles of cybersecurity training.
The rationale for the second objective was a call for cybersecurity training methods which are thoroughly evaluated (Al-Daeef et al., 2017; Alshaikh et al., 2018). Also, Peffers et al. (2007) and Hevner et al. (2004) describe an explicated evaluation process as a core part of design science research. To that end, requirements to evaluate cybersecurity training by and a process outlining how such evaluation should take place were established before the start of DC1. The process emphasizes comparative evaluation, where research should show how evaluated methods compare with existing methods for the same purpose. The requirements were guided by the research presented in Paper 8 and suggest that cybersecurity training should be evaluated in terms of user perception, impact on user behaviour, ability to provide users with knowledge and implementability. The requirements are presented in full in Section 4.2.1 Requirements for cybersecurity training.

Finally, the third objective was explored in three design cycles and resulted in the method for cybersecurity training of end-users named Context-Based Micro-Training (CBMT). The development process is briefly described in the beginning of this section, and CBMT is described in full in Section 4.6 Context-Based Micro-Training - a summary.

In addition to the just presented outcomes related to the research objectives, this research makes several contributions to research and practice. Those are outlined in the upcoming sections.

6.2 CONTRIBUTIONS TO RESEARCH

The core contribution of this research is the method for cybersecurity training of end-users, CBMT. It is, in itself, a theory that describes how such training can be carried out. It can also be seen as individual statements that are recommendations for cybersecurity training efforts. CBMT is based on principles for cybersecurity training of end-users derived from TAM and previous research in the domain. These principles were established before the first DC and refined during the research. The principles make, in themselves, a theoretical contribution from this research. Likewise, the requirements and process for evaluation established and used in this research can form a foundation for comparative evaluations of future endeavours in the domain of cybersecurity training for end-users, and that is a scientific contribution of its own. This contribution is a response to the challenge “Many training methods are not based in theory, and their effectiveness is not empirically evaluated” identified in Section 2.3 User training and Awareness in the cybersecurity domain.

A second contribution is to the understanding of usability in the cybersecurity domain in general and cybersecurity training of end-users in particular. This research highlights that security is seldom the main target for the average user who is more interested in carrying out other private or work-related tasks. Ensuring that training and practices that intend to increase the security posture put as little effort on the user as possible is crucial. On this note, this work came to include research into usability in the cybersecurity domain. It was made evident that a lot of prior research discussed usability. It has, in fact, been discussed since (at least) 1999 (Whitten & Tygar, 1999). Still, no common
understanding of what usability encompassed in the security domain could be found. As a contribution, this research analyzed how usability has been discussed in the security domain by identifying factors that promote usability. Those factors were then further researched, focusing on what factors users considered to be most important (Paper 11). The results suggested that users prefer security functions and tools to require as little effort as possible. Efforts, in this case, include time, money and device resources. It was further made evident that more advanced features like customizability were low on the users' agenda. These insights provide a better understanding of the usable security concept and can guide future research.

The contribution described above is a response to the challenges “Users are informed about how to act but not motivated to act accordingly” and “Users are not actively participating in on-demand training” identified in Section 2.3 User training and Awareness in the cybersecurity domain. The first challenge is met by showing the importance of usability in terms of the guidelines that users are suggested to follow, which is further expanded on in the next paragraph. The second challenge is met by showing the importance of minimizing the resources users need to spend on cybersecurity training and that such training can be inserted into the users' routine activities, such as checking emails or creating accounts, without compromising usability. Further, this research demonstrates that training can, recurrently, be presented to users in situations where the training is relevant. Therefore, the research also provides a solution to the challenge "Knowledge acquired during training is only retained for a limited time."

As a final key contribution to academia, this research questions whether user training is enough to support users to behave securely. In essence, the results of this research suggest that training does lead to improved behaviour. It is also demonstrated that CBMT is superior to other training methods that it has been compared to, both in terms of user perception and ability to mediate behaviour. Nevertheless, it is also shown that even with training, users struggle to meet expectations put on them by the security community. Those expectations include that users should always select good passwords, never be tricked by phishing, and adopt suggested security features, which is difficult.

Consequently, this research suggests that the guidelines imposed on users must be reviewed through a usability lens. Finding a good way to teach users behaviour that is still difficult to adopt is futile. As such, as a final contribution to academia, this research calls for a questioning of not only password guidelines but also other practices that users are expected to follow. After all, the results of this research suggest that users will follow advice if the advice is easy enough to follow. Making the advice simple enough remains an open challenge.

6.3 CONTRIBUTIONS TO PRACTICE

The key practical contribution of this work is the method for cybersecurity training of end-users, CBMT, which is summarized in the Section 4.6 Context-
Based Micro-Training - a summary. It provides an empirically proven method for implementing training that improves the cybersecurity behaviour of its users. Practitioners can use it in two ways. First, it can be used by those seeking to implement cybersecurity training for end-users as a direct guide in their work. Second, it can be used as a reference for practitioners seeking to procure training for their organization. In the latter case, it can support the procurement process by providing insight into what to look for in the solution that is to be procured. Along the same line, the implementations developed during this research are available for use under free-to-use licensing and make additional contributions to the community of practitioners.

A subsidiary practical contribution concerns password guidelines. Password guidelines have traditionally suggested that user passwords should be long (at least eight characters) and composed of a mixture of character groups (uppercase and lowercase letters, numbers, and special characters). Research demonstrates that users struggle to follow these guidelines, and the lack of usability is given as an explanation. This research resulted in another guideline that was shown to generate passwords that were easier for users to remember and still resulted in computationally secure passwords. That guideline was to use passwords composed of at least four words unrelated to the password holder. While different from traditional guidelines, emphasising length and memorability should not be controversial. In fact, it aligns well with what several large organizations, including Microsoft and NIST, now suggest (Grassi et al., 2017; Microsoft, 2019).

6.4 LIMITATIONS AND FUTURE WORK

Digitalisation continues to grow and brings improvements and opportunities for work, communication, leisure and more. The positive effects of digitalisation have not least been seen during the Covid-pandemic where people in quarantine have been able to maintain connections with friends, family and colleagues. However, digitalisation has negative consequences, such as cybercrime, which reveals a need for cybersecurity. Cybersecurity is a broad area of technical, organisational and human aspects, and this research considers cybersecurity behaviour which is one part of the human aspects.

Cybersecurity behaviour is a complex area. It is, as described throughout this research, influenced by a number of factors. While end-user training plays a central role in supporting users towards secure behaviour, it is not enough on its own. This research aimed to research cybersecurity training of end-users specifically, and the results are, to a large extent, limited to that domain. On this note, the research results already suggested a need to consider usability as a central factor in the general design of security practices. A natural direction for future work would be to study training and security practices together.

The majority of evaluations carried out in this research were comparative and assessed the effect of CBMT compared to one or more other methods for cybersecurity training of end-users. While that type of evaluation is common in cybersecurity training research, it may introduce a limitation. Different training methods are compared by how they differ from each other rather than how they could complement each other. Several different methods have been discussed
throughout this thesis, and they have different strengths and weaknesses. As one example, a simple but obvious difference between CBMT and instructor-led lectures is that a lecture will, by design, cover the presented information at a significantly deeper level. While this research argues that the CBMT method is more likely to lead to improved behaviour, that does not necessarily mean that lectures are pointless. It may be so that the best approach to cybersecurity training is to combine two or more methods, and that is an obvious direction for future work.

Another limitation of this research is the context in which it was carried out. Most of the research tasks were conducted in Sweden and with Swedish participants. That is especially true for experiments that needed the participants to be physically present. Including participants from different countries in those experiments was practically infeasible. While efforts were made to make survey-based evaluations cover larger populations, and data to support the method development was gathered from discussions at international conferences, it should be noted that the results are first and foremost representative of Swedish users. Even if the results can, in part, be transferred to other demographics, future studies replicating the results in other parts of the world are reasonable. Especially since this research identified the nation of residence as a factor that does impact the perception of cybersecurity training.

A last limitation also serves as a reflection on how samples are often drawn from populations within research in the human aspect of cybersecurity. Or rather, what populations tend to be studied. This research has attempted to use samples representative of online users in general. While this is a common approach, it assumes that the struggles users face are also general, which could be questioned. Recent studies have, for instance, found that cybersecurity behaviour is affected by factors such as cognitive ability and fatigue (Gutzwiller et al., 2020; Reeves et al., 2021). Furthermore, disabilities can impact a user’s ability to use technology (Johansson et al., 2021). Consequently, it may be reasonable to assume that different user groups face different struggles. Since the goal of any organization must be to support all of its users towards secure behaviour, a consequence could be that generalized studies should be reconsidered in favour of studies focusing on narrower user groups. That makes a final suggested direction for future work.
REFERENCES


REFERENCES


Dittrich, D., & Kenneally, E. (2012). *The menlo report: Ethical principles guiding information and communication technology research.*


REFERENCES


Goles, T., & Hirschheim, R. (2000). The paradigm is dead, the paradigm is dead... long live the paradigm: the legacy of Burrell and Morgan. Omega, 28(3), 249-268. https://doi.org/10.1016/S0305-0483(99)00042-0


Schrittwieser, S., Mulazzani, M., & Weippl, E. (2013). Ethics in security research which lines should not be crossed? In *Proceedings of the 2013 Security and Privacy Workshops (SPW)* (pp. 1-4). IEEE. https://doi.org/10.1109/spw.2013.6614700


Siponen, M., & Baskerville, R. L. (2018). Intervention effect rates as a path to research relevance: Information systems security example. *Journal of the
REFERENCES

Association for Information Systems, 19(4). https://doi.org/10.17705/1jais.00491


PUBLICATIONS IN THE DISSERTATION SERIES
INCLUDED PUBLICATIONS
PUBLICATIONS IN THE DISSERTATION SERIES


PAPER 1: ONLINE FRAUD DEFENCE BY CONTEXT BASED MICRO TRAINING

Online Fraud Defence by Context Based Micro Training

J. Kävrestad and M. Nohlberg

The School of informatics, Högskolan i Skövde, Skövde, Sweden
e-mail: {joakim.kavrestad; marcus.nohlberg}@his.se

Abstract

Online frauds are a category of Internet crime that has been increasing globally over the past years. Online fraudsters use a lot of different arenas and methods to commit their crimes and that is making defence against online fraudsters a difficult task. Today we see continuous warnings in the daily press and both researchers and governmental web-pages propose that Internet users gather knowledge about online frauds in order to avoid victimisation. In this paper we suggest a framework for presenting this knowledge to the Internet users when they are about to enter a situation where they need it. We provide an evaluation of the framework that indicates that it can both make users less prone to fraudulent ads and more trusting towards legitimate ads. This is done with a survey containing 117 participants over two groups where the participants were asked to rate the trustworthiness of fraudulent and legitimate ads. One groups used the framework before the rating and the other group did not. The results showed that, in our study, the participants using the framework put less trust in fraudulent ads and more trust in legitimate ads.

Keywords

Online fraud, fraud defence, awareness, micro training

1. Introduction

Over the past years online fraud has evolved to be an increasing crime that is targeting a large portion of the Internet users. This fact is being reported in many countries including Sweden and the USA (Brottsförebyggande rádet, 2013; IC3, 2013). As one example it was estimated that one third of the American adults experience victimization annually (Pratt, Holtfreter, & Reisig, 2010). Online frauds come in many different forms and are occurring in several different arenas including e-mail, social networks, online auction houses and telephones. The great variety of the modus operandi of the fraudsters makes online fraud defense a difficult task.

Previous research makes it clear that online fraud is not a crime that target specific groups of Internet users. Rather, it seems as if anyone that is present on the arenas were frauds are being executed faces the risk of not only being targeted by a fraudster, but also to fall for the fraudsters actions. This is shown in the research by Wilsem (2013).

The common suggestion on how to defend yourself against online fraudsters in to gather the knowledge and skills you need to avoid being defrauded before you
encounter a fraudster, as exemplified by usa.gov (2013) “The best way to fight Internet fraud is to learn how to avoid becoming a victim”.

Today, this knowledge is often presented on governmental and business webpages and the users are expected to identify and make use of the information on their own. This puts the responsibility of defense on the users rather than the actors hosting the arenas where the frauds can take place.

In this paper we suggest a model for online fraud defense that aims at educating users that are encountering a potentially fraudulent situation. The education is taking place in the moment were the fraud may be executed and is tailored to learn the user about the specific fraud attack he is currently in the risk of facing. This methodology is influenced by the concept of situated learning as described by Herrington & Oliver (1995).

With this approach we believe that the users will make use of the information because it is relevant for their current situation. It has also been discussed that when you acquire knowledge in a situation where you use that knowledge, the overall learning process provides better result compared to if you are learning in a theoretic manner, i.e. by reading from a book or webpage (Brown et al, 1989). Further, as shown by Davinson & Sillence (2010), being aware of the possibility of being defrauded will reduce the risk of being victimized. It is our belief that presenting information about online frauds just before the user enters an arena where frauds are being executed will make the user more aware and thus further reducing the risk of victimization. Similar effect was discussed by Davinson & Sillence (2010) who researched the effects of anti-phishing training. They discussed if the users behaviour was enhanced due to actual training or due to that the users awareness was increased just by being confronted with a training program.

Within this paper we also present an evaluation of the defense model that indicates that it can change user behavior in potentially fraudulent situations. The evaluation is done in an online auction house scenario.

The remainder of this paper presents our suggested defense model and our evaluation of the model

2. Proposed defence mechanism

Several researchers argue that knowledge is the best defense against online fraudsters. In example see Arachchilage and Love(2014) and Garg and Nilizadeh (2013). The same is stated by several governmental web pages including usa.gov (2013). While we do not argue with this fact we have seen that this knowledge often comes in the form of informational websites, thus creating a situation where the potential victims are required to acquire the knowledge they need before they encounter a potentially fraudulent situation.
We also believe that knowledge is the best countermeasure to online fraud but in our opinion the current situation introduces the following three issues:

- The potential victims are expected to gather knowledge before they encounter a potentially fraudulent situation. This implies that common Internet users must gather knowledge about something they may not be aware of.

- Internet users are supposed to read about online frauds in a context were the knowledge is not usable.

- The responsibility is put on the users rather than on the owners who hots the arenas were online frauds are taking place.

With our defense mechanism we make use of the ideas of situated learning that states that a learning experience is more meaningful if the learning is taking place in a context were the information is immediately useful (Herrington & Oliver, 1995). We call our approach context based micro training.

With context based micro training we developed a framework for introducing precise and tailored knowledge to Internet users in the situation were they may need it. To make the information as useful as possible to the users, the framework states the following about the information that is presented to the user:

- Relevant in the users current situation, i.e. if a user is entering an online auction house, where frauds has taken place, he will receive information about how to identify and avoid fraudsters in online auction houses.

- Interactive information meaning that the information module will require active participation from the users. As stated by Herrington & Oliver (1995) this approach increases the users awareness

The processes in the framework are shown in Figure 1.
With this approach we aim to put precise information into a user’s mind just before the users enters a potentially fraudulent situation. Since the information is tailored to the users current situation and requires participation from the user we believe that users that make use of this framework will be educated and prepared for the situation they enter and they will also be more aware of online frauds.

3. Research aim and limitations

The aim of this study is to evaluate the presented defense mechanism for use against online fraudsters. As described, the aim of the model is to provide knowledge ”in the moment” and for that reason long time effects of the mechanism is not in the scope of the study. Rather, this study aims at providing a proof of concept for the direct effects of the proposed defense mechanism. Further, this study evaluates the defense mechanism in an online auction house environment. While we strongly believe that it can be used in other environments as well, effects of the mechanism in other environments is beyond the scope of this study and could be explored in the future. Also, this study does not provide a technical solution for how to implement the mechanism. While the actual implementation is not in the scope of this study we suggest that the mechanism can, for instance, be implemented in the following ways:

- As an interactive game or questionnaire when a user in an online auction house is entering a category of goods where the owner of the auction house is currently aware of ongoing frauds.

- As a way of countering telephone related frauds by warning users that are calling or receiving calls from numbers that are related to fraudulent behavior. This can be accomplished by matching incoming calls to a database of numbers that has been reported for fraudulent actions.

The aim of this study was reached by exploring the following questions in a controlled environment:

Q1: Can the defense mechanism help users identify fraudulent ads?
Q2: Will the mechanism make the users more likely to falsely identify legitimate ads as fraudulent?

4. Research model

To generate truly reliable results one could argue that this research is best conducted with a real-world approach by testing user’s behavior in authentic situations. However, it is hard to conduct such study in an ethically appropriate manner. As example see Dittrich & Kenneally (2011) and Schrittwieser, Mulazzani & Weippl (2013). The guidelines proposed in those articles were followed in this study.

Instead, the research questions were explored in a survey-style environment. A central point in conducting a survey is that the sample of participants should represent the characteristics of the surveys intended population (May, 2001). In this case the intended population was everyone, in Sweden, that uses the Internet. May (2001) argues that the only way to generalize from the results of a survey is to use a probability sample. However May (2001) also states that using this kind of sample is not always possible. One requirement that a sample must fulfill in order to be called a probability sample is that every person in the population has an equal chance of participating in the survey. In this survey that is impossible because of the size of the population that holds a large portion of the Swedish population. A more convenient way of sampling would be to use a convenience sample where the sample is taken from people close to the researcher (Robson, 2011). Using such a sample will, however, generate less generalizable results (Robson, 2011). Since it was not feasible to use a probability sample in this study the aim was to get participants from different geographical places and with different demographic attributes. In order to achieve this, the surveys was be marketed over the Internet through social networks. This did not generate a probability sample but the sample did likely contain respondents with different backgrounds resulting in a more generalizable result than if convenience sampling where to be used.

In the survey, the participants were presented to six ads from a Swedish online auction house called Tradera.se. Three of the ads were known to be fraudulent and three were supposedly legitimate. The fraudulent ads were supplied by the Swedish online auction house Tradera and the other ads were randomly chosen from the same site. The participants was asked to rate the trustworthiness of each ad on a sex-graded scale were 1 meant that the ad was not trustworthy at all and 6 meant that the ad was completely trustworthy. The participants were guided to a website containing the survey and were randomly assigned to one of two groups called DM and non-DM. A total of 117 participants went through the full survey, 70 in the non-DM group and 47 in the DM group. The participants in the different groups performed the following tasks:

- **DM**: The participants in this group went through three learning modules designed according to the proposed defense mechanism before rating the ads. The learning modules were in the form of slideshows that presented a dialogue between a buyer and a seller. The participants were asked to
decide if the buyer was in a potentially fraudulent situation or not. Based on the participants answer they received feedback describing if the buyers behavior was insecure and in that case why.

- Non-DM: The participants in this group rated the ads without going through the defense mechanism or being presented to any training.

5. Results

This section provides the results from the survey and conclusions related to the research questions. Figure 2 shows the average answers from both groups for the fraudulent ads. The column names are formatted in the following way: “question number – group”

![Figure 2: Overview of results for the fraudulent ads](image)

As seen in the figure the participants in the DM group rated all three fraudulent ads as less trustworthy compared to the rating from the group non-DM. This result does show that the defense mechanism can, in a controlled environment, make users better at detecting fraudulent ads. This is the answer to Q1: Can the defense mechanism help users identify fraudulent ads?

![Figure 3: overview of the results for the legitimate ads](image)

Figure 3 reflects the average answers for the randomly chosen supposedly non-fraudulent ad.
As seen in the figure the participants in the group DM rated these ads as more trustworthy than the participants in the non-DM group. Thus, based on the results from this study the answer to Q2 "Will the mechanism make the users more likely to falsely identify legitimate ads as fraudulent?" appears to be no. On the contrary the participants who used the defense mechanism actually placed more trust in the supposedly legitimate ads than the participants who didn’t.

To summarize; this survey indicates that using the defense mechanism we propose in an online auction house environment can make the users less susceptible to fraudulent ads. Moreover the results indicate that the users will also put more trust in legitimate ads. However it must be said that there was a great spread in the answers for all groups over all ads. This is shown in Table 1 that presents the standard deviation for each ad and group. This shows that with or without training it is hard to distinguish a fraudulent ad from a legitimate with only the actual ad as information.

<table>
<thead>
<tr>
<th>Question</th>
<th>Standard deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud1-nonDM</td>
<td>1,48</td>
</tr>
<tr>
<td>Fraud1-DM</td>
<td>1,56</td>
</tr>
<tr>
<td>Fraud2-nonDM</td>
<td>1,51</td>
</tr>
<tr>
<td>Fraud2-DM</td>
<td>1,35</td>
</tr>
<tr>
<td>Fraud3-nonDM</td>
<td>1,64</td>
</tr>
<tr>
<td>Fraud3-DM</td>
<td>1,38</td>
</tr>
<tr>
<td>Fraud4-nonDM</td>
<td>1,60</td>
</tr>
<tr>
<td>Fraud4-DM</td>
<td>1,56</td>
</tr>
<tr>
<td>Fraud5-nonDM</td>
<td>1,65</td>
</tr>
<tr>
<td>Fraud5-DM</td>
<td>1,73</td>
</tr>
<tr>
<td>Fraud6-nonDM</td>
<td>1,68</td>
</tr>
<tr>
<td>Fraud6-DM</td>
<td>1,37</td>
</tr>
</tbody>
</table>

Table 1: Standard deviation for all survey questions
6. Discussion

This study presented a framework for defense against online fraudsters and provided a proof of concept for that framework by testing it in a controlled environment. In this particular study the framework was tested in an online auction house environment. For that reason it is not possible to tell about the effects of the framework in another setting. Furthermore we want to mention that making this kind of studies in a controlled environment is troublesome since several factors that are present in a real world situation are difficult to imitate. After all, the participants in this study did never face any real risk of actually being defrauded. Also, they did not have all the opportunities to really investigate the seller that you would have in a real situation. For one, calling the seller and offer to meet and conduct the transaction in person can be an effective way of avoiding fraudsters.

With that said the study does provide the results that we set out to find by generating a proof of concept for the defense mechanism that we propose. This is done by showing that in our test:

- A person who uses the mechanism is better at identifying a fraudulent ad than a person who does not use it and,

- A person who uses the mechanism does not falsely identify legitimate ads as fraudulent more frequently than a person who does not use it. On the contrary the results actually indicated that a person using the mechanism places more trust in legitimate ads than a person that does not use the mechanism.

7. Future work

One could argue that to generate really strong results when researching online fraud you would have to conduct research in real life scenarios. Since this would involve actually tricking real persons without their knowledge and consent it is of course impossible without breaking many of the ethical guidelines set by the research community.

Even with these problems we acknowledge that conducting studies that imitates real life scenarios is crucial in order to generate a strong basis of research with reliable results. It is our understanding that more research within the area of online fraud prevention with a focus on the users behaviors is necessary. For future research within this domain we suggest that researchers make use of gamification as a part of the methodology. While we cannot recreate a real life situation using surveys or likewise we believe that making the actual study into a game, where the participants are encouraged to do good in order to get a high score or likewise, can make the participants feel the same risks as they would in a real life situation.
8. References


PAPER 2: USERS PERCEPTION OF USING CBMT FOR INFORMATIONSECURITY TRAINING

Users perception of using CBMT for information security training

J. Kävrestad, M. Skärgård and M. Nohlberg

School of Informatics, University of Skövde, Skövde, Sweden
e-mail: {joakim.kavrestad; marcus.nohlberg}@his.se

Abstract

It is well established that user behavior is a crucial aspect of information security and archiving secure behavior through awareness and security training is the go-to solution proposed by practitioners as well as the research community. Thus, there is a dire need for efficient training methods for use in the security domain. This paper introduces ContextBased MicroTraining (CBMT), a framework for information security training that dictated that information security training should be delivered to end users in short-sequences when the users are in a situation where the training is needed. Further, the users' perception of CBMT in evaluated in an online survey where about 200 respondents are subjected to training material and asked about how they perceived them. The results show that users like the training material designed according to the CBMT framework and would prefer to use CBMT over other traditional methods of information security training.

Keywords

Information security, training, learning, user behavior, micro training, ContextBased MicroTraining, CBMT

1 Introduction

It is well established that almost any organization is supported by IT and that securing IT systems is a critical component of those organizations. While there is a multitude of technical security controls available on the market, research, as well as the practitioner community, agrees that user behavior is a key aspect of information security (Bulgurcu, Cavusoglu, & Benbasat, 2010; Safa & Von Solms, 2016). While users are commonly referred to as the weak link in security, measures have to be taken to enforce secure user behavior. As discussed by Desman (2003), it comes down to making users understand the consequences of insecure behavior and learn the users to behave in a secure way.

As described by Puhakainen and Siponen (2010), literature often suggests training as a method for encouraging secure behavior, yet there is a need for training methods that are theory-based and empirically evaluated. The goal of any training intervention would be to make users behave in a secure way. On that topic, Parsons (2018), suggest that training should not only be about making the user know how to behave but also stop and think before they behave.
In this paper, ContextBased MicroTraining (CBMT) is presented, a framework for training users to behave securely. CBMT aims to deliver information security training in short sequences and is in that sense similar to, for instance, nano learning. However, CBMT also stipulates that training should be delivered to users in the situation that it is of direct relevance. Thus, the training should be perceived as more relevant and bring a reminding effect. Further, we evaluated how CBMT is perceived by users using a survey where the subjects are presented to three CBMT modules and asked a series of questions about how they perceived using CBMT in relation to other methods of training.

The precise aim of this study is to see if a random selection of Internet users appreciates using material created according to the CBMT framework for information security training. The study is intended to be used as a pilot to prepare for a larger, more practical project.

The remainder of the paper will present the CBMT framework and then describe the research approach used in this paper and the results of the study.

2 ContextBased MicroTraining

The CBMT framework is based on the fundamental belief that people need motivation in order to learn. The idea here is that the likelihood that any adult will learn is increased if the knowledge seems meaningful for the learner (Hedin, 2006). This notion is based on the concept of andragogy, as presented by Knowles (1984). Knowles (1984) argues that adults need motivation in order to learn. The foundation in this way of thinking is that the learner will learn better if the knowledge presented seems meaningful. One way to accomplish this is to present the knowledge in a context where it is applicable. As discussed by Herrington and Oliver (1995), presenting knowledge to learners in a situation where the knowledge is applicable will cause a more meaningful learning experience. This is the first requirement that CBMT tries to facilitate.

Further, an obstacle in the sense of providing the computer user with knowledge about information security has been to make the users participate in education. One technique that has gained an increasing interest in the past years is microlearning or similar strategies, including nanolearning and micro-training. As described by Wang, Xiao, Chen, and Min (2014), nanolearning is a teaching method where information is presented in short sequences. The idea is to facilitate just-in-time learning meaning that information is provided in small chunks, thus making the time needed to absorb the information short and in an on-demand fashion (McLoughlin & Lee, 2008). As described by Bruck, Motiwalla, and Foerster (2012), there has been research showing positive results of microlearning both in terms of learner participation and satisfaction. Microtraining is the second fundamental building block of ContextBased MicroTraining.

On a practical note, CBMT can be described as a framework that describes learning objects from two directions. The first direction concerns the delivery of the learning objects and states that the learning objects should be short sequences delivered in an
on-demand fashion. The second direction concerns the content of the learning objects. In this respect, CBMT demands that the information presented in a learning module is of immediate use to the learner and therefore assumes that the information is relevant to the user in the user's current context. In this respect, CBMT tries to facilitate the concept of "learn by doing" theories that can be summarized as a describing that learners learn better when they perform tasks instead of just reading (Koedinger, Kim, Jia, McLaughlin, & Bier, 2015). CBMT is also a learning method that includes aspects of problem-based learning (PBL) in that it is designed to guide the learner through real-world tasks (Boud & Feletti, 2013). In summary, the meaningfulness is achieved by the learner doing some task related to his or her situation.

Given the discussion in the previous sections, CBMT is a teaching method where information is provided in small segments to the learner. Further, the information presented is relevant to the learner in his or her current situation. A simple way of modelling CBMT is provided in Figure 1.

![Figure 1: conceptual model of CBMT](image)

Looking at the abstract model in Figure 1, CBMT begins with a learner entering a situation or starting a task. For the sake of this description, that situation can be that the learner opens an e-mail containing a link. Based on this situation, the learner is presented to a learning module with relevant information relating to the current situation. In this example, it could be information telling the learner not to enter account information into links sent via e-mail or to verify that the e-mail address of the sender matches the source that the e-mail appears to be from. The learner is then supposed to carry on with the task, in this case reading and reacting to the e-mail. As such, CBMT is a process where the central concept is that the information presented is relevant for the situation that the learner is in. The format that the information that is presented is not specified in detail by CBMT but should comply with the ideas of nanolearning, namely facilitate just-in-time learning while the learner can maintain interest in the information.

As for the actual implementation of CBMT, there are two distinct ways in which it can be done. In the context of teaching computer users about information security, it would seem feasible to have a software monitor what is happening on the user's computer and present the learning modules whenever the users enter a situation or perform an action where he or she needs the information. In this case, the computer would decide when the user is entering a context where the information is applicable. The implementation of CBMT in such a scenario is modeled in Figure 2.
The case in Figure 2 assumes that CBMT is used to combat online fraud. In this scenario, a computer would evaluate when to detect that a user enters a situation than the user is at risk of meeting a fraudster. If so, the computer will present information to the user so that she can handle the situation.

As described by Kävrestad and Nohlberg (2015), CBMT has been evaluated as a way to teach Internet users about online fraud schemes with positive results. The method was further explored in the same context by Werme (2014) with similar results.

To summarize, CBMT is a learning method where short sequences of information are presented to the learner in a context where it is of direct relevance to the learner. The teaching method is similar to nanolearning. As described by Wang et al. (2014), nanolearning is a teaching method where information is presented in short sequences. The difference between nanolearning and CBMT is that CBMT also presents the information in a context where it is of relevance to the learner. Another difference is that CBMT in itself encourages the learner to immediately use the information presented to her. Thus, CBMT encourages retrieval of information, an important factor in learning (Karpicke & Roediger, 2008).

### 3 Methodology

This study was conducted using an online survey with Likert-style questions written in Swedish. The survey was preceded with three learning modules, designed according to the CBMT framework and delivered as online videos publicly available on YouTube. A picture demonstrating how the material was presented, in a video about creating strong passwords, is presented in Figure 3, below. All learning modules was

---

1 All the videos can be found here: https://www.youtube.com/channel/UC4gDh8JF8S0z7rjaKPu0ovg

under 60 seconds in length and contained practical elements asking the user to perform some action. The learning modules were designed to teach the participants:

- How to create strong passwords
- Detect phishing emails
- Avoid ransomware

Figure 3: Picture demonstrating one of the learning modules (Translated from Swedish)

Following the learning modules, the participants were asked questions divided into three groups:

- Demographic questions
- Questions about the specific learning modules
- Questions about CBMT in general and compared to other teaching methods.

All questions were designed as Likert-style questions where the participants were asked to rate how well they agreed to a statement. They had the following answer options:

- Fully agree
- Mostly agree
- Partially agree
- Agree to some extent
- Do not agree

In analyzing the responses, all answers were dichotomized. The answers “Fully agree” and “Mostly Agree” was converted to 1 and the other options to 0. Thus, 1 represent an agreeing answer. The dichotomized variables were used to created indexes reflecting how the participants experienced the learning modules and how they perceived CBMT in relation to other types of training.

The results of the survey will be presented using the mean values of the indexes. Further, one-sample T-test will be used to calculate a 95% confidence interval and test if the results are significantly separated from 2. 2 is used since it is half of the possible max value. Further, as described by Siponen (2001), it is reasonable to assume that training will be perceived differently between professional computers users and other
users. Thus, mean values grouped by the respondents reported computer skills will also be presented and independent sample T-test used to analyze the difference in means between those groups.

4 Results

The survey was distributed via social networks, and 198 respondents completed the survey. The answers were used to compute and analyze indexes that describe how the participants perceived the learning modules used in this study, and CBMT in general. Before answering the questions, the respondents were asked to use three learning modules designed according to the CBMT framework. They were presented to the respondents as videos and covered the following content:

- How to create strong passwords (V1)
- How to avoid phishing (V2)
- How to avoid ransomware (V3)

The remainder of this chapter will describe how the indexes were calculated, and their results.

4.1 The learning modules

The participants were asked to use three learning modules designed according to the CBMT framework. They were then asked to rate the following statements about the videos (X being the particular video):

- I find that the content about X was clearly presented.
- I find that the content about X was useful
- I find that I learned something from the video about X
- If I had seen the video in a situation related to X it would have affected my actions.

The answers to the questions were dichotomized so that the two most positive answer options were represented by 1 and the three least positive answers were represented by 0. An index of all questions was computed by adding the variables together. To exemplify, if a respondent provided positive answers to all four questions, the index value became 4, if a respondent provided positive answers to two of the questions, the index value became 2. The results are presented for the entire sample and grouped by the respondent answer to the question about whether or not she considers herself a professional computer user. The results are presented in Table 1.

As seen in table 1, the mean values for the entire sample were above 2 for all videos. This means that the average participant provided more than 2 positive responses for each video. A one-sample T-test, using 2 as test value, was used over the entire sample and showed that the mean value in the population is above two, with a 95% confidence level. The literature suggests that information security training can be perceived differently between professional computer users and regular users. Thus, the index
values grouped on this variable is also shown in Table 1. The difference in mean was tested using an independent sample T-test that shows that there is a significant difference between those groups. In summary, the analysis of how the participants perceived the learning modules suggest that the participants did perceive them as good and useful, and that non-professional computer users were more positive than professional computer users.

<table>
<thead>
<tr>
<th>Video</th>
<th>Index Mean</th>
<th>T-test (2)</th>
<th>Confidence interval</th>
<th>Mean Unprof. N=86</th>
<th>Mean Prof. N=103</th>
<th>T-test</th>
<th>Confidence interval of the difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1</td>
<td>2.7</td>
<td>0.000</td>
<td>2.53-2.86</td>
<td>2.9</td>
<td>2.5</td>
<td>0.025</td>
<td>0.05-0.70</td>
</tr>
<tr>
<td>V2</td>
<td>2.5</td>
<td>0.000</td>
<td>2.35-2.70</td>
<td>2.7</td>
<td>2.0</td>
<td>0.023</td>
<td>0.06-0.75</td>
</tr>
<tr>
<td>V3</td>
<td>2.2</td>
<td>0.013</td>
<td>2.05-2.43</td>
<td>2.5</td>
<td>2.3</td>
<td>0.004</td>
<td>0.18-0.93</td>
</tr>
</tbody>
</table>

Table 1: Statistics for indexes over videos. 95% confidence level is used in all tests, p=0.05.

4.2 CBMT in general

Following the questions about the individual learning modules, the participants were asked the following four questions about CBMT in general:

- I would like to see more videos like this
- I would like to have access to videos like this when I perform tasks that could include security risks
- I think that the videos are well-suited to teach me information security
- I liked the videos

An index reflecting the respondent’s answers to the questions was calculated in the same way as for the video-related questions. The statistics are presented in Table 2, below.

<table>
<thead>
<tr>
<th>Index Mean</th>
<th>T-test (2)</th>
<th>Confidence interval</th>
<th>Mean Unprof. N=86</th>
<th>Mean Prof. N=103</th>
<th>T-test</th>
<th>Confidence interval of the difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.7</td>
<td>0.000</td>
<td>2.48-2.84</td>
<td>2.9</td>
<td>2.4</td>
<td>0.017</td>
<td>0.08-0.82</td>
</tr>
</tbody>
</table>

Table 2: Statistics for indexes over CBMT in general. 95% confidence level is used in all tests, p=0.05.

As seen in Table 2, the confidence interval for the entire sample was 2.48 to 2.84 showing that the mean for the sample was positive to more than two of the statements. Again, non-professional users were more positive than professional users. In summary, the respondents are positive to CBMT in general, and non-professional users are more positive than professional users.
4.3 CBMT compared to other methods of training

The survey ended with the following question about CBMT compared to other methods of training:

- I prefer this type of training over classroom-training
- I prefer this type of training over written text about information security
- I prefer this type of training above longer videos online

Again, an index of the respondents’ answer was calculated. The statistics are presented in Table 3. Note that this index only contains three items, thus the max value is 3.

<table>
<thead>
<tr>
<th>Index Mean</th>
<th>T-test (2)</th>
<th>Confidence interval</th>
<th>Mean Unprof. N=86</th>
<th>Mean Prof N=103</th>
<th>T-test</th>
<th>Confidence interval of the difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2</td>
<td>0.023</td>
<td>2.02-2.3</td>
<td>2.3</td>
<td>2.0</td>
<td>0.141</td>
<td>-0.08-0.82</td>
</tr>
</tbody>
</table>

Table 3: Statistics for index over CBMT compared to other methods of training. 95% confidence level is used in all tests, p=0.05.

The results presented in Table 3 shows that the mean value of the entire sample is above 2, meaning that the respondents prefer CBMT over other types of training to a large extent. In this case there is no significant difference between non-professional and professional computer users.

5 Discussion

The aim of this paper was to analyze how the teaching framework CBMT was perceived by computer users as a method of information security training. A second aim was to investigate if CBMT was perceived differently between processional computer users and regular computer users. The evaluation was carried out by means of an online survey where respondents were asked to complete three learning modules before filling out a form with questions about how they perceived the particular learning modules, CBMT in general and if the preferred CBMT over other means of training.

The analysis was done using an index that reflected how many positive responses the respondents gave to each group of questions. The analysis of the survey data suggests that the respondents were positive to the learning modules and that they appreciated using CBMT in general. In numbers, the mean values for the entire population were above 2 positive responses out of 4 for each video and for CBMT in general. Further, the comparison of professional and non-professional computer users showed that non-professional computers users were more positive than professional computers users.

The final part of the survey analyzed if the respondents preferred CBMT over other typed of information security training. In this case, the mean values for the entire population were above 2 positive responses out of 3. This suggests that CBMT is a method of training that is preferred over others, by the users.
In conclusion, this study suggests that CBMT is a training method that is appreciated by the users, and that is preferred above other methods of training. The study also suggests that CBMT is more appreciated among users that are nonprofessional computers users. As such, the results do motivate further research into the actual effects of CBMT, especially compared to other methods of information security training.

An important note to make is that this study measured how CBMT is appreciated by users. The study is not concerned with the actual results of the different training methods. While one can argue that it is important for a training method to be appreciated by its users, one planned direction for further research is to actually use CBMT as a method of information security training in a real-world setting for which this was a pilot study. It should also be mentioned that this study was completed in a laboratory environment rather than in a real-world setting. Thus, another direction for future work would be to repeat this study in a real-world case with a larger sample. A future study should also look into differences among demographic groups, a factor that was not considered in this pilot study.

6 References


PAPER 3: USING CONTEXT BASED MICRO TRAINING TO DEVELOP OER FOR THE BENEFIT OF ALL

Using Context Based MicroTraining to develop OER for the benefit of all

Joakim Kävrestad  
University of Skövde  
Skövde, Sweden  
joakim.kavrestad@his.se

Marcus Nohlberg  
University of Skövde  
Skövde, Sweden  
marcus.nohlberg@his.se

ABSTRACT
This paper demonstrates how Context Based MicroTraining (CBMT) can be used to develop open educational resources in a way that benefits students enrolled in university courses as well as anyone who wants to participate in open-learning activities. CBMT is a framework that provides guidelines for how educational resources should be structured. CBMT stipulates that information should be presented in short sequences and that is relevant for the learner’s current situation. In this paper, CBMT is implemented in a practical ICT course using video lectures that are delivered as open educational resources using YouTube. The experiences of enrolled students as well as YouTube users are evaluated as well as the actual results of the enrolled students. The results of the study suggest that users of the video lectures appreciate the learning approach. The actual results, i.e. learning outcomes, of the enrolled students are maintained. The study also demonstrates how using CBMT as open educational resources can free up time for teachers and increase the quality of teaching by benefitting from community feedback.

Author Keywords
Open-learning; OER; Context Based MicroTraining; on-demand learning; higher education; nanolearning

ACM Classification Keywords
H4.0: General
K.3: COMPUTERS AND EDUCATION
K4.0: General

INTRODUCTION
Openness in higher education is a phenomenon that has grown in popularity and debate in recent years, globally as well as in the EU. In the report “Opening up Education”, published by the European Commission, Inamorato dos Santos and Punie [1] describe that opening up education is important for several reasons. Those reasons include making it easier and cheaper for learners to access education and that open learning helps modernize higher education, since open learning is commonly carried out using digital techniques.

The Open Education Consortium [2] describes open education as follows:
“Open education encompasses resources, tools and practices that employ a framework of open sharing to improve educational access and effectiveness worldwide.”

Cronin [3] discusses this definition further and finds that open education is an ambiguous term than can mean different things including the following:

- Open Admission
- Open as in free
- Open Educational Resources
- Open Educational practices

The reminder of this paper will concern Open Educational Resources (OER) that are defined by UNESCO [4] as:
“teaching, learning and research materials in any medium, digital or otherwise, that reside in the public domain or have been released under an open license that permits no-cost access, use, adaptation and redistribution by others with no or limited restrictions. Open licensing is built within the existing framework of intellectual property rights as defined by relevant international conventions and respects the authorship of the work”

Butcher [7] states that OER can help improve education across the world and that they are an important tool in providing education in developing countries where access to resources and classrooms may be limited.

While creating and distributing OER undoubtedly offers lots of benefits to a lot of people, there are concerns that needs to be addressed. In a paper discussing Massive Open Online Courses (MOOC), Yuan, Powell [6] discusses if MOOCs follow a sound pedagogical approach that leads to quality learning for the students and recognizes that MOOCs generally lack quality assurance controls.

In the topic of quality assurance, Butcher [7] states that quality assurance is up to the provider of education. He also argues that when an institution is publishing OER they have strong incentives of ensuring quality as the quality of the OER will reflect on the institution. Looking from the
providers point of view, Hylén [8] describes that a common argument for using OER is that OER enable community feedback that can in turn raise the quality of teaching material. Using that idea, a teacher could benefit from transforming material used in closed campus courses into OER as a quality assurance task.

In this paper, we explore how teaching material in closed campus courses can be distributed to campus students, and the general public as OER. This is done by proposing and evaluating a framework for creating OER that can be widely spread in the public domain while serving as a teaching method for student enrolled in campus courses. The framework is called Context Based MicroTraining (CBMT) and can be implemented to facilitate open on-demand learning. This paper demonstrates how CBMT can be distributed as OER and used for teaching students enrolled in campus courses. Further, the paper evaluates how students in ICT experience using CBMT over traditional classroom teaching and the impact of the teaching method on student’s results. As such, the study demonstrates a pedagogical approach to creating OER and addresses the general concerns about quality in open-learning.

The upcoming section will describe CBMT and the theoretical background to CBMT in detail while the upcoming section of this paper will in turn, describe the addressed research questions and methodology used in this paper as well as the results and conclusions of this study.

CONTEXT BASED MICROTRAINING (CBMT)

The concept of CBMT is based on the notion that people need motivation in order to learn. The idea here is that the likelihood that any adult will learn is increased if the knowledge seems meaningful for the learner [9]. This notion is based on the concept of andragogy as presented by Knowles [10]. Knowles [10] argues that an adult learner needs to be motivated in order to learn. That motivation can be external in the sense that you apply for a course to further your knowledge but it is also possible for the teacher to increase the motivation of the learner by using different techniques. As discussed by Hult [11], one such way is to adjust the examination of a course so that it supports learning instead of being a check of student knowledge regarding central concepts. The foundation in this way of thinking is that the learner will learn better if the knowledge presented seems meaningful. One way to accomplish this is to present the knowledge in a context where it is applicable. As discussed by Herrington and Oliver [12], presenting knowledge to learners in a situation where the knowledge is applicable will cause a more meaningful learning experience. This is the first requirement that CBMT tries to facilitate.

Further, an obstacle in the sense of providing the computer user with knowledge about information security has been to make the users participate in education. One technique that has gained an increasing interest in the past years is microlearning or similar strategies including nanolearning and micro-training. As described by Wang, Xiao [13], nanolearning is a teaching method where information is presented in short sequences. The idea is to facilitate just-in-time learning meaning that information is provided in small chunks, thus making the time needed to absorb the information short and in an on-demand fashion [14]. As described by Bruck, Motiwalla [15], there has been research showing positive results of microlearning both in terms of learner participation and satisfaction. Microtraining is the second fundamental building block of Context Based MicroTraining.

On a practical note, CBMT can be described as a framework that describes learning objects from two directions. The first direction concerns the delivery of the learning objects and states that the learning objects should be short sequences delivered in an on-demand fashion. On-demand learning object has the properties of not being tied to a person or location making it easy to distribute them as OER.

The second direction concerns the content of the learning objects. In this respect, CBMT demands that the information presented in a learning module is of immediate use to the learner and therefore assumes that the information is relevant to the learner in the learner’s current context. In this respect, CBMT tries to facilitate the concept of “learn by doing” theories that can be summarized as a describing that learners learn better when they perform tasks instead of just reading [16]. CBMT is also a learning method that includes aspects of problem-based learning (PBL) in that it is designed to guide the learner through real-world tasks[17]. In summary, the meaningfulness is achieved by the learner doing some task related to his or her situation.

Given the discussion in the previous sections, CBMT is a teaching method where information is provided in small segments to the learner. Further, the information presented is relevant for the learner in his or her current situation. A simple way of modeling CBMT is provided in Figure 1.

**Figure 1 conceptual model of CBMT**

Looking at the abstract model in Figure 1, CBMT begins with a learner entering a situation or starting a task. For the sake of this description that situation can be that the learner opens an e-mail containing a link. Based on this situation, the learner is presented to a learning module with short information relating to the current situation. In this example, it could be information telling the learner not to enter account information into links sent via e-mail or to verify that the e-mail address of the sender matches the source that the e-mail appears to be from. The learner is then supposed to carry on with the task, in this case reading and reacting to the e-mail. As such, CBMT is a process where the central concept is that the information presented is relevant for the situation that the learner is in. The actual format that the information that is presented in is not specified in detail by CBMT but should
comply with the ideas of nanolearning, namely facilitate just-in-time learning while the learner can maintain interest in the information.

As for the actual implementation of CBMT, there are two distinct ways in which it can be done. In the context of teaching computer users about information security, it would seem feasible to have a software monitor what is happening on the user's computer and present the learning modules whenever the users enter a situation or perform an action where he or she needs the information. In this case, you would rely on the computer to decide when the user is entering a context where the information is applicable. The implementation of CBMT in such a scenario is modeled in Figure 2.

The case in Figure 2 assumes that CBMT is used to combat online fraud. In this scenario, a computer would evaluate when to detect that a user enters a situation than the user is at risk of meeting a fraudster. If so, the computer will present information to the user so that she can handle the situation.

In the context of higher education, we realize that automatic detection is hard to achieve because of the wider range of subjects. A more feasible way to implement CBMT would be to provide the learner with a task and a series of learning modules. The task would include a number of steps where the student is supposed to use a learning module before working with a step of the task. In a simplified scenario where a carpeting student is supposed to learn how to build a table you could divide the task into several smaller activities:

1. Measure
2. Cut
3. Screw together

You would then create nanolearning modules for each activity and let the student do module one just before doing activity one, then the student does module two before embarking on activity two and so on. In this scenario, you would present the learning modules on an on-demand basis rather than in an automated fashion. The process is visualized in Figure 3.

Figure 2 CBMT used to combat online fraud

The case in Figure 2 assumes that CBMT is used to combat online fraud. In this scenario, a computer would evaluate when to detect that a user enters a situation than the user is at risk of meeting a fraudster. If so, the computer will present information to the user so that she can handle the situation.

In the context of higher education, we realize that automatic detection is hard to achieve because of the wider range of subjects. A more feasible way to implement CBMT would be to provide the learner with a task and a series of learning modules. The task would include a number of steps where the student is supposed to use a learning module before working with a step of the task. In a simplified scenario where a carpeting student is supposed to learn how to build a table you could divide the task into several smaller activities:

1. Measure
2. Cut
3. Screw together

You would then create nanolearning modules for each activity and let the student do module one just before doing activity one, then the student does module two before embarking on activity two and so on. In this scenario, you would present the learning modules on an on-demand basis rather than in an automated fashion. The process is visualized in Figure 3.

Figure 3 CBMT in education

As described by Kävrestad and Nohlberg [18], context based micro training has been evaluated as a way to teach Internet users about online fraud schemes with positive results. The method was further explored in the same context by Werme [19] with similar results. A more recent thesis by Skärgård [20] evaluated context based micro training as a method to teach information security in general and found that the method was appreciated by the users.

To summarize, CBMT is a learning method where short sequences of information are presented to the learner in a context where it is of direct relevance to the learner. The teaching method is similar to nanolearning. As described by Wang, Xiao [13], nanolearning is a teaching method where information is presented in short sequences. The difference between nanolearning and context based microtraining is that context based microtraining also present the information in a context where it is of relevance to the learner. Another difference is that CBMT in itself encourages the learner to immediately use the information presented to her. Thus, CBMT encourages retrieval of information, an important factor in learning [21].

MOTIVATION AND RESEARCH AIM

Creating and distributing OER as a part of teaching in higher education can bring several benefits to the global community, as discussed in the introduction. However, the main role of any teacher in higher education is to ensure the best education possible for the students enrolled in his or her courses. Further, the constraint of time causes a scenario where it would be ideal to incorporate creation of OER into the courses held for enrolled students rather than creating OER not connected to any course.

In this paper, we demonstrate how a practical university level course can be built around OER designed according to the CBMT framework. We then evaluate the student’s perception of learning with the use of the CBMT learning modules instead of traditional classroom teaching. Since the actual learning outcomes are usually the student’s grades, we evaluate the performance of the student’s in relation to previous years of the same course to ensure that the use of CBMT does not impact the student’s results in a negative way. Finally, we evaluate the community usage and feedback that was given from users of the OER, via YouTube. The research questions explored in this paper are the following:

- Q1: What impact will using CBMT over classroom lectures have on student’s results?
Q2: What is the students’ experience of using CBMT over classroom lectures?
Q3: How are OER based on CBMT perceived by the global community?

While the benefits delivering learning modules as OER are obviously that they contribute to the pool of open learning we also expect two benefits for the enrolled students as well. First, the presented literature suggests that context based micro training can be a teaching method that provides the learner with a more meaningful learning experience as compared to lectures and written examination. Second, one way to implement context based microtraining is through on-demand services using, for instance, recorded video lectures. As video lectures can be reused once they are created, CBMT ensures that the learners can reuse the learning modules as often as they want while the teacher can save time that can be used for other in-person learning activities, such as seminars or supervision.

**METHODOLOGY**

The methodology in this study is based on a real-world scenario where the research questions are addressed by implementing CBMT modules, distributor as OER using YouTube, in a setting with actual students that will study a practical topic that is new to them. As this study evaluates CBMT in a new context it is possible that using CBMT will have a negative impact on the student’s ability to complete a course. Thus, a pilot testing of CBMT in a controlled environment was conducted and following positive results of the pilot, CBMT was implemented in an actual course. The research process is visualized in Figure 4 below.

**Figure 4 Research process overview**

For the pilot, students from the third year of the Bachelor Degree study program Networks and Systems administration was invited to participate. The participants were split into two groups randomly, A and B. Group A was taught using traditional classroom teaching and group B was taught using Context Based MicroTraining. All participants were then be handed a test with a practical and theoretical part and the test scores from the two groups were compared. The practical test was taken from Cisco Networking Academy. Cisco Networking Academy delivers curriculum and tests to a multitude of teaching institutions around the globe. The theoretical quiz was developed by one of the researchers who has several years of experience in teaching in the subject area and is a certified Cisco Academy Instructor. Finally, a qualitative survey was sent out to the participants from group B. The purpose of the survey was to analyze how the participants perceived CBMT as a teaching method. The survey was designed to mimic semi-structured interviews as described by Robson and McCartan [22]. One could argue that in-person interviews would be a better method but since the participants in this study are students studying under the researchers, anonymous surveys were deemed to be a better
method in order to minimize bias. We argue that a face-to-face interview could impact the participants’ willingness to provide honest answers, especially if they dislike the teaching method.

Following successful results from the pilot, as outlined in the results section of this paper, the research process continued with the implementation of CBMT in an actual course. The course used for this was a course in data communication and the material thought is delivered by Cisco Networking Essentials. The course has been running for several years using traditional lectured combined with supervision where the students could practice the practical aspects of the course. During this study, the course was modified by exchanging the classroom lectures for recorded lectured developed according to the principles of CBMT. Further, a session where the student was invited to study and discuss the theoretical material was scheduled. The course was examined using a theoretical exam and a practical exam in which the students need to fully understand the course content. After the course, the students were asked to answer a survey containing Likert-type questions designed to measure their experience of using CBMT. Also, the student's results from the examination were compared with the results from the previous run of the course. In an attempt to evaluate the usefulness of the learning modules for the global community, the usage statistics and feedback from YouTube was recorded and presented. Also, the total number of positive and negative feedback objects was recorded as an attempt to evaluate the perception of the learning modules from the global community.

RESULTS FROM THE PILOT

This section details the actual execution of the pilot and presents the results in this step of the research process. Prior to the tests and the survey, the participants received teaching, Group A had a lecture and group B worked with a learning module designed according to the principles of CBMT. To mimic a realistic setting, all participants gained access to written course material and practical training exercises. The material was the same material that is used in Cisco Academy courses and covered a data communication technology called BGP (Border Gateway Protocol).

Test

The first step in measuring the effects of CBMT was to give the participant an actual test containing a practical part where they had to configure BGP and a theoretical part with questions about BGP. The theoretical part contained questions that could be a part of a real examination and was developed by one of the authors, who is a certified Cisco Academy Instructor. The practical test was a standardized test developed by Cisco.

The theoretical test consisted of seven multiple choice question that each gave one point, thus the participants could score a maximum of seven points. The practical part was graded pass or fail. Further, the time spent by the participants to take the test was also recorded. The results of the test are presented in Table 1 below.

As seen in Table 1 above, the average results for the group that used CBMT were marginally better for the theoretical as well as for the practical task. However, due to the small sample, it is hard to eliminate chance as a reason for the difference. Looking at time spent to do the test, it is clear that group B, that used CBMT needed less time, in fact the average time spent to do the test for the participant in group B was close to half the average time spent by the participants from group A. Further, the slowest participant in group B was about 25% faster than the fastest participant from group A. The difference in needed time could indicate that the participants from group B were more confident when completing the test. Overall, the results from the test indicate that CBMT provides at least as good learning outcomes as traditional classroom teaching when used to teach practical skills. Further, the difference in score and needed time indicates that CBMT produces higher learning outcomes when used to teach practical skills.

Survey

To analyze how the learners perceived CBMT, a qualitative survey was used to ask the participants in group B about their experience with CBMT. The surveys were conducted in English using google forms to ensure the anonymity of the participants. The survey contained the following questions:

Q1: How was your experience of using CBMT in this course?

Q2: What benefits do you see of using CBMT compared to traditional classroom teaching?

<table>
<thead>
<tr>
<th>Group</th>
<th>Theoretical score</th>
<th>Practical score</th>
<th>Time (min)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A - Traditional</td>
<td>6</td>
<td>Pass</td>
<td>21</td>
</tr>
<tr>
<td>A - Traditional</td>
<td>7</td>
<td>Pass</td>
<td>25</td>
</tr>
<tr>
<td>A - Traditional</td>
<td>7</td>
<td>Pass</td>
<td>20</td>
</tr>
<tr>
<td>A - Traditional</td>
<td>4</td>
<td>Fail</td>
<td>28</td>
</tr>
<tr>
<td>Group A Average</td>
<td>6</td>
<td></td>
<td>23,5</td>
</tr>
<tr>
<td>B - CBMT</td>
<td>7</td>
<td>Pass</td>
<td>15</td>
</tr>
<tr>
<td>B - CBMT</td>
<td>7</td>
<td>Pass</td>
<td>8</td>
</tr>
<tr>
<td>B - CBMT</td>
<td>7</td>
<td>Pass</td>
<td>10</td>
</tr>
<tr>
<td>B - CBMT</td>
<td>6</td>
<td>Pass</td>
<td>15</td>
</tr>
<tr>
<td>Group B Average</td>
<td>6,75</td>
<td></td>
<td>12</td>
</tr>
</tbody>
</table>
Q3: What downsides do you see of using CBMT compared to traditional classroom teaching?

Q4: Do you see any other courses where CBMT could be beneficial and in that case which?

Q5: Do you see any other situations where CBMT could be used and if so which?

Q6: Do you have any further comments about CBMT and the study?

The survey was preceded by the following informational text:

“You recently participated in a study about the use of Context Based MicroTraining (CBMT) in higher education. This survey is sent out to the participants that used CBMT in the study. We would much appreciate if you answered the five questions in the survey, your answers will be anonymous and you may end the survey at any time. As far as possible, relate your answers to the CBMT teaching method rather than the actual content provided in this study. The purpose of the surveys is for us as researchers to gain a deeper understanding about how you as students perceives the use of CBMT, positive as well as negative aspects.

As background, the purpose of CBMT is to provide knowledge in a situation where the knowledge is of relevance to learner, for instance in a scenario where the knowledge will be applied in a practical exercise or a real-life situation. Further, the idea of CBMT is to rely on re-usable, on-demand and short sequences of information that could, for instance, be provided as video lectures or games.

The results of the study will be published in scientific forums, if you wish to gain access to the results or have any other questions about the study, contact Author at email”

The results from the survey are presented in Table 2. The first column identifies the question number (Qn), the second column identifies the respondent by number (Rn) and the third column shows the answer. One respondent answered the survey in Swedish, the answers have been translated into English and are written in italic in Table 2. The answers are presented exactly as they were given.

Table 2 Survey Answers (pilot) Survey answers Note from the authors: NSA is an abbreviation for the Networks and Systems Administrations study program and the course mentioned are courses in that program.

<table>
<thead>
<tr>
<th>Qn</th>
<th>Resp.</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1</td>
<td>R1</td>
<td>I thought it worked really well. I learn while doing so this really worked for me.</td>
</tr>
<tr>
<td>Q1</td>
<td>R2</td>
<td>It was an interesting way to learn, practical practice and presentation of theory combined.</td>
</tr>
<tr>
<td>Q1</td>
<td>R3</td>
<td>Good.</td>
</tr>
<tr>
<td>Q1</td>
<td>R4</td>
<td>Good</td>
</tr>
<tr>
<td>Q2</td>
<td>R1</td>
<td>I think that CBMT has the advantage of making it available for the student to follow along the teacher both during course literature and during practical exercises. Teaching can also be &quot;on-the-fly&quot; without the restraints of the classic classroom.</td>
</tr>
<tr>
<td>Q2</td>
<td>R2</td>
<td>Easier to maintain focus when theory is mixed with practice, I also find it easier to learn while doing something myself.</td>
</tr>
<tr>
<td>Q2</td>
<td>R3</td>
<td>Possible to view the learning material multiple times and learn by doing at the same time.</td>
</tr>
<tr>
<td>Q2</td>
<td>R4</td>
<td>You can follow along with what the teacher does. Possible to pause or rewind. Possible to look at the material anytime you want.</td>
</tr>
<tr>
<td>Q3</td>
<td>R1</td>
<td>I would imagine that CBMT would be less efficient for people who have a hard time motivating themselves to study. Without the requirements of actually being in a classroom, other distractions when the student is at home, for example, could prove challenging for some.</td>
</tr>
<tr>
<td>Q3</td>
<td>R2</td>
<td>Can be hard to use in non-technical courses that are not very practical</td>
</tr>
<tr>
<td>Q3</td>
<td>R3</td>
<td>Lack of contact with persons with knowledge. Should be combined in some form with traditional teaching.</td>
</tr>
<tr>
<td>Q3</td>
<td>R4</td>
<td>Some student might procrastinate and view the video at a later time. As opposed to lectures that are at a specific point in time.</td>
</tr>
<tr>
<td>Q4</td>
<td>R1</td>
<td>All practical courses, where the student can follow along the teacher as the teacher does the exact same exercises as the students do. Having the ability to pause and go back helps tremendously, which is not always the case with traditional classroom teaching.</td>
</tr>
<tr>
<td>Q4</td>
<td>R2</td>
<td>I think it can be adopted in any courses that contain practical element. That includes almost all NSA courses especially databases, script and so on where you can practice small parts and then end with some bigger task that involves the just finished small parts. It may also be usable in courses like Linux</td>
</tr>
</tbody>
</table>
and Windows where you can do something while you see how it is done.

Q4 R3 Courses with practical elements should all benefit from this.

Q4 R4 Most practical courses (Scripting, Linux/Windows Admin, Datacom, IP telephony, Database Systems, Computer Fundamentals)

Q5 R2 When you search for information about, for instance, how to configure something, like a web server. In these cases I find it common to read step by step or watch a movie and configure the web server as you go.

Q5 R3 Probably in many situations where some sort of learning is present.

Q6 R2 It would be interesting to test during a longer period with deeper material since I think than more people than you think uses it.

Q6 R3 No.

Looking at the responses from Q1 and Q2, the respondents all state that using CBMT was a positive experience and some positive effects of using CBMT instead of traditional classroom teaching are mentioned. These include the possibility to reuse the material and the fact that CBMT enables you to work with a practical task and the theoretical material at once. As previously described, this is one of the main targets with CBMT. Looking to Q3 where the respondent could express downsides with CBMT, they mention that one problematic aspect can be that it is easier to procrastinate when you as a learner have the full responsibility to actually study. In that sense, a scheduled lecture can increase the chance of the learner actually attending at all. One respondent also mentions that a lack of contact with the teacher could be overcome by combining it with some other teaching activity.

Looking at the answers to Q4 and Q5, the participants suggest that courses with practical content could benefit from using CBMT. It is also suggested that CBMT could be used in other learning situations outside of the classroom. In summary, the survey shows that the participants in this study appreciated using CBMT as a learning method for practical content. They argue that the fact that CBMT allows for a learning-by-doing apprise and that the material is available on-demand is beneficial and preferable to traditional classroom teaching even if they also state that the lack of teacher attendance can be an issue, especially for students with procrastination behavior. Thus, even if there are concerns that have to be addressed when using CBMT in higher learning, the survey does indicate that CBMT can provide a more meaningful learning experience compared to traditional classroom teaching.

RESULTS FROM IMPLEMENTING CBMT IN AN ACTUAL COURSE

Following the positive results from the pilot, CBMT was implemented in an actual course, which was the first of three connected courses. The course was previously taught using classroom lectures and self-studies supported by supervised sessions where the students could practice the practical parts of the course. In this study, the lectures were delivered using recorded lectures developed according to the principles of CBMT. The students were also scheduled for supervision where they could work with the lectures and ask questions on the material as needed. The course ended with an examination consisting of a practical test and a theoretical test. The material taught in this course is standardized material developed by Cisco Networking material, the lectures and the tests were designed by one of the authors, who is a certified Cisco Academy Instructor. Following the examination, the students were asked to fill out a survey on how they perceived CBMT as a teaching method.

The results from the examination, with 28 participants, was compared to the results from the previous run of the course, with 23 participants. In the group of students using CBMT (heron called CBMT), 77% of the students passed the practical test compared with 79% in the previous year (heron called previous). As for the theoretical test 90% the CBMT students passed with an average score of 77% compared with the previous students were 88% passed with an average score of 75% percent. There results indicates that the use of CBMT had no or negligible impact on the students results.

Following the examination the students were handed a survey with questions about how they perceived using CBMT, all students answered the survey. The first four questions were Likert-style questions where the students were asked to rate 4 statements of a five graded scale where 5 was labeled “Fully agree” and 1 was labeled “Do not agree at all”. The questions and average response values are presented in Figure 5 below.

Looking at the answers from Q1 and Q2, the respondents all state that using CBMT was a positive experience and some positive effects of using CBMT instead of traditional classroom teaching are mentioned. These include the possibility to reuse the material and the fact that CBMT enables you to work with a practical task and the theoretical material at once. As previously described, this is one of the main targets with CBMT. Looking to Q3 where the respondent could express downsides with CBMT, they mention that one problematic aspect can be that it is easier to procrastinate when you as a learner have the full responsibility to actually study. In that sense, a scheduled lecture can increase the chance of the learner actually attending at all. One respondent also mentions that a lack of contact with the teacher could be overcome by combining it with some other teaching activity.

Looking at the answers to Q4 and Q5, the participants suggest that courses with practical content could benefit from using CBMT. It is also suggested that CBMT could be used in other learning situations outside of the classroom. In summary, the survey shows that the participants in this study appreciated using CBMT as a learning method for practical content. They argue that the fact that CBMT allows for a learning-by-doing apprise and that the material is available on-demand is beneficial and preferable to traditional classroom teaching even if they also state that the lack of teacher attendance can be an issue, especially for students with procrastination behavior. Thus, even if there are concerns that have to be addressed when using CBMT in higher learning, the survey does indicate that CBMT can provide a more meaningful learning experience compared to traditional classroom teaching.

RESULTS FROM IMPLEMENTING CBMT IN AN ACTUAL COURSE

Following the positive results from the pilot, CBMT was implemented in an actual course, which was the first of three connected courses. The course was previously taught using classroom lectures and self-studies supported by supervised sessions where the students could practice the practical parts of the course. In this study, the lectures were delivered using recorded lectures developed according to the principles of CBMT. The students were also scheduled for supervision where they could work with the lectures and ask questions on the material as needed. The course ended with an examination consisting of a practical test and a theoretical test. The material taught in this course is standardized material developed by Cisco Networking material, the lectures and the tests were designed by one of the authors, who is a certified Cisco Academy Instructor. Following the examination, the students were asked to fill out a survey on how they perceived CBMT as a teaching method.

The results from the examination, with 28 participants, was compared to the results from the previous run of the course, with 23 participants. In the group of students using CBMT (heron called CBMT), 77% of the students passed the practical test compared with 79% in the previous year (heron called previous). As for the theoretical test 90% the CBMT students passed with an average score of 77% compared with the previous students were 88% passed with an average score of 75% percent. There results indicates that the use of CBMT had no or negligible impact on the students results.

Following the examination the students were handed a survey with questions about how they perceived using CBMT, all students answered the survey. The first four questions were Likert-style questions where the students were asked to rate 4 statements of a five graded scale where 5 was labeled “Fully agree” and 1 was labeled “Do not agree at all”. The questions and average response values are presented in Figure 5 below.

Looking at the answers from Q1 and Q2, the respondents all state that using CBMT was a positive experience and some positive effects of using CBMT instead of traditional classroom teaching are mentioned. These include the possibility to reuse the material and the fact that CBMT enables you to work with a practical task and the theoretical material at once. As previously described, this is one of the main targets with CBMT. Looking to Q3 where the respondent could express downsides with CBMT, they mention that one problematic aspect can be that it is easier to procrastinate when you as a learner have the full responsibility to actually study. In that sense, a scheduled lecture can increase the chance of the learner actually attending at all. One respondent also mentions that a lack of contact with the teacher could be overcome by combining it with some other teaching activity.

Looking at the answers to Q4 and Q5, the participants suggest that courses with practical content could benefit from using CBMT. It is also suggested that CBMT could be used in other learning situations outside of the classroom. In summary, the survey shows that the participants in this study appreciated using CBMT as a learning method for practical content. They argue that the fact that CBMT allows for a learning-by-doing apprise and that the material is available on-demand is beneficial and preferable to traditional classroom teaching even if they also state that the lack of teacher attendance can be an issue, especially for students with procrastination behavior. Thus, even if there are concerns that have to be addressed when using CBMT in higher learning, the survey does indicate that CBMT can provide a more meaningful learning experience compared to traditional classroom teaching.

RESULTS FROM IMPLEMENTING CBMT IN AN ACTUAL COURSE

Following the positive results from the pilot, CBMT was implemented in an actual course, which was the first of three connected courses. The course was previously taught using classroom lectures and self-studies supported by supervised sessions where the students could practice the practical parts of the course. In this study, the lectures were delivered using recorded lectures developed according to the principles of CBMT. The students were also scheduled for supervision where they could work with the lectures and ask questions on the material as needed. The course ended with an examination consisting of a practical test and a theoretical test. The material taught in this course is standardized material developed by Cisco Networking material, the lectures and the tests were designed by one of the authors, who is a certified Cisco Academy Instructor. Following the examination, the students were asked to fill out a survey on how they perceived CBMT as a teaching method.

The results from the examination, with 28 participants, was compared to the results from the previous run of the course, with 23 participants. In the group of students using CBMT (heron called CBMT), 77% of the students passed the practical test compared with 79% in the previous year (heron called previous). As for the theoretical test 90% the CBMT students passed with an average score of 77% compared with the previous students were 88% passed with an average score of 75% percent. There results indicates that the use of CBMT had no or negligible impact on the students results.

Following the examination the students were handed a survey with questions about how they perceived using CBMT, all students answered the survey. The first four questions were Likert-style questions where the students were asked to rate 4 statements of a five graded scale where 5 was labeled “Fully agree” and 1 was labeled “Do not agree at all”. The questions and average response values are presented in Figure 5 below.

Figure 5 Answers for the first survey question

As seen in Figure 5, the answers to the questions clearly show that students appreciated using the video lectures in this course. The next section of the survey measured how the
students used the lectures. The course contained 10 recorded lectures that all contained practical elements. As seen in Figure 6, 75% of the students used 9 or 10 of the lectures.

Figure 6 self-reported lecture usage
Figure 6 shows that a majority of the students used most of the recorded video lectures.

The next question measured how frequently the students completed the practical elements in the lectures, the answers are presented in Figure 7 below. The results for this question shows that 57% of the students completed most or all practical elements and only 7% of the respondents report that they did not complete any of the practical elements.

Figure 7 self-reported engagement in practical elements
As a final question the students were asked to choose if they preferred to be taught using video lectures or classroom lectures and as seen in Figure 8, 92,9% of the participants preferred video lectures.

Figure 8 Video lectures vs. class room lectures
Evaluation of external usage of OER
The above mentioned evaluation was based on a course that was the first of three connected courses that was all thought using CBMT video lectures distributed as OER using YouTube. This section presents usage statistics and analysis of feedback given from the users of the OER on YouTube. The usage statistics are presented in Table 3. The Lectures are name Cx-n, where x is the course they was used in, C1 being the course that was the basis of the just presented evaluation, and n is the lecture number. C1 was published in the end of June 2018, C2 in the end of July 2018 and C3 in the middle of January 2019.

Table 3 OER usage statistics
<table>
<thead>
<tr>
<th>Lecture number</th>
<th>Views</th>
<th>Thumbs up</th>
<th>Thumbs down</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1-1</td>
<td>373</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>C1-2</td>
<td>153</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>C1-3</td>
<td>209</td>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>C1-4</td>
<td>112</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>C1-5</td>
<td>113</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>C1-6</td>
<td>123</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>C1-7</td>
<td>120</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>C1-8</td>
<td>93</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>C1-9</td>
<td>94</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>C1-10</td>
<td>116</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>C2-1</td>
<td>992</td>
<td>17</td>
<td>0</td>
</tr>
<tr>
<td>C2-2</td>
<td>396</td>
<td>11</td>
<td>0</td>
</tr>
<tr>
<td>C2-3</td>
<td>245</td>
<td>7</td>
<td>0</td>
</tr>
<tr>
<td>C2-4</td>
<td>257</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>C2-5</td>
<td>211</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>C2-6</td>
<td>887</td>
<td>12</td>
<td>0</td>
</tr>
<tr>
<td>C2-7</td>
<td>412</td>
<td>11</td>
<td>0</td>
</tr>
<tr>
<td>C2-8</td>
<td>452</td>
<td>18</td>
<td>0</td>
</tr>
<tr>
<td>C2-9</td>
<td>386</td>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td>C2-10</td>
<td>377</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>C3-1</td>
<td>107</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>C3-2</td>
<td>84</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>C3-3</td>
<td>71</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>C3-4</td>
<td>41</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>C3-5</td>
<td>43</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>C3-6</td>
<td>37</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>C3-7</td>
<td>39</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>C3-8</td>
<td>48</td>
<td>4</td>
<td>0</td>
</tr>
</tbody>
</table>

As seen in table 3, the lectures was viewed between 39 and 992 times, leaving a big span that can to some extent be explained by the publishing dates. While the views counters is a blunt measurement that includes views from enrolled students the numbers show that others than the enrolled students made use of the OER. Further, the fact that all lectures received some like and only one video received one dislike, in some way, an indication that the learning modules was appreciated by the community as a group.
The notion that the videos was appreciated by the community is strengthened by the fact that two comments to the videos in C2 asked for videos for C3 before they were posted, and an additional five positive comments was received to the lectures in C2.

Further, comments for two lectures mentioned errors in the lectures. Following those comments, the lectures was corrected and the old ones deleted. This process demonstrates how OER can benefit from community feedback and increase the quality of the teaching.

CONCLUSIONS

CBMT is a teaching method originally developed to teach information security. The purpose of this paper was to evaluate if CBMT can also be used as a teaching method in higher education, for practical courses while generating learning objects distributed as OER. In this study, CBMT was used in a pilot test with third-year students from the study program Networks and Systems administration. Following successful results in the pilot, CBMT was implemented as the teaching method in an actual course. In the pilot and the actual course, CBMT was evaluated by measuring the actual performance of the students and by evaluating the student’s experience of using CBMT compared to traditional classroom teaching. All learning modules was distributed as OER using YouTube and the usage of the learning modules was recorded.

The first research question addressed in this study was “What impact will using CBMT over classroom lectures have on student’s results?” During the pilot, the group using CBMT scored marginally better than the group that was thought using classroom teaching. However, when implementing CBMT in an actual course the exam scores were comparable with exam scores from the previous run of the course.

The second question addressed in this study was “What is the students’ experience of using CBMT over classroom lectures?”. This question was addressed in the pilot with a qualitative survey that indicated that students would prefer using CMBT over traditional classroom lectures. The pilot also suggested that CBMT should be well-fitted for practical courses. Similar results were obtained using a Likert-style survey to measure how the students that used CBMT in an actual course perceived CBMT. In that survey, the respondents reported that using video lectures designed according to the principles of CBMT, encouraged them to do practical tasks, motivated them in their studies and fitted well for the course content. Further, over 90% of the respondents reported that they preferred the video lectures over traditional classroom lectures. Thus, the study shows that students prefer using CBMT based video lectures over classroom lectures for practical courses.

The final question addressed in this study was “How are OER based on CBMT perceived by the global community?”. This question was answered by usage statistics from YouTube, there the OER was published, and user comments to the OER. While the instrumentation, analyzing views and reactions, must be considered blunt, the usage statistics suggests that the OER was used and appreciated by the community users. Further analysis of the comments does, even if they were few, emphasize this notion. Also, some comments pointed out errors in the OER leading to them being corrected and reposted which benefited the community users as well as the enrolled campus students.

This study examined how enrolled student experiences learning with learning modules designed according to the CBMT framework and distributed as OER. Usage statistics tracked on YouTube revealed that the learning modules was used by others than the enrolled students and since mostly positive feedback was given on YouTube, some indication was given that the learning modules was appreciated by the global community. However, the actual learning outcomes of others than enrolled students were not measured in this study.

In conclusion, this study does suggest that CBMT can indeed be a useful teaching method in higher education while generating OER useful for the global community. In this particular study, the participant's results were not affected negatively by using CBMT over traditional classroom teaching. However, it is important to notice that using recorded material can free up substantial time for the teacher and is reusable between different runs of the course. It also makes it possible to make the lectures publicly available as OER and thus, contribute to the life-long learning and the global pool of open-learning. Further, it is evident that the students participating in this study clearly preferred CBMT over classroom teaching making CBMT a teaching method that is feasible for use in practical courses in higher education.

FUTURE WORK

The results of this study suggest that CBMT can be an effective teaching method in higher education. However, the answers from the surveys also suggest that one could not completely substitute the teacher with CBMT modules. It is, of course, reasonable to argue that access to the teacher is of great value to the learning outcomes and experience in any course. Given our results, a direction for future work would be to implement and evaluate CBMT in a wider range of courses and in different subject matters.

Another note is that we did not at all examine the learning outcomes of those that was using the OERs but not enrolled in the course that functioned as test group. While we demonstrated how learning modules can be delivered as OER with positive effects for enrolled students using them, a direction for future work would be to examine the learning outcomes for those not enrolled in a course, or the course that the OERs was specifically designed for.

We are happy to provide the material that we used for other researchers to use and be inspired by.
REFERENCES


[7] Butcher, N., *A basic guide to open educational resources (OER)*. 2015: Commonwealth of Learning (COL):.


---


PAPER 4: ASSISTING USERS TO CREATE STRONGER PASSWORDS USING CONTEXTBASED MICROTRAINING

Assisting Users to Create Stronger Passwords Using ContextBased MicroTraining

Joakim Kävrestad and Marcus Nohlberg
University of Skövde, Skövde, Sweden
{joakim.kavrestad,marcus.nohlberg}@his.se

Abstract. In this paper, we describe and evaluate how the learning framework ContextBased MicroTraining (CBMT) can be used to assist users to create strong passwords. Rather than a technical enforcing measure, CBMT is a framework that provides information security training to users when they are in a situation where the training is directly relevant. The study is carried out in two steps. First, a survey is used to measure how well users understand password guidelines that are presented in different ways. The second part measures how using CBMT to present password guidelines affect the strength of the passwords created. This experiment was carried out by implementing CBMT at the account registration page of a local internet service provider and observing the results on user-created passwords. The results of the study show that users presented with passwords creation guidelines using a CBMT learning module do understand the password creation guidelines to a higher degree than other users. Further, the experiment shows that users presented with password guidelines in the form of a CBMT learning module do create passwords that are longer and more secure than other users. The assessment of password security was performed using the zxcvbn tool, developed by Dropbox, that measures password entropy.

Keywords: Security training · Passwords · ContextBased MicroTraining · CBMT

1 Introduction

As the digital era continues, almost everyone around the world is becoming ever more present online. As our dependence on digital services increases so does our need for information security, and a key aspect of information security is security behavior including the ability to select good passwords to protect our social media accounts, work accounts, encrypted data and more. However, there is a wealth of papers demonstrating that users tend to select passwords that are easy to guess for an attacker [1–3]. Practitioners, as well as researchers, continuously try to find ways to make users select good passwords, by enforcing complexity rules or using different support systems [4, 5]. Another commonly proposed solution is to use other means of authentication instead of, or in combination with, passwords. Those other means of authentication include one-time passwords, hardware tokens, and password managers, and while the security benefits are undeniable
they fail to be widely adopted [6]. A common denominator for why users select not to adopt a more secure behavior is usability, users seem to prefer ease of use over security [7, 8]. As such, a fundamental demand of any security function, especially one designed for the general population, should be usability.

In this paper, we consider a password to be a socio-technical property and argue that a secure password mechanism, for instance, an account registration web site, must not only consider computational security, but also the user. As argued by [9], a password mechanism’s effectiveness relies on its ability to make a user select a good password willingly. Yet another important factor in information security is awareness [10]. It is widely believed that users will act more securely if they are aware of the risks of insecure behavior. A common suggestion for how to make users more aware is to train them. In this paper, we propose and analyze how the use of a novel training approach can make users select good passwords during password creation.

The aim of this study is to implement and test how the learning method called ContextBased MicroTraining (CBMT) can assist users in creating stronger passwords. The aim is studied using a two-step method beginning with a survey where participants are asked to create an account. During account creation, the participants are faced with password creation guidelines in different ways and the survey measures how well they learned the password guidelines that were proposed for the survey. The second step involved an experiment were users set to register an account for a local Internet Service Provider were presented with password creating guidelines presented according to the principles of CBMT. The passwords were evaluated and measured against passwords created by a control group that was not faced with any password creation guidelines. The results of this paper will be a demonstration of how CBMT can be implemented. The contexts of passwords were chosen since is easy to measure the effect on passwords strength and passwords are unarguably crucial to security today.

The rest of this paper is structured as follows. Section 2 describes ContextBased MicroTraining (CBMT) and the password creation guidelines that were handed to participants in the study. Section 3 describes the methodology used. Section 4 presented the results of the study before it is concluded in Sect. 5.

2 Background

This research demonstrates how CBMT can be used to train users to select good passwords and measures the effects of using CBMT in a real-world context. Therefore, this chapter is devoted to an explanation of what CBMT is and the theoretical foundation of CBMT. Further, the password guidelines proposed in the CBMT learning modules are explained and motivated.

2.1 CBMT

CBMT is a theoretical framework that outlines how information security training of users can be executed. In essence, CBMT can be summarized as follows [11]:

“CBMT stipulates that training should be delivered in short sequences, in an accessible format, when needed”.

On a more practical note, this means that training designed according to the principles of CBMT should be implemented so that it is presented to a computer user when he or she is in a situation where the training is of direct relevance. Further, it should be presented in a way that is easy to understand and short to minimize disruption [12].

The CBMT framework is based on the principle that people need motivation to learn. The idea is that the likelihood that any adult will learn is increased if the knowledge seems meaningful for the learner [13]. This notion is based on the concept of andragogy as presented by Knowles [14]. Knowles [14] argues that adults need the motivation to learn. The foundation in this way of thinking is that the learner will learn better if the knowledge presented seems meaningful. One way to accomplish this is to present knowledge in a context where it is applicable. As discussed by Herrington and Oliver [15], presenting knowledge to learners in a situation where the knowledge is applicable will cause a more meaningful learning experience. This is the first requirement that CBMT tries to facilitate. Also, by providing knowledge to a user when the user needs it brings a reminding effect. In this particular case, a user creating a password will be reminded to select a strong password. As discussed by [16], reminding users to behave in a secure way is likely to be effective in the information security domain.

Further, an obstacle in the sense of providing the computer user with knowledge about information security has been to make the users participate in education. One technique that has gained an increasing interest in recent years is microlearning or similar strategies including nanolearning and micro-training. As described by Wang, Xiao [17], nanolearning is a teaching method where information is presented in short sequences. The idea is to facilitate just-in-time learning meaning that information is provided in small chunks, thus making the time needed to absorb the information short and in an on-demand fashion [18]. As described by Bruck, Motiwalla [19], there has been research showing positive results of microlearning both in terms of learner participation and satisfaction. Microtraining is the second fundamental building block of ContextBased MicroTraining.

CBMT can be described as a framework that describes learning objects from two directions. The first direction concerns the delivery of the learning objects and states that the learning objects should be short sequences delivered in an on-demand fashion. The second direction concerns the content of the learning objects. In this respect, CBMT demands that the information presented in a learning module is of immediate use to the learner and therefore assumes that the information is relevant to the user in the users’ current context. In this respect, CBMT tries to facilitate the concept of “learn by doing” theories that can be summarized as describing that learners learn better when they perform tasks instead of just reading [20]. CBMT is also a learning method that includes aspects of problem-based learning (PBL) in that it is designed to guide the learner through real-world tasks [21]. In summary, the meaningfulness is achieved by the learner doing some task related to his or her situation.

CBMT was first introduced by [22] and [23] who argued that CBMT could be used as an efficient way to counter online fraud. CBMT has been further evaluated in [11] where study participants reported that they perceived CBMT as a good way to learn about security [11]. CBMT has also been used to develop teaching material for technical courses in higher education with success [12].
In this study, CBMT is implemented as a means of teaching users how to create strong passwords at the point of account registration. In essence, a learning module is presented when a user that is creating an account hits the “create password” field. The module contains guidelines for how to create a strong password, as outlined in the next section. The approach, in this case, is inspired by security nudges as described by [24] but attempts to combine passive support with active intervention. At the end of the module, the user is asked to create her password. The steps of the learning module is presented in Fig. 1, below.

Fig. 1. Implementation of CBMT used in this study

The first part of the learning module presents the user with some fundamental password guidelines. The user may then continue to learn even more. After the second window, the user can test herself by answering three questions about the presented guidelines. An incorrect answer will generate feedback, and a correct answer will allow the user to continue. In the final windows, the user can create her password. A strength meter is also present on the last page. The user may choose to go directly to the last page from the first or second page.

2.2 Password Guidelines

This paper is concerned with teaching users to select good passwords. What a good password actually is, is a question that is debated among scientists as well as practitioners. For instance, as of October 4th 2019, Microsoft suggest long and easy to remember passwords while Apple and Yahoo suggest that a password should include as many different character groups as possible [25–27]. Looking to influential standardizing organizations, NIST now suggest that password guidelines should suggest long passwords that are easy to remember, such as passphrases [28]. On the other hand, ENISA suggest mixing character types [29]. ISO/IEC 27002:2017, as another example, does state that a good password should be easy to remember but does also discourage the use of words in passwords [30].

The password guidelines used in this paper are based on ongoing research into strong and memorable passwords and are based on [31]. They are designed to generate long passwords and read as follows:
• A good password is hard to crack and easy to remember.
• It should consist of at least four words.
• The password should not contain information relating to the password holder.
• Passwords should never be written down.
• A password can be made unique by adding the name of the site or service where it is used to itself.

3 Methodology

This paper seeks to evaluate whether the presented CBMT learning module can assist users in creating stronger passwords. As described by [32], scientific validity is enhanced if a problem is researched from several angles. This study was carried out in two steps beginning with a survey were the participants were asked to create an account and then answer some questions about the password guidelines that was presented to them upon account creation. Then the learning module was implemented on the account creation site of a local ISP. The survey measured how well the users took notice of the presented guidelines and the experiment measured the actual effect the learning module had on password strength. To ensure compliance with ethical guidelines [33], care was taken to ensure that no passwords was disclosed to the researchers or any external party. An overview of the research process is shown in Fig. 2, below.

Throughout the study, two different metrics was used to measure password strength. The first metric was password length in characters. The second metric is called score and is derived from zxcvbn, a password strength estimator developed by Dropbox [34]. According to a large study by [35], zxcvbn was found to be the most accurate password strength estimator. While zxcvbn calculates a number of metrics, the only one used in this paper is called score. The score is a value between 0 and 4 and the scored are described as follows [36]:

• 0# too guessable: risky password. (guesses < 10^3)
• 1# very guessable: protection from throttled online attacks. (guesses < 10^6)
• 2# somewhat guessable: protection from unthrottled online attacks. (guesses < 10^8)
• 3# safely unguessable: moderate protection from offline slow-hash scenario. (guesses < 10^{10})
4# very unguessable: strong protection from offline slow-hash scenario. (guesses \( \geq 10^{10} \))

The score is based on how many attempts an attacker would have to make to guess a password (entropy). To calculate the entropy, zxcvbn takes several factors into account including:

- Password length, longer passwords mean higher entropy.
- Password complexity, use of different character types mean higher entropy.
- Occurrence of common passwords, use of passwords common in leaked databases mean lower entropy, and use of individual words such as “potato”.
- Repeated patterns, repeating patterns such as abcabcabc mean lower entropy.

The full and exact algorithm used is presented in [36]. Both the score and the password length are considered to be numerical values in all statistical analyses used in this paper. The reminder of this section will detail the survey and the experiment.

### 3.1 Survey Test

The first part of the study was a survey designed to measure if the participants paid attention to the password creation guidelines presented to them during account creation. The survey itself was not anonymized. Instead, the participants were asked to register an account with their e-mail address and a password of their choosing. They were also told that they would receive personal feedback containing their answers and a summary of the answers from the rest of the population.

The participants were invited to the survey via an e-mail containing a survey link. The survey was distributed to municipalities as well as university staff and students. The link led to a web-based informed consent form where the participants were asked to accept the conditions of the study. Upon accepting the conditions, the participants were randomly assigned to one of three groups; CBMT, TEXT, and LINK. They were then forwarded to the first part of the survey, account creation. During account creation, the participants were asked to register their e-mail and create a password. Password guidelines were shown the participants in the following different ways:

- The CBMT group was shown the CBMT module after clicking on the “select password” box.
- The TEXT-group was given the same guidelines in plain text just above the registration form.
- The LINK-group was shown a link to text-based password guidelines labeled “Click here to learn more about good passwords”.

Following registration, the password was analyzed as previously described and the participants were handed questions about demographic aspects including their IT-competence. Following the demographic questions, the participants were given the following questions about the password guidelines that was shown to them during account creation:
Assisting Users to Create Stronger Passwords Using CBMT

• Concerning the password guidelines presented on the previous page, how long passwords were suggested?
• What was suggested as a way to create strong passwords?
• What was described as most important for a password to be secure?
• What was described as most important of the following?
• What tip was given on how to create unique passwords for each of your accounts?

The first question was designed to see if the user's noticed the main point of the guidelines, the password length suggestion of four words. Questions two and three were used to see if the users understood the secondary suggestions, creating long and memorable passwords. The final two questions measured if users noticed tips that were presented at later stages in the guidelines, on how to make passwords even better and unique. In data analysis, two indexes were created. One that reflected how many correct answers each respondent gave to the first three questions and one index of correct answers to all questions. The results for the first question were also analyzed on its own.

For data analysis, the survey data were grouped based on the three test-groups. The participants were further grouped based on their reported IT-competence since previous research suggests that IT-competence is a key factor in security behavior [37]. The Shapiro-Wilk's test was used to test whether the generated data were normally distributed [38], and the means and median are reported for the three variables (the first question and the indexes) in all groups. Based on central tendencies observed using descriptive statistics, hypothesis testing was used to evaluate if the tendencies were significant. Because of space limitations, the results are presented in condensed form. The hypotheses were expressed as follows:

H1: Group X scores higher than group Y regarding variable Z
H0: There is no difference between groups X and Z regarding variable Y

Further, Mann-Whitney U-test was used for hypothesis testing. Mann-Whitney U-test was selected in favor of T-test since no samples were normally distributed and are therefore more suitable than T-test [39]. The significance level used in this study is the conventional 95% meaning that results are significant if $p < 0.05$. SPSS was used for statistical analysis.

3.2 Experiment

In the second part of the study, the learning module presented in Sect. 2.1 was implemented on the account registration page of a local ISP. It was implemented so that 50% of the visitors used the learning module when they registered their account and the other 50% was presented with an unmodified version of the registration page. The unmodified registration page does not propose any password guidelines and is displayed in Fig. 3, below.

The password entered during the testing period was analyzed and password length and score were captured. Whether or not the password was created using the learning module was also recorded to allow for analysis of the effects of the learning module. For data analysis, the test data were grouped based on whether the passwords were
created using the CBMT module or not. The Shapiro-Wilks test was used to test if the generated data was normally distributed [38], then means and median was reported for the two variables in both groups. Further, Mann-Whitney U-test was used to differences in values between the two groups. Mann-Whitney U-test was used since no samples were normally distributed and are therefore more suitable than T-test [39]. The significance level used in this study is the conventional 95% meaning that results are significant if \( p < 0.05 \).

### 4 Results

This section details the results gathered from the two parts of the study.

#### 4.1 Survey

The survey was completed by 179 participants distributed among the answer groups as follows:

- CBMT: 54
- TEXT: 68
- LINK: 57

61 of the respondents rated the IT-competence as being “IT-professionals”, 50 respondents were students, 121 were working and 8 respondents reported having some other occupation. A majority of the respondents were between 20 and 30 years old (120), 31 were between 31 and 40 years and the rest were older. Following the calculations of the indexes, the mean and median values for the different metrics are displayed in Table 1, below. The measures were not normally distributed in any group, mean and median values are displayed once for all respondents and then once for all respondents that did not report being IT-professionals.
Table 1. Mean and median values or metrics from survey

<table>
<thead>
<tr>
<th>Variable</th>
<th>Group</th>
<th>Mean</th>
<th>Mean_noIT</th>
<th>Median</th>
<th>Median_noIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1</td>
<td>CBMT</td>
<td>0,59</td>
<td>0,69</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Q1</td>
<td>TEXT</td>
<td>0,40</td>
<td>0,38</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Q1</td>
<td>LINK</td>
<td>0,19</td>
<td>0,16</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Index1_3</td>
<td>CBMT</td>
<td>1,61</td>
<td>1,75</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Index1_3</td>
<td>TEXT</td>
<td>1,27</td>
<td>1,20</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Index1_3</td>
<td>LINK</td>
<td>0,77</td>
<td>0,67</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Index1_5</td>
<td>CBMT</td>
<td>2,20</td>
<td>2,44</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Index1_5</td>
<td>TEXT</td>
<td>1,86</td>
<td>1,84</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Index1_5</td>
<td>LINK</td>
<td>1,31</td>
<td>1,18</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

As seen in Table 1, the CBMT group has the highest score for all metrics, followed by the group TEXT. The group LINK that only saw a link to password creation guidelines is last in all cases. Furthermore, the values for all metrics in the CBMT group increases when the responses from IT-professionals are disregarded. The same action fields the opposite result in the group TEXT.

Looking at the descriptive statistics in Table 1, the users that were presented with password guidelines using CBMT appears to understand the contents of the guidelines to a higher degree than in the other groups. Mann-Whitney U-test was used to test if the observed tendency is significant. The test was applied pairwise and for the complete answer groups as well as for all respondents except the IT-professionals. The test and results are presented in Table 2, below.

Table 2. Results of Mann-Whitney U-test, results are significant if $p < 0.05$.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Case</th>
<th>$P$</th>
<th>$P_{noIT}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1</td>
<td>CBMT-TEXT</td>
<td>0,033</td>
<td>0,013</td>
</tr>
<tr>
<td>Q1</td>
<td>CBMT-LINK</td>
<td>0,000</td>
<td>0,000</td>
</tr>
<tr>
<td>Q1</td>
<td>TEXT-LINK</td>
<td>0,014</td>
<td>0,031</td>
</tr>
<tr>
<td>Index1_3</td>
<td>CBMT-TEXT</td>
<td>0,087</td>
<td>0,03</td>
</tr>
<tr>
<td>Index1_3</td>
<td>CBMT-LINK</td>
<td>0,000</td>
<td>0,000</td>
</tr>
<tr>
<td>Index1_3</td>
<td>TEXT-LINK</td>
<td>0,004</td>
<td>0,019</td>
</tr>
<tr>
<td>Index1_5</td>
<td>CBMT-TEXT</td>
<td>0,203</td>
<td>0,091</td>
</tr>
<tr>
<td>Index1_5</td>
<td>CBMT-LINK</td>
<td>0,000</td>
<td>0,000</td>
</tr>
<tr>
<td>Index1_5</td>
<td>TEXT-LINK</td>
<td>0,009</td>
<td>0,019</td>
</tr>
</tbody>
</table>
As seen in Table 2, all test values involving the group LINK are significant, showing that the participants shown a link to password guidelines understands the passwords guidelines to a lower degree than users shown the guidelines in text or using CBMT. Further, the test values for CBMT-TEXT are significant for Q1, showing that the users of CBMT does understand the key part of the guidelines better than the other groups. Further, the value for CBMT-TEXT for Index1_3 is significant if users that consider themselves IT-professionals are disregarded.

In conclusion, the results of the survey show that using CBMT or just plain text to present password guidelines is significantly better than presenting users with a link to the guidelines. Further, the results suggest that CBMT will make the users notice the password guidelines better than presenting the guidelines as text. It is also worth mentioning that the observed results are more significant amongst users that do not consider themselves IT-professionals.

4.2 Experiment

In the experiment, a CBMT module showing the password guidelines was implemented at the account registration page of a local ISP. The passwords created by the users during the experiment were analyzed. A password score and the password length was registered. The passwords were never made available to the researchers but keep confidential by the ISP. During the test period, data was gathered from 124 users that created new accounts. 64 was presented with the CBMT learning module (This group is referred to as CBMT) and 60 was presented with the unmodified registration page (This group is called control). The mean values for password length and score are presented in Table 3, below.

<table>
<thead>
<tr>
<th>Table 3. Descriptive statistics from experiment data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Variable</td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>Length</td>
</tr>
<tr>
<td>Length</td>
</tr>
<tr>
<td>Score</td>
</tr>
<tr>
<td>Score</td>
</tr>
</tbody>
</table>

As seen in Table 1, the values from the CBMT group is higher for password length as well as score. Further, no datasets were normally distributed and thus, the median is the most accurate measure. Reading the median values, the CBMT group scored 1.5 characters higher in password length and 1 higher in password score. The descriptive statistics bring the following hypotheses for testing:

H1: Users presented password guidelines in the form of a CBMT learning module create longer passwords than users not presented with any guidelines.
H2: Users presented password guidelines in the form of a CBMT learning module create passwords with a higher score than users not presented with any guidelines.
The corresponding null hypotheses are that no such difference can be observed. Mann-Whitney U-test was used to test if the observed tendency is significant. The results are presented in Table 4, below.

Table 4. Results of Mann-Whitney U-test, results are significant if $p < 0.05$

<table>
<thead>
<tr>
<th>Variable</th>
<th>Group</th>
<th>Mean rank</th>
<th>Sum of ranks</th>
<th>$P$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length</td>
<td>CBMT</td>
<td>70.15</td>
<td>4489.50</td>
<td>0.013</td>
</tr>
<tr>
<td>Length</td>
<td>Control</td>
<td>54.34</td>
<td>3260.50</td>
<td></td>
</tr>
<tr>
<td>Score</td>
<td>CBMT</td>
<td>71.96</td>
<td>4605.50</td>
<td>0.002</td>
</tr>
<tr>
<td>Score</td>
<td>Control</td>
<td>52.41</td>
<td>3144.50</td>
<td></td>
</tr>
</tbody>
</table>

As seen in Table 4, Mean rank and Sum of rank columns indicates that the passwords in the CBMT group are longer and have a higher score. The $p$-values are below 0.05 in both cases showing that the results are significant. In conclusion, the null hypotheses can be rejected in favor of H1 and H2. Thus, the experiment shows that the users who used CBMT to create passwords created stronger passwords than the users that used the unmodified registration page.

5 Conclusions

This paper presents the learning framework CBMT and analyzes if it can be used to help users create good passwords. The study explores the aim from two different directions; first by using a survey to measure to what degree users understand password creation guidelines presented in different ways and second, by implementing CBMT on the registration page of a local ISP and analyze the actual impact on password strength and length. Length and strength are used as independent measures since it is possible to create a longer password that is computationally weaker than a shorter. The results of the survey suggest that users that are presented with password creation guidelines with CBMT modules do indeed understand the guidelines to a higher degree than if users are presented with the guidelines as text, or with a link to password creation guidelines elsewhere. From the survey data, it is also worth mentioning that presenting password creation guidelines as text is better than a link. Furthermore, the results of the experiment show that using CBMT helps users create passwords that are longer and stronger than if the users are not presented with any password creation guidelines at all. As such, this paper concludes that using CBMT to present password creation guidelines will lead to users creating better passwords and understand the password creation guidelines to a higher degree than if the guidelines are presented in other ways.

This paper shows that CBMT can assist users in the creation of good passwords. However, it is interesting to notice that not even the participants that used CBMT noticed the presented guidelines to a very high degree. Looking at the most emphasized tip, using 4 words as the password only 59% of the respondents in the CBMT group remembered
the tip. Looking at the scores for the index of all five questions the mean value in the CBMT group was 2.2 of 5. These numbers suggest that it is hard to make users notice password creation guidelines at all. An explanation could be that users are simply not too concerned with security, or that they do not care about what a certain application proposes.

It is, however, also interesting to see that CBMT has a high impact on password quality. In this particular example, the mean password strength was increased by 1 on a 0–4 scale and the mean password length was increased by 1.5. The increase in password strength has an undeniable and direct effect on security since the passwords are much harder to crack. One explanation as to why the users using CBMT select stronger passwords might be that they understand the password creation guidelines to a greater extent. However, the relatively low scores from the survey suggests that that may not be a complete explanation. Another explanation can be that the CBMT forces the users to integrate with it and thus, reminds them of security.

The implications of this paper are twofold. The paper demonstrates and validates a concrete method for the presentation of password guidelines. The method described in this paper can be implemented by practitioners seeking to increase password security in their organization. The paper also presents a framework for how information security training can be used to improve user’s security behavior. As such, the paper contributes to the scientific and practitioner community with new insights into the information security training domain.

Following this study, future projects could further examine the results presented in this paper with more studies using other and larger samples. Another direction for future research could be to analyze how CBMT can be used in other information security contexts to, for instance, assist users in dealing with online fraud, fake news or phishing. It would also be interesting to examine the long term effects of using CBMT. Knowledge retention and organizational security awareness are good starting points. A future study could examine the password culture before, during and after using CBMT for information security training.

References

33. Schrittwieser, S., Mulazzani, M., Weippl, E.: Ethics in security research which lines should not be crossed? In: Security and Privacy Workshops (SPW), IEEE (2013)
PAPER 5: CAN JOHNNY ACTUALLY LIKE SECURITY TRAINING?

Can Johnny actually like security training?

Joakim Kävrestad\textsuperscript{a}, Evelina Friman\textsuperscript{a}, Joacim Bohlander\textsuperscript{a} and Marcus Nohlberg\textsuperscript{a}

\textsuperscript{a}University of Skövde, Högskolevägen 1, 541 28 Skövde, Sweden

Abstract

Information security is a socio technical domain where a lot of traditional efforts has been placed in the technical domain where security has been considered technical and the solutions has been technical. However, it is well know that human behavior plays a key role in information security and the user is often seen as the weakest link in the security chain. As such, information security is a socio-technical property where the social, or human, side needs increased attention. Security training is commonly suggested as the way to improve user behavior but the effects of various training efforts is also underresearched. This paper demonstrates how ContextBased MicroTraining (CBMT), a method for information security training, which has been developed over years of researched can be implemented and performs a usability evaluation of that implementation. The paper demonstrates that the CBMT method can aid in development of highly usable security training. The paper also emphasizes the need for user centered design in development of security software intended for end-users.

Keywords

CBMT, ContextBased MicroTraining, Usability, Usable security, Security training

1. Introduction

Usability and user-centred design of software is a key aspect of modern software development. Users seems to be more likely to use software designed to be highly usable, and that is a truism that hardly surprises anyone. Nevertheless, security functions that are developed to provide users with an added layer of security often fall short in the usability department \cite{1}. A challenge when it comes to security software is that an organisation will strive for an adoption rate of 100\% amongst its users so that no single user can be a weakness in the cybsecurity of that organisation. As such, usability testing of security features that are supposed to be adopted by every single user is integral \cite{2}.

Information security is, by its nature, socio-technical \cite{3} and proper security work must consider social as well as technical aspects of security \cite{4}. \cite{5} describes that Social-Technical Systems Design (STSD) considers human, social, organizational and technical factors and this is comparable to how information security is commonly described. Our paper presents a usability evaluation of the method ContextBased MicroTraining (CBMT), presented in \cite{6}, which provide guidelines for how useful information security training can be performed. CBMT stipulates that information security training should be delivered to users when they encounter a situation where the training is of direct relevance. As such, it requires one component able of detecting such situations and one component that provides the user with training with the goal of improving the users security behaviour, making CBMT socio-technical in nature.

The goal of the paper is to demonstrate how information security training can be performed according to the CBMT method and to assess how the method support development of usable information security training. The focus of this paper is on usability and thus, the social part of STSD. The paper...
Figure 1: Research overview

is structured as follows; Section 2 introduces CBMT and briefly presents the ongoing research effort around CBMT. Section 3 outlines the methodology used in this paper, Section 4 describes the usability analysis performed and section 5 relates the usability analysis to the CBMT method. The paper is concluded in section 6 with a discussion on the papers contributions and directions for future work.

2. Description of CBMT and its development

ContextBased MicroTraining (CBMT) is a method for end user training developed for information security and awareness training. This paper makes one part of an ongoing design science effort. The full research process is based on [7], [8] and[9] and described in Figure 1, below. This paper is connected to the evaluation phase of the second design cycle, as denoted in Figure 1. The previous steps in the research is presented in [6].

CBMT is a method that provides goals and guidelines for implementation of information security training. It is described as follow [6]:

Goals:

- Provide training that users want to make use of, instead of forcing users to participate in the training
- Include an awareness increasing mechanism
- Require no prior knowledge from the user
- Be short and easy to absorb
- Should minimize annoyance for all users, especially users already familiar with the subject

Guidelines:
• Delivered to users when it is relevant to their current situation. The situation can be constructed or natural.
• Delivered in short sequences
• Relevant to the users’ current situation
• Include or directly relate to a practical element
• The information presented must in itself be easy to understand
• The most crucial points of the information should be highlighted
• Must be possible to opt-out or skip

The CBMT method is based on the notion that users need motivation to learn [10] and that they learn better if learning is combined with a practical element [11]. CBMT also stipulates that training should be delivered in a situation where it is of direct relevance to the user, i.e. password training should be provided to the user when the user is about to create a password, and in short sequences. This approach is assumed to increase the likelihood that the user makes use of the provided information and provides a awareness increasing mechanism comparable to security nudges.

CBMT requires a technical element that is able to detect situations where a user needs training and an element containing the training itself. The training is intended to improve the users security behaviour, and ultimately increase organizational security culture, making CBMT an example of a socio-technical system as described by [5]. This paper aims at evaluating the social side of CBMT by performing a usability analysis of an implementation of CBMT and connecting the results of that to the theoretical method.

3. Methodology

This study is a multi-disciplinary effort with researchers in information security working with User Experience Designer(UXD) experts. The UXD experts performed a usability test of an implementation of CBMT, hereafter referred to as the implementation. The implementation was a software that provided users of a web-site with training on how to create good passwords. It was activated, and appeared as a pop-up, once a user clicked in the “Create Password” field of an account registration form and is demonstrated in Figure 2, below. The security researchers analysed the results of the usability test in regards to the CBMT method.

Due to the CoVid-19 situation that affected the world during 2020, a user participatory usability study was deemed hard to complete. Instead, the usability analysis was performed as an “individual expert review” as described by [12]. The “individual expert review” entails that the experts evaluate the target software in order to find problem areas that can decrease the users experience of the software and thus hinder user adoption och correct use. The evaluation includes the experts using the software and assessing the various steps in the software in great detail. Two UXD experts without previous knowledge of the implementation or the underlying CBMT theories evaluated the implementation individually and then combining their results. Having individual experts performing the evaluation independently and then combine their results increase the validity of the results [13]. The

1The implementation is demonstrated at:https://rr222cy.github.io/SecurityAssistantWidget/
Figure 2: Implementation of CBMT

analysis identified problem areas that were categorised according to [14] approach for categorization of problem areas and ranked based on severity. The analysis was then complemented by a one participant usability analysis, as suggested by [12], that analyzed the following requirements:

- The software should be highly learnable meaning that the user should easily understand the purpose of the software and how to use it
- The presented text should be understandable to the user meaning that the user should understand all information presented while using the software
- The user should learn something about password creation after using the software

Taking the usability analysis outcomes as input, thematic coding, as described by [15] was used to identify information relating to the theoretical CBMT method and the identified information was summarised as the result of this study. Information considering the particular implementation rather than the CBMT method was disregarded in this study since it does not impact the theoretical foundation of CBMT.

4. Usability analysis

This section describes the steps in the performed usability analysis.

4.1. Expert analysis

The implementation was analyzed by two UXD experts using the expert analysis method described by [12]. To increase validity, the two experts performed the analysis individually and then compared their results. The analysis revealed the following 22 problem areas:
1. The implementation presents a pop-up that cannot be escaped and can be seen as interrupting the user's workflow.
2. The "Create password now" button disappears if the user closes the implementation rendering the user unable to create a password at all.
3. The implementation is not expected by the user and forces the user into a workflow the user did not expect.
4. An option to navigate backwards is missing.
5. The implementation cannot be closed by clicking outside of the implementation window.
6. The user does not get visual feedback when selecting an answer in the Quiz-part of the implementation.
7. The implementation contains emojis that are displayed in different ways in different browsers.
8. The ending "Use this password" button works even if the user did not type any password.
9. The user is not made aware of the length of the quiz.
10. The graphic included in the implementation does not match the actual implementation.
11. The password typed by the user is censored and the censorship cannot be removed.
12. The quiz do not provide feedback on correct answers.
13. The implementation could include examples on "approved" passwords.
14. The implementation could include, or link to, more information about the risks with bad passwords.
15. Some buttons appear to be far from text elements.
16. The "Create you password" button is blue while other buttons with similar purpose are yellow.
17. The last sentence on the "Create better passwords by making them longer" is confusing.
18. The button used to move forwards from the last quiz question says "Next question".
19. Spelling error in question 3.
20. The graphic is oddly cropped.
21. The strength meter on the "Create password" page could be clarified with levels.
22. The module cannot recognize if a user follows or disregards the presented guidelines.

The identified issues were further classified based on severity as suggested by [14]. Issue 1-3 was classified as catastrophic, 4-11 were classified as severe, 12 - 18 were classified as smaller issues and 19 - 22 was considered cosmetic.

### 4.2. Usability test

The expert review was followed by a usability test with one participant. The participant was not an IT professional but considered himself to be a skilled computer user with general knowledge about security practices. He did, for instance, claim to possess knowledge about how to create strong passwords before the test started. The usability test was used to validate the results of the expert analysis and assess the implementation in regards to the following established requirements:

- The software should be highly learnable.
- The presented text should be understandable to the user.
- The user should learn something about password creation after using the software.
The usability test suggest that the software fulfills the analyzed requirements. Another insight from the usability test was that the participant, when asked to create an account using a standard account creation form, was surprised by the appearance of the implementation. The participant also expressed concerns about the quiz part of the implementation similar to the problems discovered by the expert review. The participant did, however, not express any concerns with the software itself, nor did the participant express any problems understanding the information presented by the implementation. To summarize, the usability analysis suggests that the implantation fulfilled the requirements established for the usability test. Further, it validates the expert review since several problem areas was identified by the participants, and one was contradicted.

5. Analysis of usability analysis in relation to the CBMT method

To relate the usability analysis to the CBMT method, the results of the usability analysis was analyzed using thematic coding. The results was classified as related to the CBMT method or related to the implementation itself. The Following bullets was considered to relate to the CBMT method:

- The implementation presents a pop-up that can't be escaped and can be seen as interrupting the users workflow (From the expert analysis and the usability test)
- The implementation is not expected by the user and forces the user into a workflow the user did not expect (From the expert analysis and the usability test)
- The implementation is easy to use and provides useful information (from the usability test)

The first two bullets suggests that a usability hinder is the fact that CBMT states that the users workflow should be intercepted under certain conditions, namely when a security situation occurs. In this case, the user does not expect the implementation to be activated since he is not aware of it and it deviates from the standard behaviour of registration forms. The final bullet suggests that the user does find the implementation useful as tool for learning about security.

The CBMT method, as well as many other common security functions, must interrupt the users workflow in order to provide its intended function. As the usability analysis highlight this as a problem it shows that developers of interrupting security functions must take special care to make those functions as user friendly as possible. The CBMT method attempts to do this by suggesting that the information presented to users should be in a short and easy-to-digest format. A conundrum that should require further research it that previous research has shown that being interruptive can improve security behaviour to the better[16], but this analysis suggests that it hinders usability. A question raised is inevitably how security behaviour can be increased with minimal negative impact on usability, and what level of interruption that is optimal. that is, however, beyond the scope of this paper.

6. Conclusions

This paper described the CBMT method developed for information security training and positions it as a social-technical system that uses technical elements to identify situations where users need training and then provides training designed to improve the users security related behaviour. We argue that usability and user-centric design is a key factor in development of security software designed for end-users as it will increase the adoption rate and acceptance amongst end-users, a pre-requisite in order to achieve the security function the software is intended to provide.
This paper subjects an implementation of CBMT to rigorous usability analysis using an expert review method where the implementation is scrutinized by UXD experts. The expert review is complemented by a usability test with one participant and the results are related back to the CBMT method. The results of the study suggests that the CBMT method can support development of usable security training algorithms that provide users with easy-to-understand information and serves as a validation of the CBMT method. This notion aligns well with previous research reporting on user perception of CBMT-based training [17, 18]. The results contribute to increased knowledge around the human element of STSD related to information security. The paper also contribute to the practical community with a concrete demonstration of how information security training can be performed.

The main negative finding in the usability analysis is that the implementation was unexpected by the user and interrupted the users workflow. It is well known that security seldom is the users primary target making most security functions perceived as interruption the users workflow [19, 20, 21]. Nevertheless, security functions is a necessity in order to establish a healthy security behaviour. As such, this study emphasises the need to employ a user-centric approach to development of security functions in order to minimize annoyance to the greatest extent possible in order to maximize acceptance and adoption.

The usability analysis performed in this study relied on a methodology that did not require a large sample of participants. The methodology was chosen since the Covid-19 pandemic made participant based usability analysis hard to perform under social restrictions that applied world-wide during the spring of 2020. One could even argue that such a study could contribute to the spread of infection and thus, putting participants at risk in an unethical manner. Follow-up studies using a participant based methodology is an obvious direction for future work. Another direction for future work could focus on evaluation user perception and learning outcomes from using CBMT over an extended period of time.

References

[8] K. Peffers, T. Tuunanen, M. A. Rothenberger, S. Chatterjee, A design science research method-


PAPER 6: CONTEXTBASED MICROTRAINING: A FRAMEWORK FOR INFORMATION SECURITY TRAINING

ContextBased MicroTraining: A Framework for Information Security Training

Joakim Kävrestad and Marcus Nohlberg
University of Skövde, Skövde, Sweden
{joakim.kavrestad,marcus.nohlberg}@his.se

Abstract. This paper address the emergent need for training measures designed to improve user behavior in regards to security. We do this by proposing a framework for information security training that has been developed for several years and over several projects. The result is the framework ContextBased MicroTraining (CBMT) which provides goals and guidelines for how to better implement information security training that supports the user in the situation where the user needs support. CBMT has been developed and tested for use in higher education as well as for the support of users during passwords creation. This paper presents version 1.0 of the framework with the latest refinements.

Keywords: Security training · Awareness · ContextBased MicroTraining · Information security

1 Introduction

It is well established that insecure user behavior is a major problem in information security [25]. Users are commonly referred to as the weak link in security and while there are many technical security measures that address technical security issues, there is still a need for ways to improve user behavior with regards to security [7]. Threat actors recognize this notion and are often exploiting users, making the need for measures towards secure behavior emergent [11]. Desmand [8] described a need for making users understand the consequences of insecure behavior and learn them to behave in a secure way [8].

The common suggestion for how to improve user behavior is through the use of training [24]. Further, there are many different suggestions on how to carry out security training, from the practitioner as well as the research community. Different training measures range from lectures to micro training and nudges or special purpose tools such as password strength meters. While there are research examples of individual studies where researchers provide good evidence that specific methods work, there are reports that suggests that organizations training programs are not grounded in empirical evidence of their validity [1, 2]. As such, the need for further research into this area is apparent.
This paper reports on research in this area that has been ongoing since 2014 intending to address the following objectives:

- O1: Develop a framework of guidelines for user training that supports user awareness and security-related decision making.
- O2: Evaluate how the framework developed in O1 can assist in making users act more securely.
- O3: Evaluate if the framework from O1 can be applied in higher education.

As such, the paper will present and discuss the framework developed in the projects and focus on the later parts of the development where the framework is refined. Following the presentation of the research process, previously published work will be accounted for and briefly described. The paper will then discuss the final part of the research process and present the final framework developed in the research. The paper will be concluded with a discussion on the topics and directions for future work.

2 Research Process

The research has been carried out in multiple steps and the complete process is outlined in Fig. 1, below. The emphasis in this paper is on the final parts of the research process (made bold in Fig. 1) The research as a whole employs a mixed-method approach using qualitative as well as quantitative methods. The reasoning behind this approach is twofold:

- Some research steps are intended to provide input to the development of the framework, making a qualitative approach feasible, while other steps intended to measure the effects of implementations of the guidelines making a quantitative approach feasible.
- Using different methods in research around the same objective, triangulation, can increase the validity of the outcomes [21].

Fig. 1. Research process
While a discussion on all methodological approaches used in the research is well beyond the scope of this paper (and previously published [12,13,16–18]) the remainder of this section will introduce the methodology used in the final research steps, “Framework refinement”.

During the evaluation step, quantitative data was used to evaluate implementations of the framework and qualitative data about the frameworks as well as the implementation of the framework was gathered. The data was gathered using free-text survey questions. Further, the suggested framework was presented at the 19th Seminar within the Framework of a Swedish IT Security Network for PhD students (SWITS) [13] and the following discussions were summarized and considered in the framework refinement. The gathered data was analyzed using the principles of thematic coding [5]. The following codes were established prior to the analysis:

- Strengths
- Weaknesses
- Clarification needed

The first code was used to identify the strengths of the framework. The second and third codes were used to identify areas in the framework that needed reconsideration or improvement. The coding was performed together by the authors and the results were used to refine the framework and establish the final framework as presented in this paper.

3 Previous Research Steps

This chapter briefly presents previous research in this project beginning with the developed framework, Context Based MicroTraining (CBMT). Then, the implementation and evaluation of CBMT based training will be presented.

3.1 CBMT and the Development Thereof

The development began with a literature search that intended to find what goals the framework should seek to fulfill. Fundamental problems in the domain of information security training were identified to be that users are not actively participating in information security training measures [19] and that users, while worried about cyber threats, lack awareness about the possible damage they can cause [22]. It was also evident that several sources reported that security measures must, in themselves, be easy to use, appear useful and interrupt the user’s normal computer usage as little as possible [3,23,28]. Following the literature search, four requirements for what was called a “Situated Learning based defense mechanism” were established:

- Provide training that users want to make use of, instead of forcing users to participate in the training
- Include an awareness increasing mechanism
– Provide training to the user when the user is in a situation where the training is relevant
– Require no prior knowledge from the user

The first two bullets were achieved by the third bullet and the idea was that information security training should be delivered to the user when the user entered a situation where the training was of direct relevance. For instance, a training module designed to teach the user about online fraud would be presented to the user when she was in a situation where she risked being defrauded [12]. A fundamental notion in the requirements is that people need motivation in order to learn and that adults will be more likely to learn if the presented information seems meaningful, a notion based on the concept of andragogy [10, 20].

A demonstrator of a defense mechanism based on the requirements was implemented, the context was online fraud. A survey containing the demonstrator and questions about how the respondents perceived it was presented. 98 respondents answered the survey and it revealed that the respondents were, overall, positive towards the defense mechanism. The survey data did, however, stress that it was important for a defense mechanism to not be enforcing and that it should be possible to read the information presented quickly [12]. This falls well in line with what Nanolearning tries to facilitate [26]. Previous research into microlearning also shows positive results in terms of learner participation [6]. Supporting a high degree of user participation is one of the fundamental problems this research aims to address. The requirements were updated, and expressed as a small framework of goals and guidelines were the goals reflect the overall goal of the framework and the guidelines are more practical implementation guidelines. The goals were the following:

– Provide training that users want to make use of, instead of forcing users to participate in the training
– Include an awareness increasing mechanism
– Require no prior knowledge from the user
– Be short and easy to absorb

And the guidelines were:

– Delivered to users when it is relevant to their current situation.
– Delivered in short sequences
– Relevant to the users current situation
– Include a practical element
– Must be possible to opt-out

Simultaneously, an experiment where participants were asked to use the defense mechanism before rating fraudulent ads from Swedish online marketplaces was carried out. A control group rated the same ads without training. The experiment showed that the group that performed the training was better at detecting fraudulent ads than the participants in the control group. They were also better at correctly identifying legitimate ads as legitimate suggesting that the defense mechanism could be useful [16].
Next, another survey measuring how the respondents perceived using training modules developed according to the framework was performed. In this case, the respondents were asked to follow three different training modules (password creation, ransomware, and phishing) and then asked about their experience. In summary, the participants were positive towards the training modules and stressed that short sequences of training in-the-moment are preferable to training that is time consuming [18]. As such, the framework was established and the research continued to an evaluation phase. The Framework was named ContextBased MicroTraining (CBMT).

To summarize, CBMT is a teaching method that suggests that information should be presented in short sequences to the learner. It should also include a practical element and be of direct relevance to the user’s current situation. A visual representation of CBMT is presented in Fig. 2, below.

![Fig. 2. CBMT overview](image)

### 3.2 Evaluation of CBMT for Use in Higher Education

Following the establishment of the framework, it was evaluated in two settings. First, for use in higher education. In this evaluation, a technical undergraduate course was used and the purpose was to measure learning outcomes of CBMT based training. The course was a Cisco Network Academy course and was selected since it was very practical in nature and it teaches a standardized curriculum and is examined using a standardized test. In this particular case, the course was thought by the researchers and the use of standardized material served as a means of minimizing bias. Applying the framework to a course was selected because it allows for a relatively controlled environment where the actual learning outcomes can be compared to the learning outcomes from previous times the course has been given.

During this evaluation, several learning modules were designed according to the goals and guidelines of the framework. The students were then handed the modules as primary lecturing material. The nature of the modules was that they asked the students to listen to a short theoretical presentation and then do or follow a practical task. One module covered a small bit of theory and the time needed to consume one module was kept to a minimum. Several modules were created and combined into video lectures that covered the full curriculum. A version of the modules can be found and used freely at YouTube\(^1\).

---

\(^1\) [www.youtube.com/playlist?list=PLEjQDf4Fr75qADv9J0UbNaiUmB8zMlw6V](http://www.youtube.com/playlist?list=PLEjQDf4Fr75qADv9J0UbNaiUmB8zMlw6V)
was combined with supervision that allowed the students to ask questions and discuss the content of the learning modules. The course ended with a practical and theoretical test. In terms of learning outcomes, the students that used the material developed according to the CBMT framework performed similar to, or slightly better than students from previous years where the same material was delivered as traditional lectures. The students were handed a survey that measured how they perceived the lecture material and 26/28 students reported that they preferred the CBMT learning modules over traditional lectures, when asked to pick one or the other. Further, the students reported that the CBMT learning modules motivated them in their studies and made them understand the theoretical material [17]. In terms of usage, 75% of the students reporting using 9 or 10 of the 10 available video lectures.

3.3 Evaluation of CBMT for Information Security Training

In another evaluation, CBMT was evaluated as a means of assisting users in selecting better passwords. In this case, an interactive CBMT module was created and implemented at the account creation page of a local internet service provider. The module was activated when a user clicked in the “create password” field and is showcased as a demonstrator at GitHub². In essence, a window presenting basic password security tips was presented, the guidelines themselves were based on Kävrestad et al. [15]. The tip was to use passwords made up of four words or more. The user could then decide to learn more or to create a password. Upon selecting learn more, the user was presented with a series of questions that gave direct feedback and upon clicking create password, the user was taken to a password creation step.

50% of the users on the web site were assigned to use the CBMT module during account creation, the other 50% used the original account creation page. The strength of passwords created by the users was measured using the zxcvbn method by Dropbox [9]. The experiment showed that users that used the CBMT module created stronger passwords than users in the control group. The effect was measured on a 4-graded scale that reflected password entropy as described by [27]. The group using the CBMT module had a median value of 3 while the other group had a median or 2, and the result was statistically significant at the 99% level.

Following the experiment, a survey was executed where participants were presented with password creation guidelines using the CBMT module, in plain text or using a link to plain text. They then received questions about the guidelines just presented to them. The survey suggested that the participants presented with the CBMT module were slightly more aware of the password guidelines than the users presented with plain text. They were significantly more aware of the guidelines compared to the users that received a link to plain text guidelines. The results of this evaluation show that CBMT can serve as a framework for the development of effective information security training that fulfilled the goals of

the CBMT framework. The results of this study are accepted for publication in IFIP SEC 2020.

4 Guideline Refinement and Establishment

Following the evaluation of the CBMT in higher education and for presentation of password creation guidelines, the framework was further refined. This refinement was used in a three-step process:

1. Insights acquired by the researchers during the evaluation were considered.
2. The framework was presented and discussed at the 19th Seminar within the Swedish IT Security Network for PhD students (SWITS).
3. Free-text answers acquired from the surveys in the evaluation phase were analyzed.

During the evaluation of CBMT for use in higher education it became evident that while the framework suggests that training should be carried out in naturally occurring situations, such as when a user is browsing the Internet, this is not always possible. In some cases, the situations need to be constructed. A constructed situation includes a situation that the user is put in rather than a situation that the user encounters. A user would, for instance, encounter phishing making that encounter a natural situation. On the contrary, a constructed situation would be when the user is asked to carry out a task as part of education or training. Subsequently, when CBMT is used in a natural situation it is used in direct relation to a practical element and does not in itself include the practical element. On the other hand, it must include a practical element itself when used in a constructed situation. The guidelines in the framework were updated to support this insight.

During the discussion at SWITS, several conference participants were positive about the framework but suggested that what the framework presents must in itself be easy to follow. The original intention of the framework was to not consider the actual material presented, only the delivery thereof. However, the consensus in the discussion at SWITS led to a new guideline reflecting that the information presented must be easy to follow. That is certainly in line with the goal that states that no prior knowledge should be required by the users. The need for this addition was further made evident from the evaluation in the context of password guidelines. It is clear that many password creation guidelines are hard to use \[4,14,29\] and one can consider the meaning of a good delivery if the information itself is hard to use.

The free text answers from the surveys in two validations steps (O2 and O3) were analyzed using thematic coding. The coding was performed by the authors together simultaneously to enhance inter-coding validity. The coding revealed no negative comments about the framework and 11 comments that were positive but did not otherwise add to the development of the framework.

Several users expressed that they did not follow the guidelines in favor of their own more complex password creation guidelines. None of these users reported
being negative about the learning module. This suggests that the learning module was not annoying for advanced users. Typical information security training tools, including this, is targeting all users. We argue that training presented to users that do not perceive that they need the training can be interpreted as an annoyance rather than provide value. It is therefore important that tools built using the CBMT framework are developed so that they minimize interruption and annoyance, and provide a way for users to skip the training, especially if it is repetitive.

In line with this reasoning, it is important that the presented material really highlights the most important aspects of the subject matter, a notion that was also identified in the analyzed material. While it is important that the presented material covers the essential information the users need, it is evident from the analyzed information that most users will only notice some aspect of the presented material. It is therefore important that the most crucial points in the material are, in some way, highlighted even more. One example of highlighting, which was used in the password training module, was to make the most important points bold.

Following the refinements, the final goals and guidelines of CBMT are as follows (modifications in the refinement step are in italic):

Goals:
- Provide training that users want to make use of, instead of forcing users to participate in the training
- Include an awareness increasing mechanism
- Require no prior knowledge from the user
- Be short and easy to absorb
- Should minimize annoyance for all users, especially users already familiar with the subject

Guidelines:
- Delivered to users when it is relevant to their current situation. The situation can be constructed or natural.
- Delivered in short sequences
- Relevant to the users current situation
- Include or directly relate to a practical element
- The information presented must in itself be easy to understand
- The most crucial points of the information should be highlighted
- Must be possible to opt-out or skip

5 Discussion

This paper reports on the latest steps of research that has been ongoing for several years and spanned several projects. The overall aim of the research has been to address the area of end-user training in information security. In this area, many suggestions for how to conduct information security and awareness training
have been presented and tested, yet we are still in the situation that end-user behavior remains one of the most highlighted threats in the cyber domain.

This research began with a review of the area and initial ideas for how information security training could be conducted leveraging theories about how humans are motivated to learn. It was found feasible to train users about topics that relate to what they are doing, and present training in situations where it is of direct relevance and use to the user. At this point, a suggested framework of goals and guidelines for how to implement training mechanisms was presented.

The suggested framework was tested and analyzed in two different contexts, higher education and password creation. Higher education was chosen because it offered an opportunity to present students with reoccurring training and an ability to measure not only the direct effect but also the learning outcomes some weeks after the training was performed, in the form of exams. Password creation was chosen as the other case since it offered a good way to measure the effects of the training. In this particular case, passwords created after being presented with a password guideline training module were measured and compared with passwords that were not created using the training module and was found to be stronger. As such, the two parts of the testing process shows that the CBMT framework can yield direct results and sustained knowledge for the user.

The emphasis in this paper has been the final refinement of the framework following the testing. The refinement was based on insights drawn during the implementation of the guidelines, conference discussions and qualitative data gathered during the testing phase. The refinement phase revealed that several users were positive to the CBMT learning modules they have used and some refinements that were previously presented.

The scientific contribution of this paper is further insight into how effective information security training should be carried out. It also presents a concrete framework for information security training that we consider to be a version 1.0. It is tested in some contexts but can be developed, tested and extended further and we encourage others to continue to research around the framework that we present. The research also raises an interesting ethical point, is it ethical to continue to use the training methods that are proven not to be effective or should effort be made into developing new and better methods?

The research also brings value to the practitioner community. First, the research has resulted in implementations of CBMT that are free to use\(^3\). Second, the paper present a concrete and tested framework for how effective information security and awareness training can be implemented.

While this paper present a framework that we argue is ready for use, there is still room for further development and verification. Future projects could take a pedagogical angle and review the framework from a pedagogical perspective.

\(^3\) Password guideline module: github.com/rr222cy/SecurityAssistantWidget, Cisco Certified Network Associate training videos: www.youtube.com/playlist?list=PLEjQDf4Fr75qADv9J0UaIUmB8zMcjw6V.
Another area for future work is to implement CBMT in more security-related contexts and evaluate the results. This can, for instance, include phishing, online fraud and more.

References

PAPER 7: CONSTRUCTING SECURE AND MEMORABLE PASSWORDS

Reprinted, as authors accepted manuscript, from Kävrestad, J., Lennartsson, M., Birath, M., & Nohlberg, M. (2020). Constructing secure and memorable passwords. Information & Computer Security. The final publication is available at Emerald via https://www.emerald.com/insight/content/doi/10.1108/ICS-07-2019-0077/full/html. License statement: 'This author accepted manuscript is deposited under a Creative Commons Attribution Non-commercial 4.0 International (CC BY-NC) licence. This means that anyone may distribute, adapt, and build upon the work for non-commercial purposes, subject to full attribution. If you wish to use this manuscript for commercial purposes, please contact permissions@emerald.com'
Constructing secure and memorable passwords

<table>
<thead>
<tr>
<th>Journal:</th>
<th>Information and Computer Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manuscript Type:</td>
<td>Original Article</td>
</tr>
<tr>
<td>Keywords:</td>
<td>passwords, Security, memorability, usability, stretegies, Computer Users</td>
</tr>
</tbody>
</table>
Constructing secure and memorable passwords

Abstract
Purpose – Using authentication to secure data and accounts has grown to be a natural part of computing. Even if several authentication methods are in existence, using passwords remain the most common type of authentication. Since long and complex passwords are encouraged by researches and practitioners alike, computer users design passwords using strategies that enable them to remember their passwords. This paper aims at finding strategies that allow for the generation of passwords that are both memorable and computationally secure.

Design/methodology/approach – The study began with a literature review that was used to identify cognitive password creation strategies that facilitate the creation of passwords that are easy to remember. Using an action-based approach, attack models were created for the resulting creation strategies. The attack models were then used to calculate the entropy for passwords created with different strategies and related to a theoretical cracking time.

Findings – The result of this study suggests that using phrases with four or more words as passwords will generate passwords that are easy to remember and hard to attack.

Originality/Value – This paper considers passwords from a socio-technical approach and provides insight into how passwords that are easy to remember and hard to crack can be generated. The results can be directly used to create password guidelines and training material that enables users to create usable and secure passwords.

Keywords passwords, memorability, security, strategies, computer security

1 Introduction
A big portion of almost everyone’s lives is linked with online services and various computer systems. We are using ICT (Information and Communications Technology) for everything from buying groceries to communication at work. Much like having a lock and key to protect what is of importance in the physical world and passports to prove your identity, the ability to identify yourself and what you are allowed to access is of high importance in the digital world. To prove one’s identity online, and thus proving yourself to be the owner of the account, authentication is used (Nielsen et al., 2014). The probably most common means of authentication are passwords (Nielsen et al., 2014, Houshmand and Aggarwal, 2017). Woods and Siponen (2018) even discuss that password use will continue to increase in the future making the need for secure passwords obvious.

While many actors try to emphasize the use of strong passwords, users tend to employ strategies to make their passwords easy to remember (Zviran and Haga, 1990, Ur et al., 2015, Stobert and Biddle, 2014). Pfleeger et al. (2015) discuss that users are afraid that they will forget their passwords if they do not employ some strategy to make them memorable. In a world where the number of accounts that every user must handle is growing, using those strategies is not at all strange. After all, the human memory is a limited resource not designed to keep track of multiple complex passwords (Vu et al., 2007). However, the consequence is that many passwords are inherently insecure and can be cracked in minutes.

The conflict between strong and memorable passwords opens up the discussion of what a secure password actually is. Much like Weirich and Sasse (2001), we argue that passwords are socio-technical properties where the user, as well as the computer system, must be considered equally. For a password to be computationally secure, it must be able to resist attacks for a reasonable amount of time, or in other words, be hard to guess using a dictionary or brute force attack. This property is typically achieved by having long passwords that contain different types of characters. It is reasonable to measure the computational security of a password in terms of how long the password can resist an attack.
Formally, that would mean dividing the total number of possible passwords by the number of passwords that can be tested in a given period of time. Seeing how users act to create memorable passwords, it is reasonable to conclude that a secure password should be computationally secure as well as memorable.

While the research and practitioner communities are well aware of the problems just described, the issue of users choosing insecure passwords remains and many organizations keep complexity requirements as the go-to solution for making users generate good passwords. However, influential standardization organs are shifting in what they recommend. NIST, for instance, removed complexity requirements from their password guidelines in favor of length (Grassi et al., 2017). Some large organizations such as Microsoft and OWASP are following and highlight understanding human behaviors as a key security factor (Microsoft, 2019, OWASP, 2019). However, other organizations including Yahoo and Apple maintain that a secure password should be complex (Yahoo, n.d; Apple, n.d). Looking at studies concerning adoption of security mechanisms, it appears clear that users tend to favor usability over security (Das et al., 2018, Whitten and Tygar, 1999). Das et al. (2018), however, shows that users are willing to actually use security features that are easy to use. Based on this, we argue that it is relevant and interesting to look into how users can be guided to create strong passwords with guidelines that are easy to use.

The purpose of this study is to meet the problem just described by looking for cognitive password creation strategies that can be used to create memorable passwords that are also computationally secure. The different password creation strategies described by Kävrestad et al. (2019) are taken into consideration in this study. First, a structured literature review is performed to identify the strategies that can help users create memorable passwords. Then, attack strategies are modeled for each identified strategy, and entropy for passwords generated with the strategies are calculated. The results identify password creation strategies that can assist in creating computationally secure passwords. As such, this paper will further the understanding about passwords and password security in general and provide the practitioner community with hands-on guidelines for how to teach users to create strong passwords.

The rest of this paper is structured as follows. Section 2 describes the methodology used in this study. Section 3 presents the outcome of the literature review and the entropy for passwords generated with strategies that support memorability. Finally, sections 5 and 6 present a discussion on the results and possible directions for future work.

2 Methodology

The aim of this paper is to identify cognitive strategies that can be used to create passwords that are computationally secure, and memorable. This goal was approached in a two-step process as follows:

1. A systematic literature review was conducted to identify cognitive strategies that help users create passwords that are memorable.
2. Strategies that fulfilled (1) were evaluated to see which of them also generate passwords that are computationally secure using an action based research approach with semi-structured interviews.

The password creation strategies taken into account in this study are based on Kävrestad et al. (2019), which describes the following password creation strategies:

- User-generated passwords which are passwords created by a user.
- System-generated passwords which are passwords generated by software.
- Words which are passwords that are simply a word.
- Word in word which are passwords created by putting one word into another, such as potatoam.
- Passphrases that are created by concatenating words.
- Mnemonic passwords that are generated by constructing a phrase and using the first letter in each word to form the password. i.e. I am a nice guy that is peeling potatoes could form the password Iaangtipp.
- Leetspeak which means that passwords are first created as words or phrases, then letters are substituted for other characters that visually resemble the original character. i.e., the password author could be 1tt1e@uthor.
- Patterns that define passwords generated by creating spatial patterns on the keyboard, such as using the corner keys or the top keyboard row.
- Letters that include passwords made up from upper or lower-case letters.
Numbers including passwords that are made up from numbers.
Special characters including passwords that are made up from special characters.
Alphanumerical which includes passwords that can be any combination of the three above classes.

The remainder of this section will describe how the two steps in the research process were implemented.

Systematic literature review
The literature review followed the process described by Kitchenham (2004). Kitchenham (2004) describes that a systematic literature review is usable when the aim is to summarize existing evidence concerning a phenomenon. It is, therefore, a suitable method in this case, where the goal is to summarize existing research concerning password memorability.

The outcomes of a literature review are heavily dependent on the databases used, search terms chosen, and the criteria applied to select relevant literature (Meline, 2006, Jesson et al., 2011). Brereton et al. (2007) state that it is important to include several databases in the review since no database alone is likely to contain all relevant papers. This literature review used the following six databases:

- IEEEExplore
- ACM Digital Library
- Science Direct
- HCI Bibliography
- Web of science
- Springer Link

The first three databases are suggested by Brereton et al. (2007) as relevant databases for software engineering making them appropriate for the topic at hand. The fourth database is aimed at human-computer interaction research and was picked due to its apparent affiliation with the topic researched. The last two databases are suggested by Kofod-Petersen (2015). The following search terms were used in all databases and the search was limited to papers published 2005 and later:

- password AND memorability
- password AND usability
- authentication AND memorability
- authentication AND usability

Following the initial searches, which resulted in 15,228 articles, the papers were analyzed to see if they meet inclusion and exclusion criteria specified for the study. Duplicates were also removed at this stage, resulting in 33 papers that were selected for further analysis. Wohlin (2014) suggests the use of backward snowballing to avoid missing relevant articles. During this process, all papers cited in the papers selected during the initial search are considered for inclusion in the analysis. Backward snowballing was employed in this study and resulted in another 28 papers that were included in the analysis, resulting in 59 included papers. Since the space available in this paper is limited, the inclusion and exclusion criteria used are summarized in Figure 1, below.
The selected papers were analyzed with a qualitative approach influenced by Wolfswinkel et al. (2013) and Braun & Clarke (2006). The analysis was conducted using the software MAXQDA and divided into the following three steps:

1. The different password creation strategies considered in this study were established as themes. This approach was used because, as discussed by Braun & Clarke (2006), pre-established themes tend to generate an in-depth analysis of some aspects of the data. In this case, the aim of the study is to generate information specifically about the memorability of certain passwords.

2. All papers were read and all text excerpts concerning password memorability were highlighted. This step is similar to the open-coding process presented by Wolfswinkel et al. (2013).

3. All marked excerpts were re-read and classified into the established themes. The sum of excerpts in each theme was further analyzed to draw conclusions about the memorability of the password creation strategies.

Action based semi-structured interviews

The result of the systematic literature review was a listing of password creation strategies that could aid users in creating memorable passwords. In the second step of the research process, an action-based approach was used to model attack strategies for passwords generated with the different strategies. The attack models were used to calculate the password entropy for passwords generated with each password creation strategy. Password entropy is defined as the number of attempts an attacker would need to exhaust all possible passwords in a case where she knows the password creation strategy used to create the password.

To create the attack models, the researchers created formal definitions of the password creation strategies and corresponding attack models. Those were used as input to interviews with one expert from each of the fields: computer forensics, penetration testing, and algorithm design. The interviews were carried out individually in a semi-structured way and analyzed using thematic coding, and the results of the interviews were used to refine the definitions and attack models.
Once the attack models were established, the entropy for each attack model and corresponding brute-force attack was calculated. The time needed to exhaust the entropy was also calculated as the entropy divided by the number of passwords that can be tested per second. How many passwords that can be tested per second is an ever-changing variable that depends on the advances of technology. Furthermore, different cryptosystems require different efforts (Kävrestad, 2018). Hitaj et al. (2019) state that it is now possible to test billions of passwords per second and a study by Brumen (2019) uses 6,877 billion password tests per second as their metric. For the purposes of this paper, we will calculate computational security in terms of how long a password can resist an attack given that 10 billion passwords can be tested per second.

3 Results

This chapter presents the data gathered during the research process. First, the systematic literature review is presented, resulting in a number of cognitive strategies that can assist in creating passwords that support memorability. Those strategies are then evaluated to identify which ones that can also generate passwords that are computationally secure.

Identifying password creation strategies that result in memorable passwords.

Following the literature search and application of inclusion and exclusion criteria, 59 papers were selected for analysis. During the analysis, passages in the papers that described how the considered classes supported or didn't support, the creation of memorable passwords were marked and analyzed. During the open coding, passages that could be interpreted as discussing password memorability were identified. Using axial coding, those passages were tied to the password creation strategies of interest in this paper, and during selective coding, the papers' distinction on whether or not the password creation strategy supported the creation of memorable passwords was identified. A summary of the results gathered is presented in Table 1, below. Note that no papers discussing the class word-in-word were found during the analysis.
<table>
<thead>
<tr>
<th>Password creation strategy</th>
<th>Papers describing high support for memorability</th>
<th>Papers describing low support for memorability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leetspeak</td>
<td>Keith et al. (2009)</td>
<td>Shay et al. (2015), Shay et al. (2016)</td>
</tr>
<tr>
<td>Patterns</td>
<td>Juang et al. (2012), Weiss and De Luca (2012), Shay et al. (2014), Veras et al. (2012), Keith et al. (2009)</td>
<td></td>
</tr>
<tr>
<td>User-generated</td>
<td>Nelson and Vu (2010), Shay et al. (2010), Vy et al. (2007), Huh et al. (2015), Keith et al. (2009), Nelson and Vu (2009)</td>
<td></td>
</tr>
<tr>
<td>Letters</td>
<td>Inglesant and Sasse (2010), Pilar et al. (2012), Shen et al. (2016), Weir et al. (2010), Bhuyan et al. (2013)</td>
<td>Inglesant and Sasse (2010), Pilar et al. (2012), Shen et al. (2016), Weir et al. (2010), Bhuyan et al. (2013)</td>
</tr>
<tr>
<td>Alphanumerical</td>
<td>Pilar et al. (2012), Melicher et al. (2016)</td>
<td>Marquardson (2012), Shay et al. (2010), Greene et al. (2014), Pilar et al. (2012), Melicher et al. (2016)</td>
</tr>
</tbody>
</table>
On an abstract level, the analyzed papers concur that user-generated passwords support memorability to a much larger extent than system-generated passwords. As described by, for instance, Huh et al. (2015) and Vu et al. (2007) it is easier to recall a password that has some personal meaning for the user. Further, passwords that are more complex also seem harder to remember, Melicher et al. (2016) discusses this in the context of alphanumerical passwords and concludes that there is a relation between using many different character classes and poor memorability. It should also be mentioned that too little data was found regarding Leet-speak passwords to draw any conclusions in regards to that strategy.

The literature review aimed to identify password creation strategies that facilitated the creation of passwords that are easy for the user to remember. Considering the information found during the literature review, the password creation strategies that facilitate the creation of memorable passwords are the following:

- Biographical passwords
- Words
- User-generated Mnemonic passwords
- User-generated patterns
- User-generated passphrases

Evaluating the complexity of passwords generated with strategies that support memorability

Following the literature review, the password creation strategies that support the creation of memorable passwords were evaluated to see in what way they support the generation of computationally secure passwords. Since biographical passwords embody a characteristic rather than a pattern that can be modeled, the following password creation strategies were taken into account during this step:

- Words
- Mnemonic passwords
- Patterns
- Passphrases

The evaluation was carried out by creating formal definitions and attack models then used to calculate a theoretical entropy for passwords generated with the different strategies. A higher entropy would suggest a more difficult password to attack. The entropy when attacking a password using a brute force attack was also calculated for comparison.

Several entropy calculations involved testing English words combined with each other. The number of English words was assumed to be 600 000 as suggested by the Oxford English Dictionary (Oxford English Dictionary, 2019). However, the actual amount of words known to an average adult, and thus the number of words likely to be used in a password, is much lower. Laufer (1998) approximates that an 18-year old’s vocabulary is about 20 000 words and a more recent study by Brysbaert et al. (2016) finds that the average 20-year old knows 42 000 lemmas, while a 60-year old knows 48 200. Thus, it is reasonable to also base entropy calculations on a number that resembles a reasonable average vocabulary, the amount used in this study is 45 000. A second metric used for entropy calculations was average word length. Smith (2012) suggests that the average length for an English word is 9.1 letters, while Bochkarev et al. (2015) suggest that the average word length is 5.1 if word length is measured based on the frequency of word use. Entropy calculations will be performed using both 9.1 and 5.1 as average word length. To summarize, the following variables are used through the remainder of this chapter:

- Word \((W) = 600 000 \text{ or } 45 000\)
- Average word length \((AWL) = 9.1 \text{ or } 5.1\) characters
- \(n\) is used as a variable for password length

The definitions and attack models were created using an action based approach where the researchers created drafts that were then evaluated and refined using input from one respective expert in the fields of digital forensics, penetration testing, and software testing. Semi-structured interviews were held separately with the three respondents and the interviews were analyzed using thematic coding where the four different password creations strategies were used as themes.
Table 2, below summarizes the definitions and attack models that were established during the interviews. The table also includes equations used to calculate the entropy resulting from each attack model and the equation for calculating the entropy related to attacking the same password type with a brute force attack.

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Formal definition</th>
<th>Attack model</th>
<th>Entropy equation (attack model)</th>
<th>Entropy equation (Brute force)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Words</td>
<td>Passwords made with a single standard dictionary word</td>
<td>Test every word in a standard dictionary</td>
<td>Word</td>
<td>$52^{\text{AWL}}$ The number of English letters to the power of the average word length</td>
</tr>
<tr>
<td>Phrases</td>
<td>Passwords created by combining any number of words from a standard dictionary. The words may be separated by one of the special characters,.!? or space.</td>
<td>Test any combination of words in a standard dictionary. Words may or may not be separated by one of five special characters.</td>
<td>$(\text{words}+5)^n$</td>
<td>$57^{(n*\text{AWL})+1}$ The number of English letters plus the five special characters to the power of the password length in words times the average word length plus one, since the password may end with a special character.</td>
</tr>
<tr>
<td>Mnemonic</td>
<td>Passwords created by first creating a phrase and then use the first letter of each word as the password. The letters may be separated by one of the special characters,.!? or space.</td>
<td>Test any combination of the first letter of words in a standard dictionary. Words may or may not be separated by one of five special characters.</td>
<td>$(\text{word}+5)^n$</td>
<td>$57^{(n+1)}$ The number of English letters plus the five special characters to the power of the password length in characters plus one, since the password may end with a special character.</td>
</tr>
<tr>
<td>Pattern</td>
<td>Passwords created by forming a pattern of keys that are adjacent to an English keyboard. The password can be made up from any of the characters on the adjacent keys.</td>
<td>Generate a dictionary for possible passwords by starting at a key x as the first password character, and then use every key adjacent to x as possible second characters, and then use every key adjacent to any of the second characters and possible third characters and so on.</td>
<td>Entropy numbers are taken from simulations performed by Chou et al. (2012).</td>
<td>$9^4$ As suggested by Chou et al. (2012).</td>
</tr>
</tbody>
</table>

Following the creation of the attack models, the entropy for each password creation strategy was calculated for passwords of length 1-10 units. A unit is the number of words or characters, whichever is suitable for the attack model. In combination with presenting the entropy when using the attack models, the entropy for a case where the same password is attacked using a brute force attack is also presented. A summary of the entropy calculations is presented.
in Figure 2, below, where the entropy of different attack scenarios is presented as logarithms to base 10. Figure 2 also holds the time needed for a password guessing attack that tests all possible passwords, with a rate of 10 billion passwords per second. Note that Figure 2 only presents a subset of the calculations made, due to space limitations.

Figure 2 Summary of entropy calculations, all numbers are presented as logarithms to base 10. Crack times according to the established cracking capabilities are shown in parenthesis.

As seen in figure 2, the attack capabilities established in this paper suggest that any password with a lower entropy than $10^{15}$ would be cracked in under one day. As such, the only password creation strategies that can generate secure passwords are passphrases or mnemonic passwords of at least ten characters. Ten-character patterns are hard to crack with a brute force attack. However, those passwords can be cracked in minutes using the attack model, suggesting that the attack model is a feasible attack. Looking to mnemonic passwords, the attack models generate extremely high cracking times and should, therefore, be considered useless and the computational security of mnemonic passwords would be based on brute force attacks. In this scenario, mnemonic password must be more than 8 characters long to reach a cracking time of more than a few days. Passphrases, on the other hand, result in high entropy even when created with just a few words. Even when using the best attack and the smallest word list, a four-word phrase would take several years to crack. The statement holds even considering the laws of probability, that state that only half the entropy needs to be tested before the password is cracked.

4 Conclusion

The overall aim of this study was to identify ways for users to create passwords that are computationally secure and easy to remember. First, the password creation strategies suggested by Kävrestad et al. (2019) were analyzed in order to identify the strategies that support the creation of memorable passwords. While there is no comprehensive study conducted with the aim of analyzing the memory aspect of all possible password creations strategies, there is a lot of
literature available on the topic. Thus, a systematic literature review was deemed suitable. The literature review showed that there is a strong consensus in the field regarding that passwords created by the user herself are easy to remember while passwords that are system generated are hard to remember. Further, passwords that hold a meaning for the user are easier to remember than other passwords and there seems to be a correlation between using many character groups and having a hard time remembering the password. Concretely, this study found that user-generated passwords that are words, passphrases, mnemonic passwords or patterns are easy for users to remember.

In the second part of the study, the password entropy for the just-mentioned password creation strategies was calculated and compared to the entropy of corresponding brute force attacks. This was done using an action based approach where attack models were developed with experts within the field. The results of this step were that passphrases can assist users in creating passwords with high entropy, and that are thus, computationally secure. The results also indicate that long passwords created with a mnemonic or patterns based strategy could be computationally secure. However, the literature review suggests that length requirements can interfere with memorability.

The logical conclusion of this study is that passphrases are a reasonable suggestion on how to create memorable passwords that are also computationally secure. As a direct result of that insight, this paper suggests that password guidelines and training should propose the use of passphrases, and possibly include separating and ending special characters. A reasonable recommendation would be that the ordinary user would be secure enough with a four-word passphrase and a professional user could be satisfied with a five-word, or longer, passphrase. Suggesting that user-generated passwords should focus more on length and memorability than complexity is well in line with NIST’s password guidelines that exclude complexity requirements and suggest that passwords should be at least 8 characters long, but users should be encouraged to create as long passwords as they want (Grassi et al., 2017).

5 Discussion

Computational security can be measured in a variety of ways, it should also be mentioned that the entropy calculated in this study is dependent on the formal definitions used. Also, the entropy is only accurate if the attacker knows what type of password to attack. To ensure that the results are valid and reasonable, the approach in this paper was to let the attack model be as simple as possible, and let the attacker have as much power as possible to create a “best-case” scenario for the attacker. For instance, the attack model for an 8-character long pattern-based password results in an entropy of $10^{9.5}$ (or just over 3.1 billion) possible passwords and can be cracked in a matter of seconds. That number is discussed in terms of the number of attempts an attacker would have to make before she can be sure that she cracked the target password. That is only true if the attacker knows that she is set to attack a password that is an 8-character long pattern-based password, and that is rarely the case. Thus, the actual difficulty of attacking any of the passwords discussed in this paper will in practice be much higher than what the results of this study let on.

It should be mentioned that password security is a complex area and this paper focus on one part of it. Another important area is password reuse, and on this topic, it should not go unmentioned that reusing the same password means that the password security can be compromised if there is a leak at any of the services where the passwords are used, regardless of the password complexity (haveibeenpawed.com, 2018). A possible way to mitigate the problem of password re-use would be to suggest that users include the site or service name where the password is used in the actual password. This approach would work as “password salting” and could at least mitigate automated attacks using leaked passwords. How that approach would affect password security is a topic for further research. This paper assumes that all possible passwords in an entropy are equally common. It is well known that users tend to select passwords with a deeper personal meaning and that some words are more common than others in passphrases. Those aspects are not considered in this study.

The remainder of this section will conclude this paper with a discussion of the limitations of this research and the papers contribution and directions for future work.

Limitations of this work
The purpose of this paper was to research methods for creation of passwords that are usable and computationally secure by identifying cognitive password creation strategies that can be used to create memorable passwords that are also computationally secure. The paper uses the password creation strategies listed by Kävrestad et al. (2019) and has not considered any other possible password creation strategies. Should any new cognitive password creation strategies arise, the methodology applied in this paper could be applied to that strategy in order to evaluate the new strategies against the strategies evaluated in this paper. It should also be mentioned that this paper only considers password entropy as a measure of computational security, while aspects such as password re-use are also very important security concerns.

Societal contribution
Password security is hard to obtain and continuous reports of password leaks show that users tend to select passwords that are indeed poor. The literature suggests that this is due to the fact that users create passwords that are easy to remember and prioritize usability over security. This paper shows how passwords that meet the users’ need for memorability and high-security demands can be created using cognitive password creation strategies. As such, this paper helps the computer user with hands-on tips on how to create good passwords. Further, the results could be used by practitioners of information security when designing security policies and information security training.

Scientific contribution
The main scientific contribution of this paper is that it provides a summary of existing, and fragmented, research around memorable passwords. While a lot of previous studies considered memorability for some distinct types of passwords, this study provides a compilation of previously existing knowledge around the memorability of different types of passwords. Also, this study highlights how different password creations strategies support the creation of memorable passwords.

Future work
This paper aimed to identify password creation strategies that can generate computationally secure memorable passwords. While the paper succeeded in doing so, the examined literature reveals that passwords are indeed a complicated topic. Considering passwords to be a socio-technical property opens up the discussion around password security to include usability as well as complexity. Thus, other factors such as password reuse and training users to actually create good passwords are areas that, while well researched, still remain unresolved. Obvious directions for future work would, for instance, be to examine how the password creation strategies discussed in this paper can minimize user’s need and tendency to reuse passwords, for instance using salting. Another direction would be to research how users can be trained, and motivated, to actually make use of good security practices and techniques, discussed in this paper and elsewhere, by for instance look into how passwordless options could be widely adopted.
References


JEYARAMAN, S. & TOPKARA, U. (2005), “Have the cake and eat it too - infusing usability into text-password based authentication systems.”, 21st Annual Computer Security Applications Conference (ACSAC'05), IEEE.


KITCHENHAM, B. (2004), Procedures for performing systematic reviews., Keele University, Keele, UK.

KOFOD-PETERSEN, A. (2015), How to do a Structured Literature Review in computer science.


Figure 1 Paper selection

190x173mm (120 x 120 DPI)
PAPER 8: EVALUATION STRATEGIES FOR CYBERSECURITY TRAINING METHODS: A LITERATURE REVIEW

 Evaluation Strategies for Cybersecurity Training Methods: A Literature Review

Joakim Kävrestad and Marcus Nohlberg

University of Skövde, Skövde, Sweden
{joakim.kavrestad,marcus.nohlberg}@his.se

Abstract. The human aspect of cybersecurity continues to present challenges to researchers and practitioners worldwide. While measures are being taken to improve the situation, a vast majority of security incidents can be attributed to user behavior. Security and Awareness Training (SAT) has been available for several decades and is commonly given as a suggestion for improving the cybersecurity behavior of end-users. However, attackers continue to exploit the human factor suggesting that current SAT methods are not enough. Researchers argue that providing knowledge alone is not enough, and some researchers suggest that many currently used SAT methods are, in fact, not empirically evaluated. This paper aims to examine how SAT has been evaluated in recent research using a structured literature review. The result is an overview of evaluation methods which describes what results that can be obtained using them. The study further suggests that SAT methods should be evaluated using a variety of methods since different methods will inevitably provide different results. The presented results can be used as a guide for future research projects seeking to develop or evaluate methods for SAT.

Keywords: Security · Evaluation · Methods · Awareness · Training · User

1 Introduction

It is well-established that insecure user behavior is one of the major challenges in cybersecurity [36]. Targeting users rather than technology is common practice for many attackers, and the need to make users more resilient to social engineering is apparent. As such, there is an obvious need to improve user behavior in regards to cybersecurity [6]. To this end, users must be helped to understand the consequences of their actions and learn how to act more securely [13]. For that purpose, user training is the go-to solution suggested in scientific research and offered by practitioners [23,32].

Security and Awareness Training (SAT) has been discussed in the scientific literature for at least two decades [38]. However, recurring reports of attacks suggest that the problem of insecure user behavior is nowhere near being solved.
Evaluation Strategies for Cybersecurity Training Methods

On the contrary, industry reports describe that human-related attacks are the most common attacks, suggesting that up to 95% of attacks include the human element [12,15,39]. Some researchers even suggest that organizations’ training programs are often not grounded in empirical evidence of their effectiveness [1,2]. Seeing how the problem of insecure user behavior is certainly not resolved, the need for further research into this area is apparent.

The goal of any SAT effort is to convey knowledge to the user so that she knows what to do, understands why to do it and how to do it [38]. As such, the ultimate goal is to improve the user behavior regarding security by providing the user with knowledge and understanding. Recent research suggests that providing knowledge is not enough as knowing what to do does not necessarily translate to correct behavior [4,31]. It is easy to argue that the proper way to evaluate SAT efforts would be to evaluate the actual outcome, the effect on cybersecurity behavior. However, such studies bring practical as well as ethical concerns. Studies on human behavior must adhere to rigorous ethical principles that impact what can be done and how, as exemplified by [35]. Practically, experimental evaluations are hard to perform, leaving room for the use of other evaluation methods [46].

This paper aims to explore recently published work in the domain of end-user cybersecurity training to identify how such training methods are evaluated and outline considerations related to the identified evaluation methods. This was done through a structured literature review where included papers were analyzed using thematic coding. The results provide insight into what evaluation methods that are used for the evaluation of SAT and what results that can be expected from them. As such, it can be used to guide future research into SAT development by providing a reference for making informed methodological decisions and respond to the need for empirically evaluated SAT methods. The results also identify what SAT methods that have been evaluated in recent research.

2 Methodology

The study was performed as a structured literature review (SLR) which followed the process outlined by [30]:

1. Formulate a research question or aim.
2. Perform literature searches.
3. Apply inclusion and exclusion criteria.
4. Perform quality assessment.
5. Extract data.
6. Analyze data.

As described by [22,27], selecting search terms and databases are essential tasks in an SLR. The search term used in this study was designed to be inclusive and capture all papers discussing end-user cybersecurity training. While a more restrictive query could have been designed, we argue that a broad search is more likely to capture all relevant studies, even if it results in a higher manual
workload regarding the application of selection criteria. The query was expressed as follows: *security AND (training OR education) AND user*. Note that the query was modified to match the syntax of the databases used in the study. The search term was applied to titles, abstracts, and keywords to focus the results. This was motivated by the argument that papers that do provide important information concerning the aim of the study are focused on cybersecurity training of end-users and will therefore include all search words in the metadata. To increase the chance that the study includes all important papers on the topic, an inclusive mindset was applied in choosing databases resulting in the use of *Scopus, Web of Science (core collection), Science Direct, dblp, and Usenix*.

All identified papers were evaluated against inclusion criteria. As suggested by [48], the criteria were established before the search process started to avoid bias during the selection process. The criteria were first applied to the abstracts of the identified papers. Paper that clearly failed to meet the criteria were excluded before the criteria were applied to the full remaining papers. Papers written by the authors of this paper were also excluded from the study to minimize bias. The criteria for inclusion were the following:

1. Published 2015 or later.
2. Not a duplication of another included paper.
3. Published in peer-reviewed journal or conference.
4. Free to access for the author.
5. Written in English.
6. Discusses the topic of this study.
7. Reports on one or more evaluations of SAT methods.

The first five criteria were used to limit the body of included papers to recent high-quality research and were, to some extent, applied automatically during the search process where publication year, language, and outlet could be configured during the search. The last two criteria were included to ensure that identified papers specifically discussed end-user training in the cybersecurity context and that they reported on findings based on their own data rather than conclusions based on cited material or similar. The included papers were analyzed using thematic coding in an open fashion, as described by [5]. During the analysis process, the papers were read and categorized in three steps:

1. All papers were read and individual methods of cybersecurity training were identified.
2. The papers were reread with the focus of identifying individual ways of evaluating training methods.
3. The goal and outcome of the evaluations presented in the papers were analyzed. At this stage, the papers were positioned according to what method they evaluated and how with the intent of analyzing how various evaluation methods are used.

EndNote Desktop was used for the categorization and coding of included papers.
3 Results

The searches, conducted on 2020-09-07, resulted in a total of 3664 papers, distributed among the included databases as follows:

- Scopus: 1997 hits
- Web of science: 1495 hits
- Science Direct: 129 hits
- dblp: 13 hits
- Usenix: 30 hits

All papers and their abstracts were loaded into EndNote, and duplicate papers were removed automatically during this process. Next, the titles and abstracts of all papers were scanned, and papers that clearly failed to meet the inclusion criteria were removed from the study, leaving 106 candidate papers. The inclusion criteria were then applied to the full body of those papers, resulting in 28 papers that were included in this study. Those papers were analyzed using thematic coding as described throughout the rest of this section.

3.1 Initial Categorization of Included Papers

During the first analysis stage, the papers were first categorized according to what type of cybersecurity training they evaluated, resulting in an overview of what SAT methods have been evaluated in recent work. An overview and listing of papers included in the review are presented in Table 1. Included papers will from hereon be referenced by the label (Ax) provided in Table 1; the number in brackets point to the entry in the reference list that provides a full reference to the respective papers.

3.2 Identification of Evaluation Methods

Following the identification of cybersecurity training types, the papers were once again analyzed focusing on what kind of evaluations they contained. At this point, four distinct methods of evaluation were identified in the papers:

- Perception evaluations: Evaluations that focused on users’ perception of a training method. This included usability studies and typically aimed to evaluate if users liked the proposed method.
- Knowledge evaluations: Evaluations that measured the knowledge gained by participants using a certain method of training.
- Simulation: Evaluations that measured security outcomes, such as phishing resilience or password behavior in a simulated scenario.
- Experimental: Evaluations that measured security outcomes, such as phishing resilience or password behavior in a naturalistic setting.
Table 1. List of included papers and initial categorization

<table>
<thead>
<tr>
<th>Papers</th>
<th>Category</th>
<th>Category description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1: [34], A2: [3], A3: [40], A4: [44], A5: [19]</td>
<td>Several</td>
<td>Papers evaluating several training categories</td>
</tr>
<tr>
<td>A6: [14], A7: [20], A8: [17], A9: [10], A10: [28], A11: [21], A12: [18], A13: [37], A14: [47]</td>
<td>Gamification</td>
<td>Papers evaluating gamified training</td>
</tr>
<tr>
<td>A15: [7], A16: [41]</td>
<td>Interactive online</td>
<td>Papers evaluating interactive material delivered online</td>
</tr>
<tr>
<td>A17: [45], A18: [25], A19: [42]</td>
<td>Lecture</td>
<td>Papers evaluating instructor-led lectures</td>
</tr>
<tr>
<td>A20: [26], A21: [49], A22: [1], A23: [51], A24: [24], A25: [9], A26: [50]</td>
<td>Situation aware</td>
<td>Papers evaluating training delivered in a situation where it is usable</td>
</tr>
<tr>
<td>A27: [29]</td>
<td>General_1</td>
<td>Evaluates the impact of progression in difficulty of material</td>
</tr>
<tr>
<td>A28: [33]</td>
<td>General_2</td>
<td>Evaluated how a variety of simultaneous methods affected phishing resilience in an organization</td>
</tr>
</tbody>
</table>

3.3 Analysis of Evaluation Methods

The included papers were analyzed once again, focusing on the methods the papers used for evaluation, the author’s comments on the used evaluation methods, and the rationale for adopting certain methods. The result in this step is an overview of what research goals are addressed using the four distinct methods of evaluation. Table 2 provides an overview of which evaluation methods are discussed in the included papers, and the remainder of this section describes the evaluation methods in more detail.

Table 2. Overview of evaluation types presented in the included papers

<table>
<thead>
<tr>
<th>Evaluation type</th>
<th>Papers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perception</td>
<td>A3, A4, A6, A7, A8, A9, A10, A12, A16, A23</td>
</tr>
<tr>
<td>Knowledge</td>
<td>A5, A11, A16, A17, A19</td>
</tr>
<tr>
<td>Simulation</td>
<td>A1, A2, A3, A4, A7, A12, A14, A15, A18, A21, A23, A24, A27</td>
</tr>
<tr>
<td>Experiment</td>
<td>A4, A5, A6, A13, A20, A22, A25, A26, A28</td>
</tr>
</tbody>
</table>

Ten of the included papers report on evaluations based on assessing participants perception using interviews or surveys. Two main types of studies can be
identified where one evaluates users’ perception of their own skill or knowledge. In contrast, the other evaluates the users’ perception of a SAT method often in terms of how enjoyable or usable it is. A rationale provided as a motivation for perception evaluations is that a more enjoyable SAT is more likely to be used by the intended users in a naturalistic setting. The most frequently discussed shortcoming is that it cannot assess the actual effect on user behavior.

A similar type of evaluation is knowledge based evaluation where the participants’ knowledge is measured, often using a survey. The rationale is that knowledge about correct behavior is a pre-condition for correct behavior. Similar to perception evaluations, a shortcoming is that actual behavior is not assessed. However, a potential benefit compared to evaluation based on perception is that risk of response bias can be lesser.

Simulations measure the effect of SAT on security behavior but in a simulated environment. Simulations are presented in 13 of the included papers. The most commonly presented study type measures the participants’ ability to distinguish between legitimate and fraudulent emails after being subjected to SAT. A few studies employ a pre-validated security awareness instrument to measure the SAT’s effect on security awareness. A1 mentions that participants will likely be primed since they know that they participate in a study, and A21 argues that as a reason for why a simulation cannot fully mimic a natural scenario. However, the rationale for using simulations over naturalistic experiments is that simulations can provide insight into behavioral change without ethical and procedural difficulties that are often associated with experiments.

Experiments are used in nine of the included papers and measure security behavior in a naturalistic setting. Experiments are often performed using penetration testing techniques or by monitoring behavior in an organization after SAT is deployed. A rationale for using experiments is that the effect on actual behavior can be measured and observed, but several included papers demonstrate that experiments present ethical and procedural challenges. The ethical challenges stem from the fact that participants are often involved without explicit informed consent, or with informed consent that does not disclose the full extent of the experiment. The argument is that telling participants that their security behavior will be studied may influence their behavior (A11, A22, A26, A28). A workaround is to use limited informed consent and debrief participants upon study completion. Another workaround is to perform the study in an organizational setting and get permission from the organization. A practical difficulty involves that experiments with deceptive components need to consider ethical clearance.

In addition to the distinct evaluation types, the coding process identified several additional methodological considerations, and those are accounted for next. The first consideration relates to the study design, where the included papers demonstrate diversity. Between-group, pre-post, and one-shot case studies are present for all four evaluation methods. One-shot case studies report on the evaluation of a single SAT method, and an obvious drawback is that it cannot provide insight into how the SAT compares to other SAT methods. One-shot
case studies are most prominently used when evaluating the users’ perception of a single SAT method. Pre-post tests typically involve a study design where participants are subjected to a measure, then presented with SAT before they are again measured. The rationale is that the effect of the SAT is then isolated. Finally, the Between-group design includes subjecting different groups to different SAT methods to compare the effects, often including one group that is not subjected to any SAT method. A rationale for using a between-group design over a pre-post test is that the pre-post test design provides an increased risk of participation bias which is arguably especially risky in studies evaluating security awareness and behavior.

Another aspect discussed in several included papers (e.g., A6, A7, A14, A15, A18) is knowledge retention, but this is only evaluated in a few of the included studies. In relation to knowledge retention, studies report that the effect of several SAT methods seems to wear off after a certain amount of time (A6). A second aspect considered in some of the included papers is if the participants would have participated in SAT if it was voluntary (A8, A10). Assessing if participants would participate voluntarily is important since prospective users need to participate in SAT for the training to be able to provide its intended effect. The effect of user unwillingness to participate in SAT is hard to account for in evaluations. A related consideration mentioned in A18 is a possible bias stemming from the participants’ participation itself. Participants who know that they participate in an awareness evaluation are likely to be more aware compared to when they are not informed about the evaluation.

3.4 Discussion on the Results

This paper reports on a structured literature review where 28 papers evaluating SAT methods were included. The evaluation methods used are classified as Perception evaluations, knowledge evaluations, simulations, and experiments. The analysis of how they are used and argued for demonstrates that they all have different benefits and shortcomings. While the end goal of any SAT is to improve user behavior, and experiments are arguably the only method that is fully capable of evaluating effects on behavior, they are practically and ethically challenging to perform. Simulations provide a less complicated alternative but are also argued to be less reliable [16, 43]. A second benefit of simulations is that the controlled nature of them allows for follow-up interviews with participants. Further, voluntary user participation is argued to be an important aspect of SAT, and perhaps the only evaluation method that captures that is perception evaluations. As such, an insight from this SLR is that an extensive SAT development project should evaluate its outcomes using diverse evaluation methods.

The results further demonstrate that bias and ethics present tough challenges for the evaluation of SAT. In addition to sources of bias common to most research on human subjects, SAT evaluations essentially evaluate awareness. A participant who participates in an awareness evaluation is bound to be more aware than the regular user. The results demonstrate that the study design is of high importance and aligns with previous publications in research methodology [8].
Concerning research ethics, true experiments are likely to involve deception and can include handling sensitive data, which is ethically challenging and highlights the importance of ethical reviews and ongoing ethical discussions.

As for the limitations of this particular study, an SLR is dependant on its included papers and therefore on its search and selection process. The process in this study was designed to include research published from the past five years in five different databases. While a broader selection of papers could have generated a larger empirical base, we argue that the included 28 papers are enough to provide insight into the evaluation methods used in recent research in this domain. This was also demonstrated by saturation experienced by the researchers during the analysis. A second possible risk in qualitative research is researcher bias, given the researchers’ heavy involvement in the analysis process. While difficult to minimize, researcher bias was handled in this study by ensuring that it was reported on in a way that enabled replication. The search, selection, and analysis process have been documented to ensure that it can be replicated and scrutinized by others.

4 Conclusions

This paper aimed to explore recently published work in the domain of end-user cybersecurity training to identify how such training methods are evaluated and outline considerations related to the identified evaluation methods. The paper identifies the four distinctive methods of Perception evaluations, knowledge evaluations, simulations, and experiments and shows that all are used in different evaluations of SAT with different challenges and benefits. As such, this study concludes that all identified evaluating types should ideally be used during the development of SAT methods. On this note, experiments and simulations are needed to provide empirical evidence as to how efficiently SAT methods can improve cybersecurity behavior while studying user perceptions of SAT methods is important in order to analyze the likelihood that users will opt to use the SAT voluntarily. The study further suggests that SAT evaluations should pay great attention to ethical challenges and bias stemming from mere participation in such studies, not least when deciding what study design to employ. This review also demonstrates that interactive and gamified training has received significant interest from researchers over the past five years.

The contribution of this paper is to the scientific community, where it provides an overview of evaluation methods used for the evaluation of SAT. The results can support future studies by providing insight into what results to expect from different evaluation methods and important considerations related to the use of the different methods. Consequently, the paper can contribute to the quality of future SAT development projects, and in the long run, to the practitioner community, which will receive even better guidelines for how to implement SAT.

This study identified participation bias and ethical challenges as two difficulties that are to be considered when evaluating SAT methods. A suggested direction for future work would be further studies into the design of ethically
sound evaluation methodologies where bias is minimized. A second direction for future work is more studies concerning the retention of knowledge gained from SAT methods. While knowledge retention is mentioned in several of the papers included in this study, it is only evaluated in a few of those.

References


44. Tschakert, K.F., Ngamsuriyaroj, S.: Effectiveness of and user preferences for security awareness training methodologies. Heliyon 5(6), e02010 (2019)


PAPER 9: EVALUATION OF CONTEXTUAL AND GAME-BASED TRAINING FOR PHISHING DETECTION

Evaluation of Contextual and Game-Based Training for Phishing Detection

Joakim Kävrestad 1*, Allex Hagberg 2, Marcus Nohlberg 1, Jana Rambusch 1, Robert Roos 2 and Steven Furnell 3

1 School of Informatics, University of Skövde, 541 28 Skövde, Sweden; marcus.nohlberg@his.se (M.N.);
jana.rambusch@his.se (J.R.)
2 Xenolith AB, 541 34 Skövde, Sweden; allex@xenolith.se (A.H.; robert@xenolith.se (R.R.)
3 School of Computer Science, University of Nottingham, Nottingham NG7 2RD, UK;
steven.furnell@nottingham.ac.uk
* Correspondence: joakim.kavrestad@his.se

Abstract: Cybersecurity is a pressing matter, and a lot of the responsibility for cybersecurity is put on the individual user. The individual user is expected to engage in secure behavior by selecting good passwords, identifying malicious emails, and more. Typical support for users comes from Information Security Awareness Training (ISAT), which makes the effectiveness of ISAT a key cybersecurity issue. This paper presents an evaluation of how two promising methods for ISAT support users in achieving secure behavior using a simulated experiment with 41 participants. The methods were game-based training, where users learn by playing a game, and Context-Based Micro-Training (CBMT), where users are presented with short information in a situation where the information is of direct relevance. Participants were asked to identify phishing emails while their behavior was monitored using eye-tracking technique. The research shows that both training methods can support users towards secure behavior and that CBMT does so to a higher degree than game-based training. The research further shows that most participants were susceptible to phishing, even after training, which suggests that training alone is insufficient to make users behave securely. Consequently, future research ideas, where training is combined with other support systems, are proposed.

Keywords: usable security; cybersecurity training; ISAT; SETA; phishing; user awareness; security behavior

1. Introduction

The world is continuing a journey towards an increasingly digital state [1]. The use of computers and online services has been a natural component of the lives of most people in developed countries for decades and adoption in developing regions is on the rise [2]. Furthermore, populations that previously demonstrated low adoption rates are now adopting and using digital services at a rapid pace [3,4]. This development is positive. On a national level, Internet adoption has been shown to positively impact financial development [2]. On the individual level, the use of digital services makes it easier for the individual to access information, healthcare, and more, while enabling social contact in situations where meeting physically is challenging or even impossible [5,6].

However, digitalization is not without risk. The move to more digital work, leisure and more also means a move to more digital crime and threats [7]. Digital threats expose users and organizations to risks daily, and the need for cybersecurity to protect against those risks is undeniable. The threat landscape is multi-faceted and includes various types of threats that can be broadly classified as technological or human [8]. Technological threats include, for instance, malware or hacking where the attacker is using technological means to destroy or gain access to devices or services. Human threats involve exploiting user behavior, typically for the same purpose. A common type of human threat is phishing,
where an attacker sends an email to the target victim and attempts to persuade the victim into behaving in an insecure way by, for instance, downloading an attachment or clicking a link and then submitting login credentials to some service. Phishing is continuously reported as the most common threat to both organizations and individuals, and therefore the topic of this paper [9–11].

At its core, phishing is when an attacker attempts to trick a user into insecure behavior. Insecure behavior typically includes downloading a malicious attachment, clicking a link or giving up sensitive information in reply to the email [12]. Phishing has traditionally been easy to spot as generic messages which are often poorly formatted with poor spelling and grammar [13]. While that is still true for some of today’s phishing campaigns, now many phishing emails are well-written and use various techniques to invoke trust [12]. Furthermore, attackers employ targeted attacks where they tailor emails to a specific recipient, a technique known as spear-phishing [9]. In such an attack, the attacker may steal the email address of a friend or coworker of the target victim and make the email appear to come from that known sender. The attacker may also research the victim and ensure that the content of the malicious email is content that the victim would, given the victim’s job position or interest, expect to receive [14].

Techniques used by attackers and techniques used to defend against phishing both include technical and human aspects [15]. An attacker will exploit human behavior to invoke trust and persuade the victim into insecure behavior. As part of the attack, the attacker may also exploit technical weaknesses in the email protocols to pose as a trusted sender or use another technical weakness to take control of the victim’s system once the victim opens a malicious attachment [12]. Likewise, several organizations employ technical measures, such as automatic filters, to defend against phishing. However, educating users on detecting phishing emails remains the most commonly suggested defense mechanism. While both technical and human aspects of phishing are important, the primary focus of this paper is on the human side, particularly on user behavior and how it can be understood and improved.

As explained by the knowledge, attitude, and behavior (KAB) model, behavior is influenced by knowledge, and attitude [16]. KAB describes that increased knowledge about an expected behavior will lead to increased awareness and, finally, a change in behavior. This relationship has been evaluated in the security domain and found to hold [17].

Information Security Awareness Training (ISAT) is commonly suggested as the way to improve user awareness [18–20]. There are several different ways to train users presented in the literature. These include providing lectures, text-based warnings, video instructions sent out via email at regular intervals, instructive games and training automatically provided to users in risky situations [21–25]. There are, however, several publications suggesting that many training efforts fail to support users towards secure behavior to a high enough degree [26,27]. Suggested reasons include that it is hard to make users participate in on-demand training, that acquired knowledge is not retained for long enough, and that knowledge does not necessarily translate to correct behavior [20,28]. Some research even suggests that training methods are not empirically evaluated to a high enough extent [29,30].

This paper seeks to evaluate the effectiveness of two promising methods for ISAT; game-based training and Context-Based Micro-Training (CBMT). Game-based training means that users are presented with an educative game and is argued to increase user participation rates and provide a more realistic training environment compared to lectures, videos, or similar [31]. CBMT means that users are presented with condensed information in situations where the training is of direct relevance. In the context of phishing, a user will receive training when opening a mailbox. CBMT is argued to increase users’ awareness and has been evaluated in the context of password security with positive results [32]. The research question addressed in this paper is:

**To what extent can the two methods, game-based training and CBMT, support users to accurately differentiate between phishing and legitimate email?**
The research was carried out as a simulated experiment with 41 participants. The participants were asked to identify phishing emails while their behavior was monitored using an eye-tracking technique. The results show that both training methods can support users towards secure behavior and that CBMT does so to a higher degree than game-based training, which makes the first contribution of this research. The research further shows that most participants were susceptible to phishing, even after training which suggests that training alone is not enough to make users behave securely. The upcoming section will elaborate on ISAT and justify the selection of CBMT and game-based training as the focus of this research. The rest of this paper will, in turn, present the research methodology results, and discuss those results and their limitations.

2. Information Security Awareness Training

ISAT has been discussed in the scientific literature for several decades, and the importance of providing ISAT as a means of improving user behavior is widely acknowledged [33–35]. ISAT intends to increase user knowledge and awareness through training. There are many and diverse, options for ISAT, and recent publications [35–37] categorize ISAT methods differently. In general terms, ISAT methods can be described as seen in Table 1. Table 1 is based on the classifications by [36,37].

Table 1. Overview of ISAT methods.

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classroom training</td>
<td>Typically provided on-site as a lecture attended as a specific point in time.</td>
</tr>
<tr>
<td>Broadcasted online training</td>
<td>Typically, brief training delivered as broadcast to large user groups using email or social networks.</td>
</tr>
<tr>
<td>E-learning</td>
<td>ISAT typically delivered using an online platform that is accessible to users on-demand.</td>
</tr>
<tr>
<td>Simulated or contextual training</td>
<td>Training delivered to users during a real or simulated event.</td>
</tr>
<tr>
<td>Gamified training</td>
<td>Gamified training is described as using gamification to develop ISAT material.</td>
</tr>
</tbody>
</table>

While ISAT has been long discussed in scientific literature and used in practice, several publications suggest that many ISAT methods fail to adequately support users towards secure behavior [26,27]. This notion is emphasized by the continuous reports of incidents where human behavior is a key component [38,39]. Three core reasons for why ISAT does not always provide its intended effect can be found in recent research:

- Knowledge acquired during training deteriorates over time [21].
- It is challenging to get users to participate in training delivered on-demand [28].
- Users are provided with knowledge, but not motivated to act in accordance to that knowledge [20].

The ISAT methods included in this research are game-based training and Context-Based Micro-Training (CBMT). Gamified training means that game concepts are applied to ISAT, with the intent to better motivate users to actively participate [28]. It is considered in this research since it is argued to better motivate and engage users when compared to other ISAT alternatives. There are several examples of gamified ISAT. The landscape includes multi-player competitive games, story-based single-player games, board games, role-playing games, quizzes, and more [28,40].

CBMT is an example of contextual training. ISAT using the CBMT method is delivered to users in short sequences and in situations where the training is of direct relevance. Phishing training is, for instance, delivered to users that are in a situation with an elevated risk of being exposed to phishing. It is argued to counter the knowledge retention and user
participation problems by automatically appearing in those relevant situations [32]. It is
also argued to motivate users towards secure behavior by providing them with training
that directly relates to the users' current situation.

3. Materials and Methods

The purpose of this study was to evaluate user behavior when assessing if emails are
malicious or not. To that end, a controlled experiment where the participants were exposed
to an inbox and asked to classify the email contained in that inbox was conducted. The par-
ticipants were scored based on how accurately they classified the emails. Furthermore, the
participants' behavior was monitored during the experiment by an eye tracker that recorded
where the participants were looking on screen. Before the experiments, the participants
were randomised into three groups; game-based training, CBMT-based training or control.
A between-group analysis was performed to identify differences between training meth-
ods and answer the research question posed. As detailed at the end of paper statements,
data supporting this paper is available as open data (https://doi.org/10.5878/g6d9-7210
(accessed on 6 March 2022)). Furthermore, the study did not require ethical review, but all
participants signed a written informed consent form detailing how the study was executed
and how data were handled. An overview of the research process is presented in Figure 1.
The rest of this section provides a detailed description of the experiment environment, data
collection procedures, collected variables, and data analysis procedures.

![Research process overview](image)

**Figure 1.** Research process overview.

### 3.1. Experiment Environment

An experiment environment containing an email system was set up on Ubuntu Linux
using the email server and management platform Modoboa (https://modoboa.org/en/
(accessed on 6 March 2022)). Both Ubuntu Linux and Modoboa were installed with default
settings. Modoboa allowed for the creation of unlimited email domains and addresses and
provided a webmail interface. Several email domains were configured so that different
types of emails could be created:

- Legitimate emails from service providers such as Google and banks.
- Phishing emails that imitated phishing emails from hijacked sender accounts.
- Phishing emails from domains made up to look similar to real domains, for instance,
lundstro.mse instead of lundstrom.se.

The fictitious company Lundström AB, and the character Jenny Andersson were
developed. The company was given the domain lundstrom.se and the character was given
the email address jenny@lundstrom.se. A persona was developed for Jenny Andersson.
The experiment participants were asked to assume Jenny's persona and classify the email
in her inbox. The persona was expressed as follows:
Jenny is 34 years old and works as an accountant at a small company (Lundström AB), and her manager is Arne Lundtröm. She lives with her husband and kids in a small town in Sweden. Your email address is jenny@lundstrom.se. You use the banks SBAB and Swedbank and is interested in investing in Bitcoin. You are about to remodel your home and have applied for loans at several banks to finance that. You shop a fair bit online and are registered at several e-stores without really remembering where. You are currently about to remodel your bathroom. Ask the experiment supervisor if you need additional information about Jenny or the workplace during the experiment.

Jenny’s inbox was populated with 11 emails where five were legitimate, and six were phishing. The legitimate emails were crafted as reasonable questions from her manager or communications from banks and craftsmen. The communications from banks and craftsmen were based on real emails taken from one of the researcher’s inboxes. The six phishing emails were crafted to include different phishing identifiers. Five different phishing identifiers were included in the experiment. They are commonly mentioned in scientific and popular literature and were the following [41–44]:

1. Incorrect sender address where the attacker may use an arbitrary incorrect sender address, attempt to create an address that resembles that of the true sender, or use a sender name to hide the actual sender address.
2. Malicious attachments where the attacker will attempt to make the recipient download an attachment with malicious content. A modified file extension may disguise the attachment.
3. Malicious links that are commonly disguised so that the user needs to hover over them to see the true link target.
4. Persuasive tone where an attacker attempts to pressure the victim to act rapidly.
5. Poor spelling and grammar that may indicate that a text is machine translated or not written professionally.

The included phishing emails are described as follows:

1. The first phishing email came from the manager’s real address and mimicked a spear-phishing attempt, including a malicious attachment and hijacked sender address. The attachment was a zip file with the filename “annons.jpeg.zip (English: advertisement.jpeg.zip)”. The text body prompted the recipient to open the attached file. In addition to a suspicious file extension, the mail signatures differed from the signature in other emails sent by the manager.
2. The second phishing email came from Jenny’s own address and prompted the recipient to click a link that supposedly led to information about Bitcoin. The email could be identified as phishing by the strange addressing and the fact that the tone in the email was very persuasive.
3. The third phishing email appeared to be a request from the bank SBAB. It prompted the user to reply with her bank account number and deposit a small sum of money into another account before a loan request could be processed. It could be identified by improper grammar, an incorrect sender address (that was masked behind a reasonable sender name), and the request itself.
4. The fourth phishing email was designed to appear from Jenny’s manager. It prompted Jenny to quickly deposit a large sum of money into a bank account. It could be identified by the request itself and because the sender address was arne@lundstrom.se instead of arne@lundstrom.se.
5. The fifth phishing email mimicked a request from Google Drive. It could be identified by examining the target of the included links that lead to the address xcom.se instead of google.
6. The sixth phishing email appeared to be from the bank Swedbank and requested the recipient to go to a web page and log in to prove the ownership of an account. It could
be identified as phishing by examining the link target, the sender address, which was hidden behind a sender name, and the fact that it contained several spelling errors.

The experiment was set up so that most phishing emails had similar legitimate counterparts. The legitimate emails included where:

1. The first legitimate email was a request from Jenny’s manager Arne. The request prompted Jenny to review a file on a shared folder.
2. The second legitimate email was a notification from a Swedish bank. It prompted Jenny to go to the bank website and log in. It did not contain any link.
3. The third legitimate email was an offering from a plumber. While containing some spelling errors, it did not prompt Jenny to make any potentially harmful actions.
4. The fourth legitimate email is a request for a meeting from Jenny’s manager Arne.
5. The fifth email is a notification from a Swedish bank. This notification prompts the user to go to the bank website and log in. It does not contain any greeting or signature with address.

The webmail interface is demonstrated in Figure 2. Figure 2 displays the layout of the included emails and is annotated to show the ordering of the emails. Legitimate emails are denoted L\(n\), in green, and phishing emails are denoted P\(n\) in red.

![Figure 2. Webmail interface used in the experiment.](image)

3.2. Participant Recruitment

Participants were recruited using a convenience sampling approach where students and employees from the University of Skövde were recruited. Participants with education or work experience in cybersecurity were excluded from the study. All participants were invited with a direct email that they were asked to reply to in order to participate. Upon registration, participants were randomly assigned to one of the three groups and provided with a description of the experiment, a description of the persona, and an informed consent form. The three groups were the following:

- **Game**: Participants in this group were prompted to play an educational game before arriving for the experiment. The game is called Jigsaw (https://phishingquiz.withgoogle.com/) (accessed on 6 March 2022) and is developed by Google. It is an example of game-based training that is implemented as a quiz and was selected for use
in this research because it is readily available for users. It also covers all the identifiers of phishing previously described. Jigsaw takes about five minutes to complete.

- CBMT: Participants in this group received computerized training developed by the research team according to the specifications of CBMT. It was written information that appeared to the participants when they opened Jenny’s inbox, as demonstrated in Figure 3. The participants were presented with a few tips and prompted to participate in further training, which led the participants to a text-based slide show in a separate window. The training takes about five minutes to complete.

- CONTROL: This group completed the experiment without any intervention.

![Translation:]
* Always read the email carefully before opening files or links
* Never share credit or account numbers, or passwords
* Contact the sender using the phone if you are uncertain

Click here to learn more
Read more at MSB...
Read more at the police...

Figure 3. Demonstration of CBMT-based training.

3.3. Experiment Procedure

On arriving for the experiment, the participant was seated in a regular office in front of a 24" computer monitor that displayed the experiment environment. The monitor was equipped with a Gazepoint GP3 HD eye tracker (https://www.gazept.com/product/gp3hd/) (accessed on 6 March 2022). The participant was asked to read the informed consent form and given the opportunity to ask questions about the experiment and study before signing it. The participant was then asked to respond to a survey with demographic questions and asked to take a seat in front of the monitor. The eye tracker was calibrated using the manufacturer’s built-in calibration sequence with nine points [45]. The calibration was considered successful when the control software deemed all nine points valid. In cases where the eye tracker could not be successfully calibrated, eye-tracking data were disregarded for that participant. This happened for three participants.

The participant was then reminded of Jenny’s persona and asked to classify the email in Jenny’s inbox. The participant was instructed to delete all phishing emails and keep all legitimate emails. The participant was asked to think aloud during the experiment, especially about how decisions to delete emails were made. The participant was also told that at least one of the emails was phishing and that a score was to be calculated based on the participants’ performance. The intent was to make the participant as aware
of phishing as possible. The rationale was that mere inclusion in the experiment would increase the participant’s awareness level, and by priming all participants to high awareness would make the awareness levels of the participants comparable. Consequently, the gathered data reflects the participants’ best ability to delete phishing rather than the ability they can be assumed to have during their daily work. Gazepoint analysis UX Edition (https://www.gazept.com/product/gazepoint-analysis-ux-edition-software/) (accessed on 6 March 2022) was used to monitor the participant’s performance in real time on an adjacent screen and for post-experiment analysis of the collected eye-tracking data. Following the experiment, the participants in the game group were asked if they had played the game before the experiment as instructed. The experiment process, from the participant’s point of view, is visualized in Figure 4.

![Figure 4. Visualization of experiment procedure. Dashed boxes only applied to some groups.](image)

3.4. Collected Variables

Variables reflecting the participants’ demographic background, score and behavior were captured during the experiment. The demographic variables were collected to enable a descriptive presentation of the sample’s demographic attributes. The score variables reflected the total number of correct classifications the participants made. The behavior variables described how the participants acted during the experiment by counting how many of the previously described phishing identifiers the participants used. Two behavior variables were collected. The first was collected manually during the experiment (behavior_manual). It was based on real-time monitoring, and the participants expressed thoughts. It reflected how many of the following actions the participant performed at least once:
1. Evaluated the sender address by hovering over the displayed name to see the real sender address.
2. Evaluated attachments by acknowledging their existence and describing it as suspicious or legitimate.
3. Evaluated links by hovering over them or in some other way verified the link destination.
4. Evaluated if the tone in the email was suspiciously persuasive.
5. Evaluated if spelling and grammar made the email suspicious.

Please note that the variables reflect what identifiers the participants used but not if they accurately interpreted the information provided by the identifier. A participant who, for instance, incorrectly evaluated a sender address as legitimate would still get the point for evaluating the sender address. The second behavior variable, behavior_tracked, was computed automatically by defining Areas of Interest in Gazepoint analysis UX Edition and counting how many times the participant gazed in those areas. Areas of Interest are defined screen areas that allow for collecting the number of times the participants gaze in those particular areas. The following three Areas of Interest were defined.

- Address, which covered the area holding the sender and recipient addresses.
- Attachment covering the area where email attachments are visible.
- Link covering the area where the true link destination appears.

The Areas of Interest were only active when they included the intended information. For instance, the Attachment area was only active when an attachment was visible on the screen. The Areas of Interest are demonstrated in Figure 5 which also shows how red dots denote where the participant is currently looking.

![Figure 5](image_url)

**Figure 5.** Demonstration of how areas of interest were defined, with AOI definitions enlarged. Please note that the Link area contains the target address of a link that is hovered over.

3.5. Data Analysis

The data were analyzed using SPSS version 25. The demographic properties of the sample were first described followed by a descriptive overview of the three variables SCORE, behavior_manual, and behavior_tracked. The proportion of participants that received perfect scores was then reported. A perfect score means that a participant identified all 11 emails correctly, or used all phishing identifiers assessed by the variables behavior_manual and behavior_tracked, respectively.

Next, Kruskal–Wallis H tests were used, with pairwise Mann–Whitney U test with Bonferroni correction as post hoc procedure, to identify significant between-group differ-
ences. Kruskal–Wallis H test performed on three or more samples will return a significant result if at least one sample is different from the others. In such a case, the Mann–Whitney U test with Bonferroni correction is used between all pairs in the sample to analyze what individual samples that are different from each other. Kruskal–Wallis H test was used over ANOVA because the data must show a normal distribution for ANOVA to be robust, and most samples did not in this case [46]. The conventional significance level of 0.05 is used throughout this paper.

4. Results

This section outlines the results of the study. It is divided into two sections were the first section outlines a descriptive overview of the data. The second section outlines the results in relation to the research question. It should be noted that three participants in the Game group reported that they did not play the provided game. This is to be expected given previous works suggesting that it is challenging to get users to participate in training [28]. All statistical procedures have been performed with and without those three participants. Results concerning the Game group are reported as \( n(m) \) were \( n \) is the result when the complete group is considered and \( m \) is the result when participants that did not play the game are omitted.

4.1. Data Overview

Data was collected over a period of about two months and included 41 participants. Two participants were removed from the data set since they reported having formal training in cybersecurity. The data collection period was intended to be longer, but data collections stopped after a security incident where the IT department warned all students and staff at the university about phishing involving attachments. Continued data collection would have risked the validity of the data set. The mean participant age was 37. Twenty-three participants identified themselves as female and 16 as male. Twenty-three participants reported being employees and 16 reported being students. An overview of the mean and median values for the collected variables and the distribution form of the variables is presented in Table 2. Please note that eye-tracking failed for three participants and the participants included for the variable behavior_tracked is therefore only 36.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Group</th>
<th>Mean</th>
<th>Median</th>
<th>Normal Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>behavior_manual</td>
<td>Control (n = 11)</td>
<td>3</td>
<td>3</td>
<td>NO</td>
</tr>
<tr>
<td></td>
<td>CBMT (n = 14)</td>
<td>4.57</td>
<td>5</td>
<td>NO</td>
</tr>
<tr>
<td></td>
<td>Game (n = 14)</td>
<td>3.64 (3.82)</td>
<td>3.5 (4)</td>
<td>NO</td>
</tr>
<tr>
<td></td>
<td>Total (n = 39)</td>
<td>3.79</td>
<td>4</td>
<td>NO</td>
</tr>
<tr>
<td>behavior_tracked</td>
<td>Control (n = 10)</td>
<td>1.9</td>
<td>2</td>
<td>NO</td>
</tr>
<tr>
<td></td>
<td>CBMT (n = 12)</td>
<td>2.5</td>
<td>3</td>
<td>NO</td>
</tr>
<tr>
<td></td>
<td>Game (n = 14)</td>
<td>2.29 (2.55)</td>
<td>2 (3)</td>
<td>NO</td>
</tr>
<tr>
<td></td>
<td>Total (n = 36)</td>
<td>2.25</td>
<td>2</td>
<td>NO</td>
</tr>
</tbody>
</table>

4.2. The Effect of Training

The effect of training was assessed by first examining the proportion of participants that received perfect scores. A perfect score means that the participants used all phishing identifiers or identified all emails correctly. The proportions of perfect scores are presented in Table 3.

Table 3 suggests that participants who received training performed better than participants in the control group for the behavior variables and that the participants in the CBMT
group outperformed the other groups for the variable SCORE. The same tendency is seen in Table 2 where mean and median results for the different sample groups are presented. Table 2 suggests that participants in the group game performed slightly better than the control group while the participants in the group CBMT outperformed the other groups with a bigger margin. The exception is for the variable behavior_tracked where the groups CBMT and game performed equally when participants who reported not playing the game were omitted from the game group.

Table 3. Proportions of perfect scores.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Group</th>
<th>Perfect Scores</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCORE</td>
<td>Control (n = 11)</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td>CBMT (n = 14)</td>
<td>21.4%</td>
</tr>
<tr>
<td></td>
<td>Game (n = 14)</td>
<td>0% (0%)</td>
</tr>
<tr>
<td></td>
<td>Total (n = 39)</td>
<td>7.7% (8.3%)</td>
</tr>
<tr>
<td>behavior_manual</td>
<td>Control (n = 11)</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td>CBMT (n = 14)</td>
<td>64.3%</td>
</tr>
<tr>
<td></td>
<td>Game (n = 14)</td>
<td>14.3% (18.2%)</td>
</tr>
<tr>
<td></td>
<td>Total (n = 39)</td>
<td>28.2% (30.6%)</td>
</tr>
<tr>
<td>behavior_tracked</td>
<td>Control (n = 10)</td>
<td>9.1%</td>
</tr>
<tr>
<td></td>
<td>CBMT (n = 12)</td>
<td>57.1%</td>
</tr>
<tr>
<td></td>
<td>Game (n = 14)</td>
<td>42.9% (54.5%)</td>
</tr>
<tr>
<td></td>
<td>Total (n = 36)</td>
<td>38.5% (45.5%)</td>
</tr>
</tbody>
</table>

Kruskal–Wallis H test was used to identify variables with statistically significant between-group differences. The results are presented in Table 4.

Table 4. Kruskal–Wallis H tests.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Kruskal–Wallis H</th>
<th>p-Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCORE</td>
<td>13.965 (12.531)</td>
<td>0.001 (0.002)</td>
</tr>
<tr>
<td>behavior_manual</td>
<td>16.270 (15.434)</td>
<td>0.000 (0.000)</td>
</tr>
<tr>
<td>behavior_tracked</td>
<td>5.569 (7.332)</td>
<td>0.062 (0.026)</td>
</tr>
</tbody>
</table>

The Kruskal–Wallis H tests suggest that at least one sample is different from the others when $p < 0.05$, as is the case for the variables SCORE and behavior_manual. The same is also true for the variable behavior_tracked when users who did not play the game are omitted. Pairwise Mann–Whitney U tests with Bonferroni correction was used to test what variables that were significantly different from each other. The results are presented in Table 5.

Table 5. Pairwise post hoc tests. Please note that post hoc tests for the variable behavior_tracked were only computed in the case when participants in the group Game, who did not play the game was omitted because the corresponding Kurskal-Wallis H tests was only significant in that case.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Groups</th>
<th>p-Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCORE</td>
<td>Control-Game</td>
<td>1.000 (1.000)</td>
</tr>
<tr>
<td></td>
<td>Control-CBMT</td>
<td>0.005 (0.003)</td>
</tr>
<tr>
<td></td>
<td>Game-CBMT</td>
<td>0.003 (0.023)</td>
</tr>
<tr>
<td>behavior_manual</td>
<td>Control-Game</td>
<td>0.502 (0.277)</td>
</tr>
<tr>
<td></td>
<td>Control-CBMT</td>
<td>0.000 (0.000)</td>
</tr>
<tr>
<td></td>
<td>Game-CBMT</td>
<td>0.021 (0.102)</td>
</tr>
<tr>
<td>behavior_tracked</td>
<td>Control-Game</td>
<td>X (0.083)</td>
</tr>
<tr>
<td></td>
<td>Control-CBMT</td>
<td>X (0.036)</td>
</tr>
<tr>
<td></td>
<td>Game-CBMT</td>
<td>X (1.000)</td>
</tr>
</tbody>
</table>
In this case, the difference between two variables is statistically significant when \( p < 0.05 \). Table 5 shows that CBMT is separated from the groups game and control for the variables SCORE and behavior_manual while control and game cannot be separated. For behavior_tracked, game and CBMT cannot be separated but are both separated from control.

5. Discussion

This research explores how effectively Information Security Awareness Training (ISAT) can support users to accurately identify phishing emails. The research evaluated two methods that were discussed as being promising in recent literature, namely game-based training and training based on CBMT. The research was conducted as a simulated experiment that measured how the participants behaved when assessing whether emails were phishing or not, and how accurately they classified email. The statistical analysis shows that participants in the CBMT group had higher scores than users in the game or control group. In terms of behavior, participants in the CBMT group performed better than the game and control group for the manually collected variable. However, the CBMT and game groups were equally strong for the variable computed based on eye-tracking data. In conclusion, both game-based training and CBMT are shown to improve user behavior in relation to phishing while only CBMT can be shown to improve users’ ability to accurately classify phishing emails.

One reason could be that CBMT provides an awareness increasing mechanism in addition to training while game-based training does not. The game-based training is delivered to participants on a regular basis and was mimicked in the experiment by letting the participants take the training prior to arriving for the experiment. CBMT is, by design, presented to users when they are entering a risky situation and that was mimicked by presenting the CBMT training to participants just before starting the experiment. The difference in how the training was delivered could account for the difference in results between the two groups. In fact, the effect of awareness increasing mechanisms have been evaluated in prior research with good results [47,48]. This research extends those results by suggesting that awareness increasing mechanisms combined with training are likely to have a positive effect on users’ ability to accurately identify phishing emails.

While training was proven to improve participants’ ability to identify phishing, it can be noted that less than 10% of the participants were able to identify all emails correctly. Furthermore, less than 50% of the participants evaluated all of the phishing identifiers and even if the participants in the CBMT group received training just before starting the experiment, 35.7% of those participants missed one or more phishing identifiers. Yet, most organizations explicitly or implicitly expect users to correctly identify all phishing emails all the time. The present research shows that even if users are provided with training just before being tasked with identifying phishing, and instructed to actively search for phishing, very few users are able to fulfill the expectations of that security model. The implication of this result is that the security model or the feasibility of using training alone to reach it must be questioned. One could, for instance, question if we should follow a paradigm where users are expected to change according to how computers work. A more useful paradigm could be to modify the way that computers work to match the abilities of the users. A similar viewpoint is presented by [49] who questions why the responsibility for cybersecurity is individualized through the notion of the “stupid user”. Instead, ref. [49] suggest that user-oriented threats should be managed by security professionals, and managers, at a collective level. Likewise, ref. [50] calls for a more holistic approach to anti-phishing methods.

5.1. Limitations

A given limitation of this study comes from participation bias. Participation bias is known to impact simulated experiments in cybersecurity awareness [22]. The expected effect in this study is that participants are more aware than they would be in a naturally occurring situation. Thus, the scores are expected to reflect the participants’ best ability.
rather than their average performance. Using a between-group design, we still argue that differences between ISAT methods identified in this research are valid. However, it is likely that the actual performance of the included methods will be lower in a natural environment. On a similar note, the method cannot account for organizational factors such as leadership support and social pressure, which are known to impact cybersecurity behavior [51].

A second limitation concerns sampling where this research included participants studying, or working at, a university. As such, the results are representative of that population and any inference beyond that population should be avoided. On this topic, recent research argues that there are indeed demographic differences in the ability to detect phishing [52]. The number of participants is a further limitation and a higher participant number would have been preferable. In this case, data collection was stopped following a cybersecurity incident that prompted the IT department to broadcast a phishing warning. Participants performing the experiment after that event would have been exposed to information not presented to other participants and that would have introduced bias into the dataset.

A third possible discussion under the umbrella of limitations is how the different types of training were presented to the participants. The participants placed in the game group were asked to play a game before arriving for the experiment while participants in the CBMT group were subjected to training on arrival. There is, therefore, a chance that participants in the game group forgot some of the training, or forgot to play the game entirely. The design is argued to mimic the natural behavior of the two training types and both retention and failure to play are two previously discussed obstacles with game-based training delivered in a format that requires active participation [28]. Consequently, any effect of the experimental design mimics an expected effect in a natural environment.

5.2. Future Work

While training can undoubtedly support users to identify phishing emails, this study suggests that training alone is not enough and that opens up several future research directions. First, future studies could focus on combining training with modifying the way emails are presented to users. One could imagine that finding ways to make it easier for users to find and interpret phishing identifiers could improve users’ ability to identify malicious emails. A possible example could be to rewrite links in the text body of emails to always show the full link address, which is unclickable, instead of allowing clickable hyperlinks with arbitrary display names. A similar possible direction is to further research predicting user susceptibility to phishing using artificial intelligence [53]. That could identify a user in need of training and then provide tailored training. A second direction for future work could be to replicate this study with a different population. That would allow for identification of differences and similarities between, for instance, technical and non-technical users, male and female users, and users of different age.

A more theoretical direction for future work could be to evaluate the strength of the relationships in the KAB model and to evaluate the relationship between behavior and actual outcomes of that behavior. In certain situations, including phishing, applying a correct behavior is not enough, since a user also has to interpret the result of that behavior. For instance, a correct behavior would make a user control the real target of a link, and to make a decision about the email the user needs to interpret the trustworthiness of the link target. Furthermore, one could assess the possible effect of usability on the relationship between the constructs in the KAB model. One can imagine that knowledge about a certain behavior is more likely to result in that behavior if the effort to comply is low.

Author Contributions: Conceptualization, J.K., M.N. and J.R.; methodology, J.K, M.N. and J.R.; software, R.R. and A.H.; validation, All.; formal analysis, J.K.; investigation, J.K.; resources, J.K.; data curation, J.K.; writing—original draft preparation, J.K.; writing—review and editing, M.N., J.R. and S.F.; supervision, S.F.; project administration, J.K.; funding acquisition, J.K, M.N., J.R., R.R. and A.H. All authors have read and agreed to the published version of the manuscript.
Funding: This research was funded by The Swedish Post and Telecom Authority grant number 19-10617.

Institutional Review Board Statement: Ethical review and approval were waived for this study, due to the fact that it does not require ethical clearance under the Swedish Ethical Review Act. Ethical Review Act dictates that research including sensitive personal data, physical interventions on living or deceased persons, methods that aim to affect persons physically or mentally, methods that can harm persons physically or mentally, or biological material from living of deceased persons [54]. Since this research does not fall under any of those criteria, ethical clearance has not been applied for. The study has been discussed with the chairperson of the council of research ethics at the University of Skövde.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Data supporting this research can be found at: https://doi.org/10.5878/g6d9-7210 (accessed on 6 March 2022).

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

Abbreviation

The following abbreviations are used in this manuscript:

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISAT</td>
<td>Information Security Awareness Training</td>
</tr>
<tr>
<td>CBMT</td>
<td>Context-Based Micro-Training</td>
</tr>
<tr>
<td>SETA</td>
<td>Security Education, Training, and Awareness</td>
</tr>
<tr>
<td>KAB</td>
<td>Knowledge, Attitude, and Behaviour</td>
</tr>
<tr>
<td>SPSS</td>
<td>Statistical Package for the Social Sciences</td>
</tr>
<tr>
<td>ANOVA</td>
<td>Analysis of variance</td>
</tr>
</tbody>
</table>

References


50. Alabdan, R. Phishing attacks survey: Types, vectors, and technical approaches. Future Internet 2020, 12, 168. [CrossRef]


PAPER 10: A TAXONOMY OF SETA METHODS AND LINKAGE TO DELIVERY PREFERENCES.

A taxonomy of SETA methods and linkage to delivery preferences

Abstract. Cybersecurity threats targeting users are common in today’s information systems. Threat actors exploit human behavior to gain unauthorized access to systems and data. The common suggestion for addressing this problem is to train users to behave better using SETA programs. The notion of training users is decades old, and several SETA methods are described in scientific literature. Yet, incidents stemming from insecure user behavior continue to happen and are reported as one of the most common types of incidents. Researchers argue that empirically proven SETA programs are needed and point out focus on knowledge rather than behavior, and poor user adoption, as a problem with existing programs. The present study aims to research user preferences regarding SETA methods, with the motivation that a user is more likely to adopt a program perceived positively. A qualitative approach is used to identify existing SETA methods, and a quantitative approach is used to measure user preferences regarding SETA delivery. Our research shows that users prefer SETA methods to be effortless and flexible and outline how existing methods meet that preference. The results outline how SETA methods respond to user preferences and how different SETA methods can be implemented to maximize user perception and thereby support user adoption.

Keywords: cybersecurity, information security, security training, security behavior, security awareness, user training, SETA.
A taxonomy of SETA methods and linkage to delivery preferences

INTRODUCTION

The global transition into the digital era has unfortunately been accompanied by continuous reports of security breaches and incidents. As such, the need for appropriate cybersecurity to safeguard individuals and organizations is undeniable. One of the attack vectors commonly exploited by attackers to gain access to systems is the human element. In essence, users are regarded as a weak link and therefore directly targeted in contexts such as malware, phishing and other online scams. The attackers’ aim is often to make the user perform some action that will put them or their organization at risk, and the resulting vulnerability is one of the major challenges in cybersecurity today (Safa & Von Solms, 2016).

There is a resultant need to improve user behavior regarding cybersecurity (Bulgurcu, Cavusoglu, & Benbasat, 2010). A common notion on how to do that is to make users understand the negative consequences of their actions and teach them how to behave in a more secure way (Desman, 2003). The most common approach to this is using Security Education, Training, and Awareness (SETA) programs (Joinson & van Steen, 2018; Puhakainen & Siponen, 2010). These are intended to provide users with the knowledge and skills they need to behave in a secure manner (D'Arcy, Hovav, & Galletta, 2009).

While SETA efforts have been discussed in the scientific literature for at least two decades (Siponen, 2000), the continuous incidents stemming from insecure user behavior demonstrate that the issue is nowhere near being solved. Several reasons for this can be found in existing literature, where some researchers suggest a lack of SETA programs based on empirical evidence of their effect (Al-Daeeef, Basir, & Saudi, 2017; Alshaikh, Maynard, Ahmad, & Chang, 2018). Further, Bada, Sasse, and Nurse (2019) question the design of security systems and policies themselves in addition to SETA practices. They further argue that SETA
programs should not only provide knowledge but must promote desired behavior. Similarly, Parsons (2018) suggests that providing knowledge is not enough for a SETA program to be effective since knowledge does not always translate to behavior. A further obstacle is that of user adoption. Naturally, any SETA program must be adopted and used by its intended users in order to provide its intended effect. However, several researchers suggest that SETA programs struggle to get users to accept and adopt them in practice (Gjertsen, Gjaere, Bartnes, & Flores, 2017; Kim, 2014).

Users' willingness to adopt information systems is influenced by their perception of that information system (Davis, 1989). Our paper seeks to further the understanding of how users perceive SETA methods by studying user preferences regarding its delivery and relating that to existing programs. To that end, delivery preferences were researched using a web-based survey. A structured literature review was then conducted to identify existing programs. The results of the two steps were combined to produce an overview of how users perceive the current SETA methods. The paper contributes to the understanding of users’ delivery preferences and can, in that regard, be used to guide future research into the development of SETA methods. The results can also be used by practitioners seeking to develop or procure SETA programs for their organization.

The remainder of our paper is structured as follows: The next section provides a theoretical background for our study. Then, the research objectives addressed are explicated, leading to the description of the research methodology that was applied. The results are then presented and discussed before the paper is concluded with conclusions that can be drawn for our research.

THEORETICAL BACKGROUND
The notion that the human element is an integral part of cybersecurity is not new and has been studied for several decades (Siponen, 2000). Nevertheless, the human element is only considered in a fraction of the research being conducted in cybersecurity (Rahman, Rohan, Pal, & Kanthamanon, 2021). In fact, Rahman et al. (2021) show that about one percent of the publications in top cybersecurity conferences between 2015 and 2020 focus on the human element. This can be contrasted to industry reports that continuously describe human-related attack vectors as the most used, even suggesting that up to 95% of all security breaches are because of the human element (Cybint, 2020; EC-Council, 2019; Soare, 2020). Even allowing for the fact that many of these breaches will not call for safeguards or responses that specifically fall into a ‘human aspects’ category, there still seems to be a significant disconnect between the extent to which people contribute to our breaches and the degree to which we address them in our security posture.

Cybersecurity behavior has proven to be a complicated and multi-faceted issue. On the one hand, behavior is impacted by contextual aspects. One such example would be that behavior is likely to be different between a user’s work-related and private use. That since the user is likely to be constrained by policies and technical security controls at work, but not equally so at home (Mashiane & Kritzinger, 2018). Individual factors such as gender, stress level, the user’s security awareness and knowledge, and predisposition to being suspicious are also important factors influencing the users' response to different situations (Chowdhury, Adam, & Skinner, 2019; Donalds & Osei-Bryson, 2020; Harrison, Vishwanath, & Rao, 2016). Previous research also suggests that personality traits such as impulsivity and willingness to take risks affect security behavior (Anwar et al., 2017; Hadlington, 2017). It is well known that humans in different parts of the world act differently and hold different values. This is also true in the cybersecurity domain, where it has been observed that users from different cultures, often treated as residents in different countries, differ in terms of cybersecurity behavior (Ameen et
al., 2020; Onumo, Cullen, & Ullah-Awan, 2017). While cybersecurity behavior is a complex matter, training interventions are commonly suggested to improve users' behavior (Anwar et al., 2017; Bada et al., 2019; Evans, Maglaras, He, & Janicke, 2016; Safa et al., 2015). Training interventions for the purpose of improving user behavior with regard to cybersecurity are commonly called Security Education, Training, and Awareness (SETA) programs (Yoo, Sanders, & Cerveny, 2018). While some SETA methods can be argued to target IT or security professionals, the present research is limited to SETA methods targeting employees or private users (Hu, Hsu, & Zhou, 2021b).

While it is arguably under-represented in relation to its significance, SETA methods is nonetheless a long-established theme in scientific literature. For example, in 2000, Siponen described that awareness training must be delivered to users so that they know what to do, are motivated on why to do it, and trained on how to do it (Siponen, 2000). More recent studies suggested that knowledge of what to do does not necessarily mean that users behave securely (Boss, Galletta, Lowry, Moody, & Polak, 2015; Parsons, 2018; Siponen, Mahmood, & Pahnila, 2014). The goal of SETA methods is to make users behave securely. In organizations, the expectations relating to secure behavior are formalized using policies. To enable users to behave securely, they must be made aware of how to act and provided with the appropriate skills to act accordingly. Further, appropriate behavior should be made part of the user's everyday practices, such that it becomes part of the organizational culture (Thomson, Von Solms, & Louw, 2006).

To ensure that SETA programs provide their desired effect, they should be empirically evaluated (Puhakainen & Siponen, 2010). SETA programs can easily be argued to be information systems artifacts. The evaluation thereof has been extensively discussed in the literature and seen as an integral part of, for instance, design science (Hevner, March, Park, & Ram, 2004). Evaluation can occur using various empirical methods, including experiments,
case studies, surveys, action research, and more (Offermann, Levina, Schönherr, & Bub, 2009; Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007). The aim of such evaluations is to determine how well an artifact works and in the information security domain, that ought to translate to demonstrating its effect on information security behavior. Further, considering the effect sought after by employing SETA programs, security behavior is a natural factor to evaluate by. However, evaluating user behavior is difficult (Vroom & Von Solms, 2004). One factor that may limit the validity of such validations is that participants included in evaluations of their awareness, and told of that fact, are likely to be more aware than they would otherwise be (Joinson & van Steen, 2018). Performing the same evaluation without informing the participants will instead present ethical challenges (Renaud & Zimmermann, 2018).

Drawing from the discussion above, including knowledge gained from a SETA program as another metric to evaluate SETA programs by is reasonable. To act securely, a user must know what secure behavior entails. Thus, a SETA program must be able to transfer knowledge to the user in order to be effective. Further, contemporary research stresses the need for user-centered design and usability of security features (Das, Dingman, & Camp, 2018; Khan, Hengartner, & Vogel, 2015). An integral part of user-centered design is to evaluate users' perception of an artifact iteratively during a design project (Vredenburg, Mao, Smith, & Carey, 2002). As such, evaluating user perception of a proposed SETA program is reasonable. The Technology Acceptance Model (TAM) further emphasizes the usefulness of evaluating user perception and suggests that user perception is an essential precursor for user adoption (Davis, 1989). Subsequently, user adoption is crucial in ensuring that the SETA program can provide its intended effect.

Several distinct approaches to SETA are discussed in recent literature, including instructor-led lectures, efforts in gamification, interactive training methods, and more. One example
included providing training on detecting phishing e-mails using lectures that participants attended physically at a specific time (Reinheimer et al., 2020). In that particular case, the training was followed by a reminder sent out as text, interactive examples, video, or short text. The study found that the effect of the lecture had worn off after six to eight months but that the reminders helped the participants maintain the effect longer (Reinheimer et al., 2020). On gamification, a gamified artifact developed to increase awareness of online self-disclosure in social media was developed and evaluated in an experiment that collected data from the participants' Facebook pages (Dincelli & Chengalur-Smith, 2020). They found that a text-based intervention had a longer-lasting effect than a visual intervention.

An experimental study that examined the effects of combining training with a warning in the context of fraudulent web pages found that presenting training to users in combination with a warning in potentially dangerous situations is as effective as warnings alone when it comes to security behavior in that particular situation. The study also found that users who received training retained the knowledge for at least three weeks (Xiong, Proctor, Yang, & Li, 2019).

Regardless of how effective a SETA method is regarding knowledge transfer and behavioral change, it must be adopted by its intended users if it is to provide that effect (Gjertsen, Gjære, Bartnes, & Flores, 2017). However, recent research suggests that organizations struggle to get users to actively participate in SETA programs (He & Zhang, 2019; Reeves, Calic, & Delfabbro, 2021). The Technology Acceptance Model is a theoretical model commonly used to explain acceptance or rejection of information systems (Rahimi, Nadri, Afshar, & Timpka, 2018), and was introduced by Davis (1989), with several extensions having been suggested since then (Lee, Kozar, & Larsen, 2003). TAM includes three core constructs that influence a user’s decision to adopt technology; Perceived usefulness (PU), Perceived ease of use (PEOU), and Intention to use (IU) (Hess, McNab, & Basoglu, 2014). IU is a determinate for actual use and is influenced by PU and PEOU. PU is also influenced by PEOU (Venkatesh
& Davis, 2000). Applied to SETA methods, TAM highlights the importance of user perception as a precursor to user adoption. The domain of the present study is user perception of SETA methods, and it seeks to investigate how SETA delivery options support user perception viewed from the perspective of TAM.

Hu et al. (2021b) describe that purpose, target audience, level, and delivery method make distinct aspects of SETA methods. Our research focuses on the delivery method and considers the level part of the delivery method. The motivation is that delivery method is scarcely discussed in previous research and that delivery method has been found to impact user preference of SETA methods (Hu et al., 2021b; Reeves, Calic, & Delfabbro, 2021). Looking at the SETA methods presented in this section, it becomes evident that SETA delivery can be discussed in different aspects. Conceptualizing those aspects, they describe how the training is delivered, when the user receives it, what level of information the training contains, and what medium it is presented in. Those aspects are briefly summarized in Table 1.

Table 1 Identified aspects of SETA delivery

<table>
<thead>
<tr>
<th>Aspect</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>How training is delivered</td>
<td>How includes the practices used when delivering training. This includes physical presentations, short sequences sent via e-mail, plain text the user is expected to find and read, etc.</td>
</tr>
<tr>
<td>When the user is trained</td>
<td>This concerns the timing of the training. E.g., is the user scheduled for training, should it be on-demand, or it is sent at regular intervals</td>
</tr>
<tr>
<td>What level of information that is presented</td>
<td>This concerns the detail level of the information the user is provided with</td>
</tr>
<tr>
<td>What medium it is presented in</td>
<td>Medium describes the medium the training is in, such as games, video, or plain text.</td>
</tr>
</tbody>
</table>

The level aspect is directly derived from Hu et al. (2021b) who state that SETA can be delivered with different levels of information. Hu et al. (2021b) also describe the delivery method as important for the efficiency of a SETA program. Our research has expanded this into
considering how and when training is delivered, and what medium is used for its presentation. The rationale is that previous literature identified that those three aspects impact user perception of SETA programs. Kävrestad, Skärgård, and Nohlberg (2019) show that users prefer digital training over physical and exemplifies the impact of the ‘how’ aspect. Reinheimer et al. (2020) exemplifies the ‘when’ aspect by researching how the timing of training impacts user preferences. The ‘medium’ aspect is exemplified by Tschakert and Ngamsuriyaroj (2019), where user preferences in relation to training based on video, text and games are researched.

**RESEARCH OBJECTIVES**

As so far demonstrated, user behavior has attracted interest from researchers and practitioners for a long time. Yet, security issues and breaches stemming from human behavior seem as common as ever before (Ani, He, & Tiwari, 2019; Hatfield, 2018; Zimmermann & Renaud, 2019). While SETA programs are continuously suggested as means to solve the problem of insecure user behavior, researchers argue that many SETA programs lack a theoretical basis and empirical evaluation of effectiveness (Abraham & Chengalur-Smith, 2019; Siponen & Baskerville, 2018).

Various research efforts evaluating aspects of SETA methods have been published. For instance, in the context of phishing, a recent review shows that training methods using an embedded approach managed to showcase strong results (Al-Daeef et al., 2017). Several other studies suggest that the effects of training interventions wear off unless the training is reinforced (Kim, Lee, & Kim, 2018; Lastdrager, Gallardo, Hartel, & Junger, 2019). Scholars also suggest that awareness-increasing mechanisms, such as warnings, promote secure behavior (Xiong et al., 2019; Yang, Xiong, Chen, Proctor, & Li, 2017). However, there is a lack of empirical reviews evaluating and comparing different SETA methods. Further, Hu et al. (2021b) describes that delivery of SETA programs is an important topic that has not received much attention in past research. To that end, the aim of our study is to:
Evaluate user preferences regarding SETA delivery and discuss the results in relation to existing methods for SETA.

The first part of the research aim concerns evaluating how the SETA methods meet user preferences regarding SETA delivery. To this end, our study examines user preferences of SETA delivery in regard to the aspects presented in Table 1, and thereby meets the following objective:

**O1: Identify user preferences regarding the delivery of SETA methods.**

The second aspect of the aim is to outline existing methods for SETA. A taxonomy describing identified SETA methods in terms of the aspects presented in Table 1 was developed. The result is a summation of SETA methods discussed in scientific literature. The following objective was established for this process:

**O2: Develop a taxonomy of SETA methods.**

Once user preferences are identified, the results will be used to extend the taxonomy of SETA methods to include how those compare with regard to user preferences. The resulting taxonomy presents the SETA methods discussed in scientific literature and how those respond to user preferences. The objective addressed in this step was:

**O3: Evaluate how existing SETA methods respond to user preferences for SETA delivery.**

Previous studies suggest that it is reasonable to assume that SETA methods will be perceived differently amongst professional users and other users (Siponen, 2001). Our study explores this notion in relation to the aforementioned objectives.

**RESEARCH APPROACH AND RESULTS**
Our study uses a mixed-methods research design where a qualitative approach is used to identify and classify existing SETA methods, and a quantitative approach is used to measure user preferences regarding SETA methods. The research design follows three distinct steps and intends to meet the overall research goal: *Evaluate user preferences regarding SETA delivery and discuss the results in relation to existing methods for SETA.*

First, a survey is used to measure user preferences regarding SETA delivery. Next, a literature review is conducted to identify existing SETA methods and describe how they deliver SETA. The results are then combined to display how existing SETA methods respond to user preferences. Figure 1 shows an overview of the research process and the expected primary outcomes of each research process. The remainder of this section will describe the method and results for each research step.

![Figure 1 Research process overview](image)

**Identification of user preferences regarding SETA delivery**

A web-based survey was used to research our study’s second objective: *Identify user preferences regarding SETA delivery.* Once the survey had undergone pilot testing, it was sent out to participants by the survey provider Webropol. It was sent out to a sample of 10 times the target sample size, using e-mail, and the survey was open until enough answers were
collected. The data collection period lasted for about a week. The study’s primary focus was Swedish internet users, and 834 respondents were recruited from here, while 314 and 304 were recruited from Italy and the UK, respectively, to assess the generalizability of the results and detect inter-European cultural differences.

**Instrumentation**

The research team developed a survey of five questions, and the questions were designed to let the participants pick their two most favored options of various aspects of SETA delivery. The order of the answer-alternatives was randomized within each question to minimize exposure to question-order bias.

To ensure that the survey was easy to understand and measured the right things, we performed a pilot procedure to evaluate the survey. The pilot included the following steps:

1. Pilot the survey with random participants recruited using social media. The participants were explicitly asked to report if the survey was easy to understand.

2. Evaluate the survey using two participants who took the survey supervised by a researcher using a think-aloud approach to evaluate participants’ perception of the survey questions.

3. Evaluate the survey through an interview with a statistician to evaluate the appropriateness of the questions in relation to the intended statistical procedures.

4. Pilot the survey by distributing it to research colleagues asked to evaluate the survey in relation to the research goals.

The survey was distributed to the survey participants once it was positively evaluated. The survey items are presented together with the results throughout this section. The items are also outlined in Appendix C with references to the previous work that they are based upon.
Sampling

The study used a stratified sampling method where subgroups were created based on a range of variables, and proportional samples were drawn from each subgroup to create probability samples as described by Henry (1990). The subgroups were created based on gender, age, and geographical region. Once the subgroups were created, equal proportions of each subgroup were recruited to the survey to ensure representative samples using simple random sampling as described by Scheaffer, Mendenhall III, Ott, and Gerow (2011). A stratified sampling method was selected since it is expected to produce samples representative of the sampled populations (Rahi, 2017). The sample was obtained using a web panel; thus, the possible participants were limited to members of the web panel, which introduced a risk of sampling bias. This risk was counteracted by using stratified random sampling as just described. Further, the possible exclusion of individuals not using computers is not considered problematic as our research topic does not concern that group. Using a web panel has been suggested to provide a higher level of data reliability than surveys administered over telephones since it reduces the researcher bias (Braunsberger, Wybenga, & Gates, 2007).

Data Analysis and results

The participants were first asked about what gender they identified themselves as, their age, and their perceived IT competence. The results to those questions are presented in Table 2 and provide a demographical overview of the sample. Table 2 showcases an approximately even split by gender across all three sample groups and a generally similar level of balance in the age-related subgroups.

Table 2 Demographic overview of survey respondents

<table>
<thead>
<tr>
<th>Variable</th>
<th>Answer</th>
<th>Sweden (n=834)</th>
<th>UK (n=304)</th>
<th>Italy (n=314)</th>
<th>All (n=1452)</th>
</tr>
</thead>
</table>

Page number 13
The participants rated their own IT proficiency by selecting one of four competence groups. The competence groups were described to the participants as follows:

- **Professional** - working in, hold a degree in, or study IT
- **Expert user** - Interested user and know my way around IT. Usually asked to help people with home routers, printer installations, etc
- **Average user** - I use IT with no major problems, but need help occasionally
• Below Average - I have a hard time using IT and feel like I need help with tasks that others do with ease

The remainder of this section examines the questions measuring the participant’s preferences in the four aspects of SETA delivery. The discussion is structured according to the four established aspects of information security training and ends with a conclusion that summarizes the results. The results are presented as percentages of participants that picked a particular option, and 95% confidence intervals (CI) are calculated as the maximum CI for a specific question and sample combination as described by Wheelan (2013). Two values are significantly different when their CI does not overlap.

The data is presented for the entire dataset and split based on the sampling groups to identify general tendencies and differences between the sample groups. The impact of IT proficiency will be tested by redoing the data analysis procedure without the respondents who report being IT professionals. The survey data was analyzed using the software SPSS.

How Training is Delivered

To evaluate how users prefer to have cybersecurity training delivered, the survey participants were asked to pick the two options they favored the most of the following:

• In physical lectures/presentations that I attend at a specific time
• In recorded lectures/presentations delivered to me via e-mail
• In written text delivered to me digitally
• In short sequences presented in a context where they are relevant, e.g., password tips when I am creating a password
• In short sequences sent to me at regular intervals
The results for the complete dataset (All) and split into the nation-based groups are presented in Table 3. Each proportion should be interpreted as +/- the confidence interval and non-overlapping confidence intervals signify proportions significantly separated from each other.

**Table 3 Preferences on how to receive security training/education, separated by national sample groups**

<table>
<thead>
<tr>
<th>Select how you would prefer to receive information security training/education</th>
<th>All (n=1452)</th>
<th>Sweden (N=834)</th>
<th>UK (N=304)</th>
<th>Italy (N=314)</th>
</tr>
</thead>
<tbody>
<tr>
<td>In physical lectures/presentations that I attend at a specific time (O1)</td>
<td>21.0%</td>
<td>18.5%</td>
<td>21.1%</td>
<td>27.7%</td>
</tr>
<tr>
<td>In recorded lectures/presentation delivered to me via e-mail (O2)</td>
<td>38.2%</td>
<td>38.2%</td>
<td>34.2%</td>
<td>42.0%</td>
</tr>
<tr>
<td>In written text delivered to me digitally (O3)</td>
<td>44.9%</td>
<td>45.4%</td>
<td>43.4%</td>
<td>44.9%</td>
</tr>
<tr>
<td>In short sequences presented in a context where they are relevant, e.g., password tips when I am creating a password (O4)</td>
<td>55.0%</td>
<td>60.4%</td>
<td>50.0%</td>
<td>45.2%</td>
</tr>
<tr>
<td>In short sequences sent to me at regular intervals (O5)</td>
<td>40.9%</td>
<td>37.4%</td>
<td>51.3%</td>
<td>40.1%</td>
</tr>
<tr>
<td>95% Confidence interval</td>
<td>2.6%</td>
<td>3.4%</td>
<td>5.6%</td>
<td>5.5%</td>
</tr>
</tbody>
</table>

Table 3 shows that most respondents prefer to have SETA delivered in short sequences in situations where the training is relevant. The tendency is statistically significant for the samples “all” and “Sweden.” Further, Physical sessions attended at a specific time is the least favored option, with statistical significance in all answer groups. The other options share overlapping confidence intervals, and no meaningful conclusions can be drawn regarding how the participants prioritize them.

To test if the results are affected by IT proficiency, respondents who reported being IT professionals were removed from the dataset, and the results recalculated. The results are shown in Table 4 below.

**Table 4 Preferences on how to receive security training/education, with answers from IT professionals being disregarded**

<table>
<thead>
<tr>
<th>Select how you would prefer to receive information security training/education</th>
<th>All (n=1274)</th>
<th>Sweden (N=756)</th>
<th>UK (N=274)</th>
<th>Italy (N=244)</th>
</tr>
</thead>
</table>

Page number 16
In physical lectures/presentations that I attend at a specific time (O1) & 19.4% & 17.9% & 20.1% & 23.4% \\
In recorded lectures/presentation delivered to me via e-mail (O2) & 37.8% & 37.7% & 33.6% & 42.6% \\
In written text delivered to me digitally (O3) & 46.4% & 46.8% & 43.4% & 48.4% \\
In short sequences presented in a context where they are relevant, e.g., password tips when I am creating a password (O4) & 55.2% & 59.8% & 50% & 46.7% \\
In short sequences sent to me at regular intervals (O5) & 41.3% & 37.8% & 52.9% & 38.9% \\
95% Confidence interval & 2.7% & 3.6% & 5.9% & 6.3% \\

As seen in Table 4, the results are slightly different from those presented in Table 3. However, all differences have overlapping CI and are therefore not significant. The resulting conclusion, in this case, is that IT proficiency cannot be shown to have any impact on how users prefer to have SETA delivered. The results for how users prefer to have SETA delivered are that the most preferred option is to have it presented in short sequences when it is of direct relevance (contextual). That is followed by training sent digitally. The least preferred option is to attend physical sessions at a specific time. The results indicate national differences since no significant difference can be seen between UK and Italy regarding contextual training and training delivered at regular intervals or on-demand.

**When Training is Delivered**

The aspect of when users prefer to partake in training was explored using two questions where the participants were asked to pick their two most favored answer options. The set of options and results are presented in Table 5. The value in parenthesis holds the results for the dataset, excluding participants who report being IT professionals. The results will be presented in this manner from hereon to preserve space.

**Table 5 Preferences on when to receive security training/education**

<table>
<thead>
<tr>
<th>Select when you would prefer to receive information security training/education</th>
<th>All (n=1452)</th>
<th>Sweden (N=834)</th>
<th>UK (N=304)</th>
<th>Italy (N=314)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The data presented in Table 5 suggest that O3 is favored for the groups “All,” “Sweden,” and “UK,” followed by O2. The CI for O2 and O3 overlap for the “UK” sample. O2 is favored by the “Italy” group but with a CI that overlaps with O3. Further, O1 is the least favored for all answer groups with non-overlapping CI in all groups except “Italy.” As such, the results suggest that users prefer to have training delivered contextually with on-demand as a close second. Attending SETA programs in planned sessions is the least preferred option. The results are slightly changed when answers from IT professionals are disregarded but not so that the conclusions are changed.

The results for the second question in this aspect are presented in Table 6. The values in parenthesis show the results when the answers from participants reporting to be IT professionals are disregarded.
O1 is the answer option that is preferred in all answer groups. It is significantly preferred over any other option for the groups “All” and “Sweden” while the CI overlaps with O3 for “UK” and with O2 and O3 for “Italy.” O4 is the least preferred option in all groups except “Sweden,” where all options except O1 are well within the CI and should be seen as equal. Disregarding answers from participants who state that they are IT professionals has a slight but insignificant impact on the results. The data gathered using this question further the results presented in Table 5, suggesting that contextual delivery is most preferred while attending training at a specific time is least preferred. The data also emphasizes the notion of national differences regarding when users prefer to have SETA programs delivered.

**Level of Provided Information**

The level of information the user preferred was explored using one question where the respondents were again asked to pick their two most favored options. The options presented to the participants and the results are presented in Table 7 below. The values in parenthesis show the results when answers from the participants that consider themselves to be IT professionals are disregarded.

**Table 7 Preferences on level of information received**

<table>
<thead>
<tr>
<th>Select what level of information you prefer</th>
<th>All (n=1452)</th>
<th>Sweden (N=834)</th>
<th>UK (N=304)</th>
<th>Italy (N=314)</th>
</tr>
</thead>
<tbody>
<tr>
<td>I want to receive the most important bullets and options for more and deeper information (O1)</td>
<td>73.2% (73.3%)</td>
<td>77.9% (77.5%)</td>
<td>71.4% (73.0%)</td>
<td>62.4% (60.7%)</td>
</tr>
<tr>
<td>I want to receive only the most important bullets (O2)</td>
<td>69.8% (71.3%)</td>
<td>74.9% (75.5%)</td>
<td>65.5% (67.5%)</td>
<td>60.2% (62.3%)</td>
</tr>
<tr>
<td>I do not want any security related information (O3)</td>
<td>18.2% (17.9%)</td>
<td>16.5% (16.7%)</td>
<td>19.1% (19.0%)</td>
<td>21.7% (20.5%)</td>
</tr>
<tr>
<td>I want to receive all information on a subject (O4)</td>
<td>38.8% (37.5%)</td>
<td>30.6% (30.3%)</td>
<td>44.1% (40.5%)</td>
<td>55.7% (56.6%)</td>
</tr>
<tr>
<td>Maximum 95% CI</td>
<td>2.50%</td>
<td>3.1%</td>
<td>5.6%</td>
<td>5.5%</td>
</tr>
</tbody>
</table>
The data presented in Table 7 shows that O1 is favored by all answer groups, followed by O2. The CI of O1 overlaps with the CI of O2 in all cases and with O4 for the answer group “Italy.” O3 is the least preferred option in all answer groups. The results show that users want to receive security-related information concisely where the most essential information should be in focus. Further, while O1 and O2 can’t be separated with statistical significance, the data suggests that the possibility of receiving deeper information is favorable. While the tendencies are consistent over all national groups, there are national differences in the gathered data. The results are slightly, but insignificantly, impacted by removing responses from IT professionals.

**What Medium That is Preferred**

The last aspect of cybersecurity training evaluated in our paper concerns the medium used to deliver the training. The participants were asked to pick their two most favored options. The options presented to the participants and the results are shown in Table 8 below. The values in parenthesis show the results when answers from the participants that consider themselves to be IT professionals are disregarded.

<table>
<thead>
<tr>
<th>Select in what mediums you prefer to access information security training</th>
<th>All (n=1452)</th>
<th>Sweden (N=834)</th>
<th>UK (N=304)</th>
<th>Italy (N=314)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Written text (O1)</td>
<td>66.0% (67.0%)</td>
<td>68.5% (69.8%)</td>
<td>63.8% (64.6%)</td>
<td>61.5% (60.7%)</td>
</tr>
<tr>
<td>Video (O2)</td>
<td>57.7% (57.5%)</td>
<td>59.0% (58.2%)</td>
<td>54.6% (55.1%)</td>
<td>57.3% (57.8%)</td>
</tr>
<tr>
<td>Audio (O3)</td>
<td>17.7% (17.0%)</td>
<td>12.6% (12.4%)</td>
<td>22.4% (21.9%)</td>
<td>26.8% (25.8%)</td>
</tr>
<tr>
<td>Interactive Video/Game (O4)</td>
<td>29.0% (28.7%)</td>
<td>30.6% (29.6%)</td>
<td>25.7% (26.6%)</td>
<td>28.0% (28.3%)</td>
</tr>
<tr>
<td>Face to Face (e.g. Lecture or one-on-one) (O5)</td>
<td>29.6% (29.8%)</td>
<td>29.4% (29.9%)</td>
<td>33.6% (31.8%)</td>
<td>26.4% (27.5%)</td>
</tr>
<tr>
<td>Maximum 95% CI</td>
<td>2.50%</td>
<td>3.3%</td>
<td>5.6%</td>
<td>5.5%</td>
</tr>
</tbody>
</table>
Table 8 shows that O1 is favored in all answer groups with non-overlapping CI for “All” and “Sweden” and with CI overlapping with O2 for “UK” and “Italy.” O4 and O5 share CI in all answer groups, and O3 is included in the same CI for “UK” and “Italy.” The results suggest that Written text or Video are the most preferred forms of cybersecurity training while the others are less favored with some national differences. Italian respondents are, for instance, more positive towards audio-based training than Swedish respondents. Still, the data suggests that users generally prefer Audio to a lesser extent than Interactive videos or games, or physical sessions. The results are only impacted in an insignificant way by disregarding responses from IT professionals.

**Summary of survey results**

The survey aim was to meet the first objective of our paper: Identify user preferences regarding SETA delivery. This was done by surveying respondents' preferences regarding four aspects of SETA delivery. A summary of the results of the survey is presented in Table 9.

*Table 9 Summary of survey results*

<table>
<thead>
<tr>
<th>Aspect</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>How training is delivered</strong></td>
<td>The strongest conclusion is that the participants preferred digital training over physical sessions. Among digital delivery methods, the results demonstrate a tendency towards preferring contextual training over training delivered in some other way.</td>
</tr>
<tr>
<td><strong>When the user is trained</strong></td>
<td>The data regarding this aspect suggests that SETA delivered at a flexible time is preferred over scheduled delivery. A tendency towards preferring to access SETA programs on-demand or having it appear in a situation of relevance can also be seen.</td>
</tr>
<tr>
<td><strong>What level of information that is presented</strong></td>
<td>The results show that most users want to receive security-related information. Further, the participants prefer to receive the most important information, with or without an option for more information, to receive all information on a topic.</td>
</tr>
<tr>
<td><strong>What medium it is presented in</strong></td>
<td>Regarding the medium of presentation, three groupings can be observed in the data. The respondents prefer to have SETA programs as text or video, while two less preferred mediums are interactive videos or games, or face-to-face instructions. Finally, audio-based training was the least preferred option.</td>
</tr>
</tbody>
</table>
Our research also evaluated whether the survey results were consistent over different intra-European cultures. While the central tendencies were similar, there were variations between the national sample groups. The most apparent difference is that the Italian sample does not have as discriminative results as the Swedish and UK samples. As such, the study demonstrates that there are indeed distinct cultural variations in how cybersecurity training is perceived, and this notion aligns well with prior research (Al Neaimi & Lutaaya, 2018; AlSabah, Oligeri, & Riley, 2018; Onumo et al., 2017). Additionally, IT competence does not impact user preferences regarding SETA delivery to any meaningful degree.

**Development of a taxonomy of SETA methods**

The first objective of our study was to *develop a taxonomy of SETA methods*. A structured literature review was performed to identify SETA methods described in scientific literature and describe those according to the four aspects identified in Table 9, namely:

1. How they deliver training,
2. When they deliver training,
3. What level of information they provide, and
4. What medium they use.

The SLR began with establishing a process based on Paré and Kitsiou (2017). The SLR process and output from the different steps are presented in Figure 2.
The search query was developed to identify all papers that discussed SETA methods. It was applied to titles, abstracts, and author keywords to ensure that the searches resulted in papers primarily discussing SETA methods. Since the study intends to identify SETA methods in general, no exclusion was made based on publication date. The searches were executed on 2021-02-11 and resulted in 3739 hits distributed as follows:

- Web of Science (Core Collection): 1472 hits
- Science Direct: 148 Hits
- Scopus: 2119 hits

Web of Science and Scopus were included as recognized international repositories of peer-reviewed publications. Science Direct, a publisher repository, was also included since it includes several journals specifically relevant to the aim of the research. The selection process continued by applying the inclusion criteria described in Table 10. The abstracts of all identified papers were downloaded and imported into Endnote. 409 papers were identified as duplicates and removed from the SLR. The selection process continued in two further steps resulting in a total of 76 papers that were included in the survey:

1. Titles and abstracts were analyzed, and papers out of the study’s scope were excluded (174 papers remained after this step).
2. The full body of the papers was scanned during the analysis process resulting in 76 papers being included in the survey.

Table 10 SLR inclusion criteria

<table>
<thead>
<tr>
<th>Inclusion criteria</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Published in a peer-reviewed conference or journal</td>
<td>Ensures quality of included papers</td>
</tr>
<tr>
<td>Written in English</td>
<td>Ensures that included papers can be understood by the researchers</td>
</tr>
<tr>
<td>Not a duplication of another included paper</td>
<td>Ensures that publications are only included once</td>
</tr>
<tr>
<td>Describes SETA methods intended for end-users</td>
<td>Limits the review's scope to publications describing SETA methods rather than just presenting or mentioning it</td>
</tr>
<tr>
<td>Describes at least one SETA method well enough to allow for the analysis to identify at least two of the aspects of interest for the study</td>
<td></td>
</tr>
</tbody>
</table>

The included papers were analyzed using thematic coding in an open fashion (Braun & Clarke, 2006). The papers were analyzed one by one as follows:

1. The paper was read until a SETA method was identified.
   - If the SETA method was not previously identified, it was added as a new method.
   - If the SETA method was previously identified, the paper was connected to that SETA method.
   - If no SETA method was identified, the paper was excluded from the study

2. Information regarding the four aspects of how the SETA method is delivered was extracted from the paper and added to the taxonomy.

3. 1 and 2 were re-iterated until no more SETA methods could be identified in the paper.

The coding procedure is exemplified in Appendices A and B. Appendix A presents the coding of one single paper while Appendix B illustrates the complete coding for a single SETA method. Table 11 lists the identified SETA methods linked to the paper they appear in. Full
references to the included papers are found in the reference list. Note that one paper may discuss several SETA methods.

Table 11 Identified SETA methods and papers they appear in

<table>
<thead>
<tr>
<th>Method</th>
<th>Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out-of-bands simulation</td>
<td>(Aldawood &amp; Skinner, 2019; Burris, Deneke, &amp; Maulding, 2018; Ntokas, Maratou, &amp; Xenos, 2015; Yamin, Katt, &amp; Gkioulos, 2020)</td>
</tr>
<tr>
<td>Attack simulations</td>
<td>(Aldawood &amp; Skinner, 2019; Alwanain, 2020; Bakar, Mohd, &amp; Sulaiman, 2018; Caputo, Pfleeger, Freeman, &amp; Johnson, 2014; Carella, Kotsoev, &amp; Truta, 2017; Dodge Jr, Carver, &amp; Ferguson, 2007; Dodge &amp; Ferguson, 2006; Higashino, Kawato, Ohmori, &amp; Kawamura, 2019; Jansson &amp; von Solms, 2013; Lee et al., 2019; Pirocca, Allodi, &amp; Zannone, 2020; Styles &amp; Tryfonas, 2009)</td>
</tr>
<tr>
<td>E-learning</td>
<td>(Abawajy, 2014; Aldawood &amp; Skinner, 2019; Arain, Tarraf, &amp; Ahmad, 2019; Charoen, Raman, &amp; Ofman, 2008; Cooper, 2008; Cox, Connolly, &amp; Currall, 2001; Dlamini &amp; Modise, 2012; Dukarm, Dill, &amp; Reith, 2019; Eminağaoğlu, Uçar, &amp; Eren, 2009; Figueroa &amp; Ayyagari, 2015; Furrnell, Warren, &amp; Dowland, 2003; Goluch et al., 2007; Gundu &amp; Flowerday, 2013; Hagen &amp; Albrechtsen, 2009; Hansche, 2001; He et al., 2020; Hepp, Tarraf, Birney, &amp; Arain, 2018; Jenkins &amp; Ducikova, 2013; Jensen, Dinger, Wright, &amp; Thatcher, 2017; Labuschagne &amp; Eloff, 2012; Mashiane, Dlamini, &amp; Mahlangu, 2019; McCoy &amp; Fowler, 2004; Oroszi, 2019; Power &amp; Forte, 2006; Schürmann, Jensen, &amp; Sigbjörnsdóttir, 2020; Shaw, Chen, Harris, &amp; Huang, 2009; Shaw, Keh, Huang, &amp; Huang, 2011; Smith, Mediavilla, &amp; White, 2018; Tschakert &amp; Ngamsuriyaroj, 2019; Younis &amp; Musbah, 2020)</td>
</tr>
<tr>
<td>Interactive E-learning</td>
<td>(Alkhamis &amp; Renaud, 2016; Kovačević &amp; Radenković, 2020; Moul, 2019; Tan et al., 2020; Tsokkis &amp; Stavrou, 2018)</td>
</tr>
<tr>
<td>Regular security updates</td>
<td>(He et al., 2020; Power &amp; Forte, 2006)</td>
</tr>
<tr>
<td>Instructor-led lecture</td>
<td>(Albrechtsen &amp; Hovden, 2010; Aldawood &amp; Skinner, 2019; Carella et al., 2017; Charoen et al., 2008; Cox et al., 2001; Ding, Meso, &amp; Xu, 2014; Dlamini &amp; Modise, 2012; Eminağaoğlu et al., 2009; Ferreira, Correia, &amp; Da Costa Pereira, 2005; Hansche, 2001; Heikka, 2008; Mashiane et al., 2019; McCoy &amp; Fowler, 2004; McCrohan, Engel, &amp; Harvey, 2010; Nogwina, Gumbo, &amp; Ngqulu, 2019; Power &amp; Forte, 2006; Tschakert &amp; Ngamsuriyaroj, 2019)</td>
</tr>
</tbody>
</table>
Table 12 presents an overview of the SLR results as a taxonomy of the identified SETA methods and a description of how each method delivers SETA regarding the aspects discussed in our research. The methods are described further and evaluated regarding user preferences in the upcoming section.

<table>
<thead>
<tr>
<th>Method</th>
<th>How training is delivered</th>
<th>When the user is trained</th>
<th>What level of information that is presented</th>
<th>What medium it is presented in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out-of-bands simulation</td>
<td>Digitally</td>
<td>On-demand or at a scheduled time</td>
<td>Unspecified leaning towards extensive</td>
<td>Unspecified interactive digital material</td>
</tr>
<tr>
<td>Attack simulations</td>
<td>Digitally but can include physical elements</td>
<td>Unspecified but commonly contextual or scheduled session</td>
<td>Unspecified</td>
<td>Unspecified</td>
</tr>
<tr>
<td>E-learning</td>
<td>Digitally</td>
<td>On-demand or on a regular basis</td>
<td>Unspecified leaning towards extensive</td>
<td>Unspecified digital material</td>
</tr>
<tr>
<td>Interactive E-learning</td>
<td>Digitally</td>
<td>On-demand or on a regular basis</td>
<td>Unspecified leaning towards extensive</td>
<td>Unspecified interactive digital material</td>
</tr>
<tr>
<td>Regular security updates</td>
<td>Digitally</td>
<td>On a regular basis</td>
<td>Brief</td>
<td>Video or text</td>
</tr>
<tr>
<td>Instructor-led lecture</td>
<td>Physically</td>
<td>At a scheduled time</td>
<td>Extensive</td>
<td>Unspecified</td>
</tr>
<tr>
<td>Gamified training</td>
<td>Digitally</td>
<td>On-demand or on a regular basis</td>
<td>Unspecified leaning towards extensive</td>
<td>Gamified material</td>
</tr>
</tbody>
</table>

Table 12 Taxonomy of identified SETA methods
### Evaluation of SETA methods with regards to SETA delivery

This section describes each identified SETA method and discusses each method in relation to the identified user preferences regarding SETA delivery. It meets the research's third objective: *Evaluate how existing SETA methods respond to user preferences for SETA delivery.*

#### Out-of-bands simulations

Out-of-bands simulations allow the user to experience cybersecurity events, act on them, and experience the results of their actions. This training type is discussed in four of the included papers making it one of the least discussed training types. The training is delivered using a digital platform that can be sent to the user in numerous ways. The training may take place at a set time but may also be available on-demand. The level of information presented to the user can vary but goes beyond a simple warning or bullet list. The medium used to deliver out-of-bands simulations is some unspecified online material. In light of the identified user preferences, Out-of-bands simulations can avoid the delivery options least favored by the participants; physical training at fixed times. However, it cannot be delivered in a context where it is of direct relevance because it is defined as a simulated scenario. As for the level of information provided to users, this SETA type leans towards providing users with extensive information while users prefer less elaborate information. In that regard, our research suggests
that simulating one security-related event at the time and keeping information concise can improve user perception of Out-of-bands simulations.

**Attack simulations**

An attack simulation is a SETA method where an attack is simulated against a group of users, and the results of the attack are reported to the users to raise awareness. The included literature primarily discusses simulated phishing attacks, but password guessing attacks are also mentioned. Two main methods for attack simulations are found in the literature. In the first case, users are being targeted by an attack, and if they fall for the attack (e.g., clicks a link in a false phishing e-mail), they are directed to an informational web page intended to provide training on phishing. In the other case, a phishing attack is carried out and statistics calculated (e.g., how many users were tricked by the attack). The results are communicated to the users, commonly using e-mail or a physical presentation. The assessment focuses on the information presented to the users and suggests that brief information presented digitally as part of the simulated attack is the most preferred method. Presenting information during physical sessions is less preferred, and in any case, brief information is preferred over extensive. If training is embedded in the attack simulation, the approach matches the user preference identified in our study. Likewise, attack simulations where information is presented to users during a longer physical session are less appreciated.

**E-learning and interactive E-learning**

E-learning is one of the most commonly discussed SETA methods, mentioned in 30 included papers. Subsequently, it is discussed in somewhat different ways and, in some cases, called interactive E-learning discussed in another five papers. What signifies E-learning is that training is delivered digitally in a flexible manner. Learners are typically able to access the E-learning material on-demand and may or may not be reminded about it, for instance, using
regular e-mail notifications. There are examples of E-learning modules that range from very brief to very comprehensive in terms of information presented, and the use of mediums is also varying. The difference between E-learning and interactive E-learning is that interactive E-learning modules are designed with interactivity as a mandatory component, while E-learning may or may not have interactive elements. Our research suggests that users prefer less interactive elements and that the digital and flexible properties of e-learning are favorable. However, the survey results show that users prefer brief information while most e-learning approaches lean towards more extensive information. Nothing is hindering SETA programs delivered as e-learning to be brief, and a result of our research is that such e-learning is more likely to be appreciated by its users.

**Regular security updates**

Regular security updates include information sent to users using digital means and at regular intervals and are discussed in two included papers. The information is brief and in the form of text or videos. Both the level of information and used mediums match well with identified user preferences. However, while regular updates are preferred over scheduled physical sessions, contextual delivery is preferred over regular updates.

**Instructor-led lectures**

Instructor-led lectures are the third most commonly discussed SETA method and are described in 18 included papers. It involves participants participating in a scheduled session led by an instructor. The sessions can be interactive and commonly cover various topics or detailed information surrounding a single topic. Owning to the physical nature of this SETA method, that it does provide detailed information and is restricted to a scheduled time, it is a poor match to the user preferences identified in our research.

**Gamified training and game contests**
The second most commonly discussed SETA method is gamified training, discussed in 25 included papers. Gamified training is SETA, where game mechanics are used to make the process of learning cybersecurity more engaging. In terms of SETA delivery, it shares many similarities with E-learning in that it is commonly delivered digitally in an on-demand fashion. The delimiter between gamified training and e-learning is that gamified training uses, by definition, a game as the medium of delivery. Like e-learning, training delivered on-demand or on a regular basis can be appreciated by users, albeit not as appreciated as contextual delivery. The gamified training described in most of the included papers presents the users with extensive information while users prefer briefer information. There is, however, no reason why gamified training can’t be developed to provide brief information, and our research suggests that such a design would increase user appreciation. A variety of gamified training is game contests, and the major difference between the two is that game contests require more than one participant and take place at a scheduled time. A game contest means that the game is competitive, and the participants compete against each other or against a defined scenario. The multi-player nature requires that game contests occur at a scheduled time, or at least a time agreed upon by the participants. The added competitive element is intended to engage users. However, our research suggests that the scheduled nature of game contests is a challenge in terms of user preferences.

**Context-based training**

In four included papers, context-based training is discussed as training presented to users in potentially risky situations. Phishing training is, for instance, presented to a user with an elevated chance of encountering a phishing e-mail. The level of information presented is described as narrow with or without an option for more information. The medium is described in the literature as undefined, but the examples show text, video, and interactive elements. The contextual and brief nature of context-based training matches the user preferences.
identified in our research. Further, a suggestion from our research is to use text or video as the medium for information presentation.

**Written materials**

Written materials are described in three included papers and include physical text in various forms. It may take the form of a book or a more brief textual description such as a pamphlet and is accessible to the holder on-demand. While written materials' physical nature does not match identified user preferences, the textual presentation does. Our research further suggests that users can appreciate brief written materials while more extended materials requiring more effort will struggle in terms of user preferences.

**Security awareness campaigns**

Security awareness campaigns are mentioned in four included papers as efforts where physical information campaigns are being executed using posters, pamphlets, and similar. The material is physical, and the delivery time is best described as continuous since the campaign material is constantly present during the campaign time. The information is brief, and the medium is commonly text with or without graphical components. Continuous delivery is not included in our research. Still, since it is not contextual nor requires users to attend at a specific time, it can be argued to match on-demand or regular delivery which is fairly appreciated by the participants in our research. Further, the brief and text-based nature of campaign material is a good match to user preferences identified in our research. It should also be noted that security awareness campaigns are discussed in some papers as a combination of SETA methods during a limited time. That can, for instance, mean that a physical session starts a campaign and is followed by pamphlets and access to e-learning. Such combinations of SETA methods are not considered in our research.

**DISCUSSION**
Our paper aimed to *Identify existing methods for SETA and evaluate to what extent those methods meet user preferences in regards to the delivery of SETA*. This goal was met by a mixed-method approach using a web-based survey to research user preferences regarding SETA delivery and a literature review to identify SETA methods discussed in scientific literature. The results of those steps were combined by discussing how the identified SETA methods matched user preferences.

The first objective, *Identify user preferences regarding SETA delivery*, was researched using a survey that measured how users prefer to have SETA programs delivered in four different aspects; when, how, what level of information, and what mediums were preferred. The results suggest that users are interested in having a system deliver SETA in situations where the training is relevant or access SETA programs on-demand. Delivering SETA in a specific situation means that the user is interrupted when training is presented, causing a disruption. Hu, Hsu, and Zhou (2021a) studied the effect of perceived disruptions on behavioral intentions and found indications that disruptions could negatively impact behavioral intentions. However, other recent research found evidence that contextual SETA programs effectively mediates behavioral change (Kävrestad & Nohlberg, 2020; Zimmermann & Renaud, 2021). Additionally, Wu, Moody, Zhang, and Lowry (2020) showed that security notifications are important mediators of security behavior, but too intrusive notifications can irritate users and influence security behavior negatively. In light of related research, our research suggests that contextual SETA programs can be positively received by users, but care must be taken so that it is not too disruptive. Given the research showing positive effects of contextual training, finding a good level of disruption makes a key direction for future work as that is likely to result in SETA programs that are both effective in terms of behavioral change and user perception.
Further, our research suggests that users want to get only the most important information presented to them digitally rather than in face-to-face sessions. On an abstracted level, this suggests that users are interested in security to the degree that they want to know what to do and how. However, they do not want to spend a lot of effort on the matter. This notion aligns well with previous research showcasing that security is often not a top priority for users (Caulfield, Spring, & Sasse, 2019; Sombatruang, Onwuzurike, Sasse, & Baddeley, 2019).

The results suggest that users prefer SETA programs to be flexible or contextual, and require little effort from the participants. A low proportion of the participants preferred options requiring that SETA subjects are educated at a specific time or place, and a larger proportion preferred more flexible options. That is in line with how Davis (1989) describes the TAM construct *perceived ease of use (PEOU)* as how effortless a person believes using a system will be. The results are also in line with Venkatesh and Davis (2000), who suggest voluntariness as a factor that influences the TAM constructs *Perceived usefulness (PU)* and *Intention to use (IU)*. Based on the results of our research, three recommendations for increasing PEOU, PU, and IU for SETA programs can be made based on our study:

1. The timing of SETA should be flexible or contextual. That allows the user to control when they participate in SETA programs, which invokes a sense of voluntariness.
2. The presented material should be short and relevant for the user. Short material ensures that the effort needed by the user is kept to a minimum. Further, keeping the material relevant is argued by Venkatesh and Davis (2000) to increase PU.
3. The primary medium should be text, but enabling users to choose their preferred medium is beneficial.

Our research included participants from three different nations to enable a discussion on the generalizability of the results. Samples from Sweden, the UK, and Italy were acquired. While the central tendencies were similar, a more detailed analysis revealed distinct differences. As
such, the study demonstrates that there are indeed distinct cultural variations in how cybersecurity training is perceived, and this notion aligns well with prior research (Al Neaimi & Lutaaya, 2018; AlSabah et al., 2018; Onumo et al., 2017). The most apparent difference is that the Italian sample does not have as discriminative results as the Swedish and UK samples. A possible explanation could be that the proportion of IT professionals is higher in the Italian sample. That is, however, contradicted by the data showing that IT proficiency has little or no impact on the results. Therefore, a more likely explanation is that Italians are more diverse with respect to SETA delivery preferences.

While our study does not go beyond identifying differences between the three national samples, it does demonstrate that cybersecurity training is perceived differently in different cultures, even in an intra-European context. A natural implication of this insight is that any SETA program seeking to maximize user acceptance should account for cultural factors. Understanding the users' preferences where the program is to be applied and tailoring it accordingly will likely increase user acceptance and effectiveness.

A further factor considered in the survey was if IT professionals perceive cybersecurity training differently than regular users. This factor was explored by removing responses from IT professionals from the sample and comparing those results to the results of all participants. Our study could not identify any difference between IT professionals and regular users. As such, the study suggests that the effect of IT proficiency may be subordinate to other demographic factors in the domain of cybersecurity training, such as the nation of residence, as demonstrated in our study.

The second objective was to develop a taxonomy of SETA methods. This objective was met using a structured literature review which included the databases Web of Science, Scopus, and Science Direct. Seventy-six papers where SETA methods were discussed were identified and analyzed, and the identified SETA methods were categorized, resulting in the list of SETA
methods presented in Table 12. The different SETA methods were further described in the previous section.

The third objective of our research was to evaluate how existing SETA methods respond to user preferences for SETA delivery. This objective was met by analyzing the identified SETA methods in relation to the survey results. The overview of SETA methods revealed great flexibility in how various SETA methods could be delivered. For instance, E-learning can be in almost any medium and delivered using e-mail, word of mouth, or in various other ways. As a result, it is difficult to determine how well a SETA method matches user preferences since that depends highly on its implementation. Consequently, the discussion was held from the perspective of the SETA method's ability to meet the identified preferences. It can be seen as both an evaluation and recommendations for implementing the different methods. On that topic, it is noticeable that SETA methods that are more flexible and require less effort from the user are generally perceived as more positive. It is reasonable to conclude that users will perceive SETA programs as more positive if they are easy to consume and do not require much time.

Limitations and future work

Human aspects of cybersecurity, of which end-user training is a sub-domain, is a complex matter influenced by multiple factors such as cultural factors, gender, age, and more (Abbasi, Zahedi, & Chen, 2016; Butler & Butler, 2018; Hashim & Mahamad, 2017). Our study only examines the impact of cultural background on cybersecurity training preferences, and other sociodemographic aspects are not accounted for. Furthermore, the cultural background can be interpreted in different ways and at different levels. Our paper considers the cultural background equal to the nation of residence, presenting possible limitations. One such limitation is that it does not account for how immigration may impact the culture of a nation or how immigrants may respond to the survey performed, causing possible sampling errors.
The selected approach was chosen since it was considered practically feasible. The risk of sampling errors, while acknowledged, was not considered likely to have any high impact on the results. Another limitation in this regard is how the study defines cultural background. Culture can be considered to include social-economic status, organizational culture, or more and is a complex matter in itself (Hofstede, Hofstede, & Minkov, 2005; Spencer-Oatey & Franklin, 2012). Our study does not attempt to debate what culture is, and the used definition was chosen for sampling purposes. Nevertheless, the results should be interpreted in the light of culture being considered nation of residence. A direction for future work could be to assess cultural differences as organizational or regional cultures.

A second constraint of the study regards how user preferences were measured. Four aspects of cybersecurity training were established, and user preferences in each of those were analyzed. Using a survey methodology, a list of answer options was developed, and this approach inherently includes a risk of not providing the respondents with an exhaustive list. The study aimed to include aspects and answer alternatives that reflected the range of possibilities in how things can be done in an attempt to allow the participants to choose the options best aligning with their views. Literature was consulted to identify reasonable aspects and options. Free-text fields were added to all questions to capture the respondents' ideas that the participants could not express with the pre-decided alternatives. Nothing in the provided free-text answers suggested that the aspects or options were narrow or incomplete, suggesting a high degree of internal validity in the survey. Further, participants were asked to pick their two most preferred choices rather than evaluating each choice individually. The result is nonparametric data where it is hard to quantify how much one option is preferred over another. For instance, the results show that only 17.7% of the respondents picked audio-based training as their preferred option, while 66% picked textual training. While more participants surely preferred textual training, the results do not reveal that effect's size. On a similar note,
the difference in sample sizes may also introduce limitations. The study was designed with one larger sample of 800 respondents and two smaller or 300 participants each. As demonstrated by the reported confidence intervals, the precision of the measurements in the smaller samples is lower than the precision in the larger sample. However, we argue that all sample sizes are large enough to provide reliable results and that the statistical approach and description thereof counteract this potential validity concern.

Further, the included SETA methods were identified using an SLR methodology. An inherent risk of an SLR methodology is not finding all possible articles of relevance. Our research used three scientific databases, employed a wide search string, and did not exclude articles based on publication year. That approach is argued to minimize the risk of not finding important material. Further, given that the purpose of the SLR was to identify SETA methods rather than to assess all research on the matter fully, we argue that the results of the SLR fit the purpose of our research even if some articles on the subject may not be included in it. A limitation specifically related to qualitative SLR is that difficulties arise when conflicting findings are uncovered (Petter, DeLone, & McLean, 2008). The impact of that limitation in our study is argued to be limited since the nature of the SLR is descriptive and aimed to capture how different SETA methods could work rather than to analyze which of them is best. On the topic of the SLR, it should also be mentioned that the resultant taxonomy is a result of the research interpretation of the included publications. The taxonomy presented in our research reflects one way of categorizing SETA, and owning to the flexible nature of many SETA methods, other classifications are perhaps possible. One example could be that our research differentiates between gamified SETA methods and game contests while those could be in the same category.

The nature of our study is that it is a study analyzing user perceptions of SETA methods. As demonstrated in the literature, cybersecurity training can be measured in different ways and
with different purposes. While one example is measuring user perceptions (Jin, Tu, Kim, Heffron, & White, 2018), other ways include measuring the knowledge gained by the user (Taneski, Hericko, & Brumen, 2015) or actual behavioral change (Kävrestad & Nohlberg, 2020). While any training intervention aims to achieve behavioral change, measuring that is complicated. However, user perception is a precursor to adoption and deserves research attention (Agarwal & Prasad, 1998; Shin, Lee, Shin, & Lee, 2010). Our study is to be positioned as a perception study. The effect various SETA methods may have on cybersecurity behavior is outside of its scope and a potential direction for future work.

**CONCLUSIONS**

Our research aimed to *Identify existing methods for SETA and evaluate to what extent those methods meet user preferences regarding the delivery of SETA.* In doing so, our paper makes several contributions to the researcher and practitioner communities.

**Practical contributions**

Our research contributes to the practitioner community in two ways. First, the results showcase how users prefer to have SETA delivered. That can serve as a guideline for practitioners implementing SETA programs or for decision-makers seeking to procure or implement SETA programs in their organization. On that note, the results of our paper highlight that users prefer to have SETA presented in flexible and easy-to-digest ways, preferably in situations where the training is of direct relevance. The results also show that SETA methods are flexible in how they can be implemented and can serve as a guideline for implementing SETA methods to maximize user appreciation.

Second, the results presented in our paper emphasize that user perception of SETA programs is dependent on the user’s cultural background. While the cultural background is, in our paper, discussed as the nation of residence, it can be assumed that organizational cultural
differences also affect the perception of SETA. Examining the user preferences within the own organization to ensure that the organization implements a SETA option that aligns with the perceptions of the own users is recommended. Our paper contributes to the practitioner with a methodology that can be used to survey the user preferences in the own organization and evaluate what SETA method would be most positively perceived in the organization.

Research contributions

Our paper reports on research into user preferences of SETA methods and, in doing so, contributes to the research community in several ways. The core contribution of our study is increased knowledge of user preferences regarding SETA delivery, where the study shows that users prefer SETA programs to be voluntary and flexible. The study shows that users are generally interested in receiving training and prefer to have a system deliver it when they need it or access it on demand. Further, the study suggests that users want to get only the most important information presented to them digitally rather than in face-to-face sessions. On an abstracted level, this suggests that users are interested in security to the degree that they want to know what to do and how, but they do not want to spend a lot of effort on the matter. This notion aligns well with previous research showcasing that security is often not a top priority for users (Caulfield et al., 2019; Sombatruang et al., 2019). Therefore, the second contribution of our paper is that it highlights the notion that security is not the most important matter for users, and future cybersecurity research that affects end-users should be performed with that notion in mind.

The third contribution is that the study emphasizes that perception of and preferences regarding cybersecurity training differs based on cultural factors. This is a factor that should be considered in future research in cybersecurity training. However, our study could not identify any difference between IT professionals and regular users. As such, the study suggests that the effect of IT proficiency may be subordinate to other demographic factors in
the domain of cybersecurity training, such as the nation of residence, as demonstrated in our study.

Finally, our study provides an overview of SETA methods discussed in scientific literature as a fourth contribution. Eleven different methods for SETA, published in 76 articles, are presented and analyzed, making our paper, to the best of our knowledge, the most comprehensive taxonomy of SETA methods, describing how different SETA methods can be delivered, available in scientific literature.

REFERENCES


## Appendix A – Example of coding of one included paper

<table>
<thead>
<tr>
<th>Paper</th>
<th>Method</th>
<th>How</th>
<th>When</th>
<th>Level</th>
<th>Medium</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aldawood &amp; Skinner, 2019</td>
<td>OOB simulation</td>
<td>Digital</td>
<td>On-demand or scheduled time</td>
<td>Interactive</td>
<td>Learners experience simulated attacks in a safe environment</td>
<td></td>
</tr>
<tr>
<td>Aldawood &amp; Skinner, 2019</td>
<td>Attack simulations</td>
<td>Digital</td>
<td></td>
<td></td>
<td>Learners experience simulated attacks in the real environment, with or without the learners' knowledge.</td>
<td></td>
</tr>
<tr>
<td>Aldawood &amp; Skinner, 2019</td>
<td>E-Learning</td>
<td>Digital</td>
<td>On-demand</td>
<td>Extensive</td>
<td>Video or text</td>
<td>Describes videos and governing documents that employees can access on-demand</td>
</tr>
<tr>
<td>Aldawood &amp; Skinner, 2019</td>
<td>Instructor-led</td>
<td>Physical</td>
<td>Scheduled time</td>
<td>Extensive</td>
<td></td>
<td>Describes training in seminar or conference forms</td>
</tr>
<tr>
<td>Aldawood &amp; Skinner, 2019</td>
<td>Gamified</td>
<td>Digital</td>
<td>On-demand</td>
<td>Leaning towards extensive</td>
<td></td>
<td>Games where learners encounter scenarios</td>
</tr>
<tr>
<td>Aldawood &amp; Skinner, 2019</td>
<td>Campaigns</td>
<td>Physical</td>
<td>Brief</td>
<td>Text</td>
<td>Describes infographics and similar with basic information</td>
<td></td>
</tr>
</tbody>
</table>
### Appendix B – Example of coding for one SETA method

<table>
<thead>
<tr>
<th>Paper</th>
<th>Method</th>
<th>How</th>
<th>When</th>
<th>Level</th>
<th>Medium</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aldawood &amp; Skinner, 2019</td>
<td>Campaigns</td>
<td>Physical</td>
<td>Brief</td>
<td>Text</td>
<td></td>
<td>Describes infographics and similar with basic information</td>
</tr>
<tr>
<td>Cox et al., 2001</td>
<td>Campaigns</td>
<td>Physical</td>
<td>Continuous</td>
<td>Brief</td>
<td>Text</td>
<td>Describes a short “security checklist” to be circulated among users in an unspecified way.</td>
</tr>
<tr>
<td>Eminağaoğlu et al., 2009</td>
<td>Campaigns</td>
<td>Physical</td>
<td>Continuous</td>
<td>Brief</td>
<td>Text</td>
<td>Describes posted with slogans and graphics</td>
</tr>
<tr>
<td>Mashiane et al., 2019</td>
<td>Campaigns</td>
<td>Physical</td>
<td>Continuous</td>
<td>Brief</td>
<td>Text</td>
<td>Describes posters with short messages</td>
</tr>
</tbody>
</table>
## Appendix C – Survey questions and answer options

<table>
<thead>
<tr>
<th>Item</th>
<th>Options</th>
<th>Sources</th>
</tr>
</thead>
</table>
| Select how you would prefer to receive information security training/education | In physical lectures/presentations that I attend at a specific time (O1)  
In recorded lectures/presentation delivered to me via e-mail (O2)  
In written text delivered to me digitally (O3)  
In short sequences presented in a context where they are relevant, e.g., password tips when I am creating a password (O4)  
In short sequences sent to me at regular intervals (O5) | Reinheimer et al. (2020). Kävrestad, Skärgård, and Nohlberg (2019). |
| Select when you would prefer to receive information security training/education | I want it at a scheduled time (e.g. a planned session) (O1)  
I want it on-demand (O2)  
I want a system to detect when I need it and present it then (O3)  
I want it to be delivered to me at regular intervals (O4) | Reinheimer et al. (2020). Kävrestad, Skärgård, and Nohlberg (2019). |
| Select if you would be most likely to listen to, and make use of, password tips given to you | When you are about to create a password (O1)  
When you are at work reading your e-mail (O2)  
When you are at home (O3)  
At work as part of an employee day or similar (O4) | Reinheimer et al. (2020). He & Zhang (2019). |
| Select what level of information you prefer                          | I want to receive the most important bullets and options for more and deeper information (O1)  
I want to receive only the most important bullets (O2)  
I do not want any security related information (O3)  
I want to receive all information on a subject (O4) | Hu et al. (2021). |
| Select in what mediums you prefer to access                         | Written text (O1)  
Video (O2)  
Audio (O3) | Reeves, Calic, & Delfabbro (2021). Tschakert and Ngamsuriyaroj. Gjertsen, |
<table>
<thead>
<tr>
<th>information security training</th>
<th>Interactive Video/Game (O4)</th>
<th>Gjære, Bartnes, &amp; Flores (2017).</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Face to Face (e.g. Lecture or one-on-one) (O5)</td>
<td></td>
</tr>
</tbody>
</table>
PAPER 11: WHAT PARTS OF USABLE SECURITY ARE MOST IMPORTANT TO USERS?

What Parts of Usable Security Are Most Important to Users?

Joakim Kävrestad, Steven Furnell, and Marcus Nohlberg

1 University of Skövde, Skövde, Sweden
{joakim.kavrestad,marcus.nohlberg}@his.se
2 University of Nottingham, Nottingham, UK
steven.furnell@nottingham.ac.uk

Abstract. The importance of the human aspects of cybersecurity cannot be overstated in light of the many cybersecurity incidents stemming from insecure user behavior. Users are supposed to engage in secure behavior by use of security features or procedures but those struggle to get widespread use and one hindering factor is usability. While several previous papers studied various usability factors in the cybersecurity domain, a common understanding of usable security is missing. Further, usability covers a large range of aspects and understanding what aspects users prioritize is integral for development of truly usable security features. This paper builds on previous work and investigates what usability factors users prioritize and what demographic factors that affects the perception of usability factors. This is done through a survey answered by 1452 respondents from Sweden, Italy and UK. The results show that users prefer security functions to minimize resource consumption in terms of cost, device performance and time. The study further demonstrate that users want security functions to require as little effort as possible and just work. Further, the study determines that nation of residence and IT-competence greatly impacts the perception of usability for security functions while gender and age does so to a much lesser extent.

Keywords: Usability · Usable security · Cyber security · Human · User · Perception

1 Introduction

Cybersecurity is a property that is undeniably integral to modern individuals, organisations, and even nations [1, 2]. Much like [3], we consider cybersecurity to be a socio-technical property and a high level of security can only be achieved if social as well as technical factors are considered [4]. The importance of the social, or human, side of security is widely acknowledged by researchers as well as practitioners [5, 6]. Several recent industry reports even suggest that the human element is a part of most cybersecurity incidents, further emphasizing its importance [7, 8]. On this note, a preferable scenario is that users increase their security
level through use of security functions such as e-mail encryption or multi-factor authentication, and security practices such as good password creation and management strategies [9–12]. However, while such practices have been on the market for several decades, they are not in widespread use. As demonstrated in several previous papers, the (perhaps perceived) lack of usability seems to be a big part of the answer to why [13–15].

While the primary task of a security function is to provide security, functions designed to be used by end-users cannot do so unless they are adopted by users, and correctly used. Incorrect use can lead to a false sense of security or even be harmful [9]. For instance, password managers are considered a good way to use unique passwords for various accounts while only having to remember one master password. However, if that password is compromised, all accounts related to it are also compromised [16]. The consequence of security functions or practices not being adopted is obvious, the security they intend to provide is not provided. This is what often happens to so-called secure password guidelines which prompt users to use long and complex passwords. Many users are unwilling to follow this guideline and select insecure passwords instead [17]. There are several theories that can be used to explain how users choose to adopt security functions and procedures. Three theories commonly used in cybersecurity can be briefly described as follows:

- Protection Motivation Theory (PMT) where [18] describe that peoples decision to protect themselves against a supposed threat are influenced by how severe and likely the person perceives the threat, how effective a preventative measure is, and the persons perceived ability to engage in that measure.
- Theory of Planned Behaviour (TPB) which highlights that actual behaviour is influenced by a persons perception of how easy or difficult a certain behaviour is [19].
- Technology Acceptance Model (TAM) which in its original form describe that a users decision to adopt a technology is based on how useful she perceives the technology to be, and how easy she perceives it to be to use the technology [20,21].

Applied to the cybersecurity domain, PMT, TPB, and TAM demonstrate that usability is precurser to user adoption of security functions and practices. User adoption, in turn, is an obvious precursor to whatever security a function or practice is intended to add. As such, usability is a crucial aspect to research in relation to end-user security. While there has been a fair bit of research conducted on usability of security functions, a fundamental issue seems to be that there is no common understanding of what usability means to the cybersecurity community. This is demonstrated how various previous papers consider usability of security functions in vastly different ways. To exemplify, [22] evaluates a subset of usability criteria in the context of phishing, and [23] discusses usability in the context of IoT access control without further describing what usability in that context entails. Further, the System Usability Scale (SUS), presented by [24] as been adopted in the cybersecurity domain by, for instance, [25]. While SUS measures important aspects of usability it does not factor in all aspects that are
considered important in the cybersecurity domain, for instance risk associated with incorrect use [9].

A recent literature review [26] summarizes how usable security has been discussed in 70 scientific publication from 2015 to 2020. [26] presents 31 aspects of how usability has been studied in the cybersecurity domain, and groups those into 14 themes. Our study seeks to expand on the work conducted by [26] by exploring which of those aspects that are considered the most important by users. The study was performed as a survey reaching more than 1400 respondents and provides insight into what usability features that users perceive as most important. It also investigates how the perception of usability features is impacted by various demographic variables. As such, it provides insight that can support practitioners towards development of usable security functions and procedures. The study further provides the research community with a better understanding of what users considers to be the most important usability aspects, and how demographic aspects impact the perception of usable security.

The rest of this paper is structured as follows; Sect. 2 describes the methodological approach, Sect. 3 presents and analyses the results which are further discussed in Sect. 4 before the paper is concluded, and directions for future work are presented in Sect. 5.

2 Methodology

With the purpose of collecting quantitative data from a large sample of respondents, a web-based survey was used. The survey panel company Webropol was hired for the distribution of the survey and while this approach restricted the range of possible participants to the members of Webropol’s panel, it is a practically feasible method to achieve a sample of high quality [27]. It also minimizes demographic bias, and accidental sampling bias common when distributing web based surveys using, for instance, social media [28]. A stratified sampling approach was used to generate a probability sample [29]. The panel members were split into strata based on gender, age, and geographical region. Equal proportions from each strata were then recruited using simple random sampling [30]. The primary target of the survey was Swedish users, and the target sample size for Swedes was set to 800 respondents. With the goal of comparing the results to users from other European nations, samples with a target size of 300 respondents were drawn from UK and Italy. UK and Italy was chosen since they, according to [31], belong to different culture groups than Sweden.

The survey was part of a larger survey and, for the purpose of this paper, contained demographic questions describing the respondents perceived gender, IT-competence and age. The participants were then asked to pick the five most and least important usability aspects from a list of 21 aspects derived from [26]. The original list by [26] included 31 aspects. However, the surveys development and testing phase revealed that several of those were too similar, or could be perceived in different ways by the respondents. They were therefore combined and/or reworded to ensure that the list of options was easy for the respondents to
understand. For instance, [26] describe compatibility with systems and services, and compatibility with other security solutions as two separate usability aspects. In this study, they were combined into one answer option stating *It should work with all sites and services I use so that I only need one tool of each type*. Further, [26] describes several types of interference to the users workflow and those were combined to one statement expressed as *It should not interfere with the way I work*. The complete list of aspects is presented along with the results to save space, and appeared to the participants in randomized order to minimize responder bias. Both questions were followed by a free-text field where the respondents could add additional comments. Before the survey was distributed, it was taken through a pilot procedure in three steps:

1. A small sample was recruited using social media, and those respondents were specifically asked to provide feedback on the structure and readability of the survey.
2. Two respondents were asked to fill out the survey under personal supervision from a researcher, they were also asked to continuously express their thoughts while filling it out.
3. The survey was distributed to a sample of peers who were asked to assess it in relation to the research aim.

For data analysis, the percentage of respondents picking each aspect was first reported and a maximum 95% confidence interval computed as suggested by [32]. Next, the impact of various demographic factors was investigated by testing how the distribution of answers was impacted when the results of the full sample was divided based on nation, gender, IT-proficiency and age, respectively.

The statistical analysis was performed using chi-square because of the non-parametric nature of the collected data [33], and formally measured if the distribution of data points within a demographic group differed from an expected distribution with statistical significance. The conventional significance level of 95% was adopted in this study. Note that, while data is presented as percentages throughout this study, frequencies in absolute numbers was used for the chi-square tests.

### 3 Results and Analysis

Webropol distributed the survey to a sample of 10 times the target sample size and the survey was open for one week. A total of 1452 respondents completed the survey, and were distributed over the national answer groups as follows:

- Sweden: 834 participants
- Italy: 314 participants
- UK: 304 participants.

The respondents were rather evenly divided based on gender and spread through various age groups as shown in Table 1. However, reported level of IT-competence differed between the groups, with Italian respondents reporting to be more IT-competent, on average.
Table 1. Demographic overview (in percent)

<table>
<thead>
<tr>
<th>Gender</th>
<th>Sweden</th>
<th>UK</th>
<th>Italy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Female</td>
<td>45.6</td>
<td>53.3</td>
<td>43.9</td>
</tr>
<tr>
<td>Male</td>
<td>54.2</td>
<td>46.7</td>
<td>55.7</td>
</tr>
<tr>
<td>Other/Prefer not to say</td>
<td>0.3</td>
<td>0</td>
<td>0.2</td>
</tr>
<tr>
<td>Age</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18–25</td>
<td>8.3</td>
<td>1.0</td>
<td>4.1</td>
</tr>
<tr>
<td>26–35</td>
<td>20.3</td>
<td>18.1</td>
<td>21.3</td>
</tr>
<tr>
<td>36–45</td>
<td>18.8</td>
<td>25.7</td>
<td>31.2</td>
</tr>
<tr>
<td>46–55</td>
<td>23.9</td>
<td>18.1</td>
<td>20.7</td>
</tr>
<tr>
<td>56–65</td>
<td>15.3</td>
<td>21.4</td>
<td>15.3</td>
</tr>
<tr>
<td>66–75</td>
<td>13.3</td>
<td>15.5</td>
<td>7.3</td>
</tr>
<tr>
<td>Above 76</td>
<td>0.1</td>
<td>0.3</td>
<td>0</td>
</tr>
<tr>
<td>IT-Competence</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Professional - working in, Hold a degree in or study IT</td>
<td>9.4</td>
<td>9.9</td>
<td>22.3</td>
</tr>
<tr>
<td>Expert user - Interested user that know my way around IT. Usually asked to help people with home routers, printer installations etc.</td>
<td>22.3</td>
<td>19.4</td>
<td>27.7</td>
</tr>
<tr>
<td>Average user - I use IT with no major problems but need help occasionally</td>
<td>65.1</td>
<td>64.1</td>
<td>38.5</td>
</tr>
<tr>
<td>Below average - I have a hard time using IT and feel like I need help with tasks that others do with ease</td>
<td>3.2</td>
<td>6.6</td>
<td>11.5</td>
</tr>
</tbody>
</table>

The respondents were then provided with the following information before they were asked to rate what five usability aspects they perceived as most and least important.

This part of the survey concerns what properties a security tool or functions should possess for you to use it. We want you to select the five most and the five least important properties from a list of 21 properties. A security tool or function includes anything designed to improve your level of IT-security and that you can choose to use. Some examples are:

- Password creation guidelines (suggestion for password length, complexity, etc.)
- Encryption software, for instance, e-mail encryption tools used to encrypt e-mails or data encryption tools used to encrypt your computer
- Browsing filters that warn you if you are visiting a web site that can be fraudulent
- Malware (eg Viruses and Ransomware) protection software.

We want to know which of the following properties you consider to be the most important and the least important. The first question will ask you to check the five most important properties and the second will ask you to check the five properties you think is least important.
All questions are followed by a text-box where you can input additional comments.

The available options and the percentage of respondents choosing each option is displayed in Table 2, sorted in order of preference according to the complete data-set.

Table 2. Percentage of participants picking the respective options as the most important.

<table>
<thead>
<tr>
<th>Option</th>
<th>Sweden</th>
<th>UK</th>
<th>Italy</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>It should not be costly</td>
<td>41.5</td>
<td>50.3</td>
<td>44.0</td>
<td>43.7</td>
</tr>
<tr>
<td>It should be easy to understand and navigate the interface</td>
<td>42.6</td>
<td>42.8</td>
<td>32.8</td>
<td>40.5</td>
</tr>
<tr>
<td>It should not impact the performance of my device</td>
<td>42.5</td>
<td>46.7</td>
<td>30.3</td>
<td>40.2</td>
</tr>
<tr>
<td>It should not take a lot of time to use</td>
<td>41.0</td>
<td>32.6</td>
<td>35.4</td>
<td>38.0</td>
</tr>
<tr>
<td>Information about how to use it should be easy to find and understand</td>
<td>36.3</td>
<td>32.2</td>
<td>32.2</td>
<td>34.6</td>
</tr>
<tr>
<td>It should work with all sites and services I use so that I only need one tool of each type</td>
<td>37.4</td>
<td>31.0</td>
<td>20.4</td>
<td>32.3</td>
</tr>
<tr>
<td>It should not interfere with the way I work</td>
<td>31.5</td>
<td>30.9</td>
<td>24.2</td>
<td>29.9</td>
</tr>
<tr>
<td>It should require as little interaction from me as possible</td>
<td>33.3</td>
<td>27.6</td>
<td>21.0</td>
<td>29.5</td>
</tr>
<tr>
<td>I should not need to learn how to configure or manage it, and default configuration should be safe to use</td>
<td>30.7</td>
<td>24.3</td>
<td>22.3</td>
<td>27.6</td>
</tr>
<tr>
<td>It should not take a lot of time to install</td>
<td>25.2</td>
<td>28.6</td>
<td>27.4</td>
<td>26.4</td>
</tr>
<tr>
<td>When I need to make a decision, the tool should provide information about the different options</td>
<td>20.0</td>
<td>20.7</td>
<td>27.7</td>
<td>21.8</td>
</tr>
<tr>
<td>It should not put me under time pressure</td>
<td>20.4</td>
<td>19.1</td>
<td>20.4</td>
<td>21.1</td>
</tr>
<tr>
<td>It should be developed by, or recommended by someone I trust</td>
<td>20.0</td>
<td>19.4</td>
<td>19.1</td>
<td>19.7</td>
</tr>
<tr>
<td>Benefits and effects of using different security options should be clearly presented</td>
<td>14.0</td>
<td>15.8</td>
<td>29.9</td>
<td>17.8</td>
</tr>
<tr>
<td>The tool should provide feedback such as progress updates, system status etc.</td>
<td>15.4</td>
<td>16.5</td>
<td>16.2</td>
<td>15.8</td>
</tr>
<tr>
<td>It should allow me to customize the configuration to my liking and adapt it to my skill level</td>
<td>13.2</td>
<td>14.1</td>
<td>21.7</td>
<td>15.2</td>
</tr>
<tr>
<td>I should be able to adjust the interface to my preference</td>
<td>11.3</td>
<td>14.5</td>
<td>25.16</td>
<td>14.9</td>
</tr>
<tr>
<td>It should be predictable; similar tasks should work in the same way and it should be easy to recognize requirements and conditions during setup</td>
<td>14.2</td>
<td>13.5</td>
<td>16.9</td>
<td>14.6</td>
</tr>
<tr>
<td>It should be possible to handle accounts for different users</td>
<td>8.2</td>
<td>14.5</td>
<td>20.7</td>
<td>12.2</td>
</tr>
<tr>
<td>It should be perceived as cool by others</td>
<td>2.6</td>
<td>4.9</td>
<td>12.4</td>
<td>5.2</td>
</tr>
<tr>
<td>Maximum 95% CI</td>
<td>3.3</td>
<td>5.6</td>
<td>5.4</td>
<td>2.6</td>
</tr>
</tbody>
</table>

As seen in the Table 2, a general tendency is that the respondents favour aspects that minimize cost and resource consumption as well as ease of use. The preferred ease of use properties can be summarized as properties where interaction and time consumed using the security function is minimized. On the other hand, properties speaking to customizability are less favoured. National differences can be observed for several properties, and those will be further explored below.
The results for the second question, asking the respondents to pick the five properties they perceived as least important, are presented in Table 3. It is sorted in order of preference according to the complete data set.

Table 3. Percentage of participants picking the respective options as the least important.

<table>
<thead>
<tr>
<th>Option</th>
<th>Sweden</th>
<th>UK</th>
<th>Italy</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>It should be perceived as cool by others</td>
<td>79.6</td>
<td>66.8</td>
<td>39.8</td>
<td>68.3</td>
</tr>
<tr>
<td>It should be possible to handle accounts for different users</td>
<td>48.8</td>
<td>38.8</td>
<td>25.5</td>
<td>41.7</td>
</tr>
<tr>
<td>I should be able to adjust the interface to my preference</td>
<td>36.1</td>
<td>29.9</td>
<td>28.0</td>
<td>33.6</td>
</tr>
<tr>
<td>It should allow me to customize the configuration to my liking and adapt it to my skill level</td>
<td>36.9</td>
<td>30.6</td>
<td>22.6</td>
<td>32.5</td>
</tr>
<tr>
<td>It should be developed by, or recommended by someone I trust</td>
<td>31.4</td>
<td>29.0</td>
<td>32.8</td>
<td>31.2</td>
</tr>
<tr>
<td>The tool should provide feedback such as progress updates, system status etc.</td>
<td>33.6</td>
<td>28.0</td>
<td>26.1</td>
<td>30.8</td>
</tr>
<tr>
<td>It should not take a lot of time to install</td>
<td>31.1</td>
<td>22.0</td>
<td>27.4</td>
<td>28.4</td>
</tr>
<tr>
<td>It should not put me under time pressure</td>
<td>24.2</td>
<td>29.3</td>
<td>31.5</td>
<td>26.9</td>
</tr>
<tr>
<td>When I need to make a decision, the tool should provide information about the different options</td>
<td>19.8</td>
<td>30.3</td>
<td>27.7</td>
<td>23.7</td>
</tr>
<tr>
<td>Benefits and effects of using different security options should be clearly presented</td>
<td>23.7</td>
<td>19.1</td>
<td>22.3</td>
<td>22.5</td>
</tr>
<tr>
<td>It should be predictable; similar tasks should work in the same way and it should be easy to recognize requirements and conditions during setup</td>
<td>21.1</td>
<td>24.0</td>
<td>23.9</td>
<td>22.3</td>
</tr>
<tr>
<td>It should require as little interaction from me as possible</td>
<td>16.2</td>
<td>22.0</td>
<td>28.7</td>
<td>20.1</td>
</tr>
<tr>
<td>It should not be costly</td>
<td>17.2</td>
<td>18.8</td>
<td>28.0</td>
<td>19.8</td>
</tr>
<tr>
<td>I should not need to learn how to configure or manage it, and default configuration should be safe to use</td>
<td>17.4</td>
<td>22.7</td>
<td>20.4</td>
<td>19.2</td>
</tr>
<tr>
<td>It should work with all sites and services I use so that I only need one tool of each type</td>
<td>13.9</td>
<td>20.1</td>
<td>16.6</td>
<td>15.8</td>
</tr>
<tr>
<td>It should not interfere with the way I work</td>
<td>13.1</td>
<td>15.1</td>
<td>20.7</td>
<td>15.2</td>
</tr>
<tr>
<td>It should not take a lot of time to use</td>
<td>10.0</td>
<td>17.1</td>
<td>21.0</td>
<td>13.8</td>
</tr>
<tr>
<td>It should not impact the performance of my device</td>
<td>10.8</td>
<td>14.8</td>
<td>19.1</td>
<td>13.4</td>
</tr>
<tr>
<td>Information about how to use it should be easy to find and understand</td>
<td>8.2</td>
<td>11.8</td>
<td>19.4</td>
<td>11.4</td>
</tr>
<tr>
<td>It should be easy to understand and navigate the interface</td>
<td>7.1</td>
<td>9.9</td>
<td>18.5</td>
<td>10.1</td>
</tr>
<tr>
<td>Maximum 95% CI</td>
<td>2.7</td>
<td>5.3</td>
<td>5.4</td>
<td>2.4</td>
</tr>
</tbody>
</table>

As seen in Table 3, the least preferred options follow the same line as the most preferred option. Customizability options are in this case selected over options speaking to ease of use and limited need for interaction. Further, Tables 2 and 3 suggest that the participants do not care about how cool the functions are perceived by others and are not interested in spending time and money on security features and functions.
The next part of the analysis investigated how the results are impacted by
the examined demographics aspects; nation, perceived gender, perceived IT-
competence and age. Chi-square was used to measure if the distribution of data
points within a demographic group differed from an expected distribution, given
the complete data set. The analysis first measured the effect of each individual
demographic on each data point. The analysis then measured the effect of gen-
der, age and IT-competence within each national answer group. As such, 168
tests were performed and, given the permitted space, not presented in detail. To
exemplify, the first test measured the impact of nation on the option *It should
not be costly* for the question *most*. Key statistics are presented in Table 4.

**Table 4.** Example of statistical analysis using chi-square and the option *It should not be costly* for the question *most*

<table>
<thead>
<tr>
<th>Answer</th>
<th>Sweden</th>
<th>UK</th>
<th>Italy</th>
<th>Chi-square</th>
<th>Sig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes - Observed</td>
<td>344</td>
<td>153</td>
<td>138</td>
<td>7.475</td>
<td>0.024</td>
</tr>
<tr>
<td>Yes - Expected</td>
<td>364.7</td>
<td>132.9</td>
<td>137.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No - Observed</td>
<td>490</td>
<td>151</td>
<td>176</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No - Expected</td>
<td>469.3</td>
<td>171.1</td>
<td>176.7</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The hypothesis tested in this example is that *Nation impacts the number of respondents who perceive ‘It should not be costly’ as one of the most important usability aspects for security features*. The hypothesis is supported given that the p-value is below 0.05, which is true in this case. Table 5 provides an overview of the demographic aspects that were shown to have a significant impact on what usability aspects respondents rank as most important. Significant tests are marked with an asterisk (*).

As shown by Table 5, demographics do impact what usability aspects respondents perceive as most important and nation of residence and perceived IT-competence are the most prominent demographic aspects while age and gender impacts far fewer of the usability aspects. It could, however, be noted that nation and IT-competence impact the same aspects in nine cases and the sample from Italy is distributed differently than the other sampling groups on the demographic of IT-competence (as seen in Table 1). Thus, it is hard to say if the perception of those aspects is impacted by IT-competence, nation, or both. Table 6 provides an overview of the demographic aspects that were shown to have a significant impact on what usability aspects respondents rank as least important, significant tests are marked with an asterisk (*). While there is some variation between Tables 5 and 6, nation and IT-competence are the demographic factors influencing the perception of most usability aspects. Gender and age, on the other hand, influence below 25% of the aspects.
Table 5. Overview of what demographics that had a significant impact on what usability aspects that were perceived as *most* important, in the complete data set (n = 1452). It is ordered with most frequently picked option in the complete sample on top.

<table>
<thead>
<tr>
<th>Option</th>
<th>Nation</th>
<th>Age</th>
<th>IT-comp.</th>
<th>Gender</th>
</tr>
</thead>
<tbody>
<tr>
<td>It should not be costly</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>It should be easy to understand and navigate the interface</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>It should not impact the performance of my device</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>It should not take a lot of time to use</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information about how to use it should be easy to find and understand</td>
<td></td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>It should work with all sites and services I use so that I only need one tool of each type</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>It should not interfere with the way I work</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>It should require as little interaction from me as possible</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I should not need to learn how to configure or manage it, and default configuration should be safe to use</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>It should not take a lot of time to install</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>When I need to make a decision, the tool should provide information about the different options</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>It should not put me under time pressure</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>It should be developed by, or recommended by someone I trust</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Benefits and effects of using different security options should be clearly presented</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The tool should provide feedback such as progress updates, system status etc.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>It should allow me to customize the configuration to my liking and adapt it to my skill level</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I should be able to adjust the interface to my preference</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>It should be predictable; similar tasks should work in the same way and it should be easy to recognize requirements and conditions during setup</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>It should be possible to handle accounts for different users</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>It should be perceived as cool by others</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 6. Overview of what demographics that had a significant impact on what usability aspects that were perceived as least important, in the complete data set (n = 1452). It is ordered with most frequently picked option in the complete sample on top.

<table>
<thead>
<tr>
<th>Option</th>
<th>Nation</th>
<th>Age</th>
<th>IT-comp.</th>
<th>Gender</th>
</tr>
</thead>
<tbody>
<tr>
<td>It should be perceived as cool by others</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>It should be possible to handle accounts for different users</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>I should be able to adjust the interface to my preference</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>It should allow me to customize the configuration to my liking and adapt it to my skill level</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>It should be developed by, or recommended by someone I trust</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The tool should provide feedback such as progress updates, system status etc.</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>It should not take a lot of time to install</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>It should not put me under time pressure</td>
<td>*</td>
<td></td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>When I need to make a decision, the tool should provide information about the different options</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Benefits and effects of using different security options should be clearly presented</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>It should be predictable; similar tasks should work in the same way and it should be easy to recognize requirements and conditions during setup</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>It should require as little interaction from me as possible</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>It should not be costly</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I should not need to learn how to configure or manage it, and default configuration should be safe to use</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>It should work with all sites and services I use so that I only need one tool of each type</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>It should not interfere with the way I work</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>It should not take a lot of time to use</td>
<td>*</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>It should not impact the performance of my device</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>Information about how to use it should be easy to find and understand</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>It should be easy to understand and navigate the interface</td>
<td>*</td>
<td>*</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4 Discussion

The aim of this study was twofold; the first aim was to analyze what usability aspects that users consider most important for security functions, and the second was to identify demographic aspects which affect how those usability aspects are perceived. The study continued on the work by [26] and derived 21 usability...
aspects from the list of 31 usability aspects presented there. The study was conducted using a web based survey in order to generate a large sample of respondents, and resulted in a data set with survey data from 1452 individual respondents from Sweden, Italy and UK. The survey was carefully developed by the research team and evaluated in a three-step pilot procedure to ensure that is was appropriate for the study aim and easy to understand for respondents.

The first aim was meet by two questions where the respondents were asked to rate the five usability aspects they perceived as most and least important. The intent was to let the two question combined serve as a form of triangulation around the question of what aspects the respondents considered to be most important [34]. The results show that the usability aspects perceived as most important are those reflecting resource minimization and ease of use. The aspects perceived as least important reflect customizability interfaces and behaviour. One respondents commented as follows; “Needs to be free. Runs in the background with no input from me. Should run without impacting on my use of technology”. That quote is a good summary of the study’s results in regards to the first aim. This notion aligns well with previous research suggesting that users just want cybersecurity to work.

The second aim was meet by dividing the dataset based on nation, gender, age and reported IT-competence and analyzing if any of those factors significantly impacted the respondents perception of the usability aspects. Repeated chi-square tests revealed that nation and IT-competence both affected the perception of up to 75% of the included usability factors while age and gender both only impacted about 25%. It should be noted that the distribution of answers to the demographic question about IT-competence is uneven between the national sample groups, and that can impact the results in this case. Still, the results do suggest that nation of residence does impact how users perceive the importance of usability aspects. This notion aligns well with previous research suggesting that both culture and IT-competence are important factors in human aspects of cybersecurity [35]. However, the study also suggest that age and gender does not affect how users prioritize usability aspects of security functions to any large extent, and this is surprising due to previous research suggesting age and gender to be important factors in cybersecurity in general [36–39].

By extending the work by [26], this study contributes to the academic community with increased understanding about what the concept of usable security entails. It does so by providing an analysis of what usability aspects that users consider to be most important and is, to the best of our knowledge, the first publication of that sort. This paper also demonstrate the complex nature of the human aspects of cybersecurity and emphasizes the need for continued research in pursuit of generalizable results that can help the community move towards better cybersecurity behaviour with cost-effective means.

As a contribution to practitioners, the results of this survey insight depicting what security aspects to focus on when implementing security features. Since the results of this survey shed light on what usability features that are prioritized by the most users, it also shows which of those aspects a feature appealing to as
many users as possible should include. Perhaps at least as important, it uncovers which aspects that are perhaps not worthwhile to put efforts into.

5 Conclusions and Future Work

The first part of this study asked the respondents to rank the five most and five least important usability aspects of security functions. The available aspects are presented in Table 2. As a summary, the results suggest that respondents prioritize resource effective security functions. The functions should not be costly, impact device performance, or require a lot of time to use. This notion is emphasized by several free-text comments stating that “it should just be there and work”. The results also show that the respondents want security functions to be easy to use and to understand. As a general rule, usability aspects speaking to more advanced use are found at the bottom of the list of preferred aspects. Those aspects include customizability, ability to handle multiple accounts and existence of feedback from the security features.

The second part of the analysis evaluated if nation, gender, age or IT-competence had an impact on what usability aspects that are most or least preferred. This analysis showed that nation and IT-competence had the most widespread impact with nation impacting the perception of about 75% of the aspects, and IT-competence impacting about 55%. It should here be noted that the answers to the demographic question about IT-competence are unevenly distributed between the national sample groups, and that can impact the results in this case. Finally, age and gender both impacted the perception of less than 25% of the included usability aspects, suggesting that those demographics are not as important when it comes to the perception of usability in relation to security functions.

This paper shows that several demographic aspects can impact the usability aspects that users prioritize for security functions. Given the limitations of space, it was not possible to dwell into the nature of this effect and further analysis of the demographic effect in this, or other, data sets is a natural continuation of this work. Further areas for future work could be to expand on this study by including more demographic aspects such as disabilities or more different nation groups.

References