The Data Base for Advances in Information Systems

A taxonomy of SETA methods and linkage to delivery preferences

Joakim Kävrestad
University of Skövde

Marcus Nohlberg
University of Skövde

Steven Furnell
University of Nottingham

Date of Acceptance: 10/9/2022

Please cite this article as follows:

Kävrestad, J., Nohlberg, M., & Furnell, S. (Forthcoming). A taxonomy of SETA methods and linkage to delivery preferences. *The DATA BASE for Advances in Information Systems*, In Press.

A taxonomy of SETA methods and linkage to delivery preferences

Joakim Kävrestad
University of Skövde

Marcus Nohlberg
University of Skövde

Steven Furnell
University of Nottingham

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 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 problems 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. We show 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, thereby supporting user adoption.

Keywords: Cybersecurity; Security Training; Security Behavior; Security Awareness; User Training.

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-Daeef, 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.

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).

Table 1. Identified Aspects of SETA Delivery

Aspect	Description
How training is delivered	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.
When the user is trained	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
What level of information that is presented	This concerns the detail level of the information the user is provided with
What medium it is presented in	Medium describes the medium the training is in, such as games, video, or plain text.

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:

> Objective 1 (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:

> Objective 2 (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:

> Objective 3 (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.

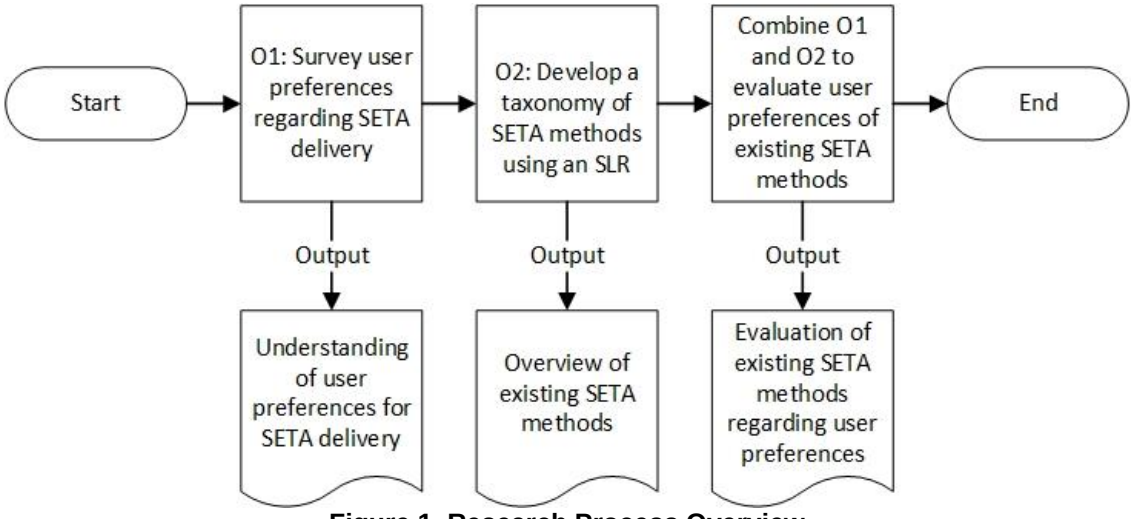

Figure 1. Research Process Overview

Identification of User Preferences Regarding SETA Delivery

A web-based survey was used to research our study's first 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.

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

Table 2. Demographic Overview of Survey Respondents

Variable	Answer	Sweden (n=834)	UK (n=304)	Italy (n=314)	All (n=1452)
Gender	Male	54.2%	46.7%	55.7%	53.0%
	Female	45.6%	53.3%	43.9%	46.8%
	Prefer not to say	0.3%	0%	0.2%	0.2%
Age	18-25	8.3%	1%	4.1%	5.9%
	26-35	20.3%	18.1%	21.3%	20.0%
	36-45	18.8%	15.7%	31.2%	22.9%
	46-55	23.9%	18.1%	20.7%	22.0%
	56-65	15.3%	21.4%	15.3%	16.6%
	66-75	13.3%	15.5%	7.3%	12.5%
	Above 76	0.1%	0.3%	0%	0.1%
IT proficiency	Professional	9.4%	9.9%	22.3%	12.3%
	Expert user	22.3%	19.4%	27.7%	22.9%
	Average user	65.1%	64.1%	38.5%	59.2%
	Below Average	3.2%	6.6%	11.5%	5.7%

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 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 3. Preferences on How to Receive Security Training/Education, Separated by National Sample Groups

Select how you would prefer to receive information security training/education	All (n=1452)	Sweden (N=834)	UK (N=304)	Italy (N=314)
In physical lectures/presentations that I attend at a specific time (O1)	21.0%	18.5%	21.1%	27.7%
In recorded lectures/presentation delivered to me via e-mail (O2)	38.2%	38.2%	34.2%	42.0%
In written text delivered to me digitally (O3)	44.9%	45.4%	43.4%	44.9%
In short sequences presented in a context where they are relevant. e.g., password tips when I am creating a password (O4)	55.0%	60.4%	50.0%	45.2%
In short sequences sent to me at regular intervals (O5)	40.9%	37.4%	51.3%	40.1%
95% Confidence interval	2.6%	3.4%	5.6%	5.5%

Table 4. Preferences on how to Receive Security Training/Education, With Answers from IT Professionals Being Disregarded

Select how you would prefer to receive information security training/education	All (n=1274)	Sweden (N=756)	UK (N=274)	Italy (N=244)
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

Select when you would prefer to receive information security training/education	**All (n=1452)**	**Sweden (N=834)**	**UK (N=304)**	**Italy (N=314)**
I want it at a scheduled time (e.g. a planned session) (O1)	34.8% (35.1%)	30.7% (30.8%)	38.5% (39.8%)	42.0% (43.0%)
I want it on-demand (O2)	56.2% (54.9%)	56.6% (54.9%)	52.3% (51.8%)	58.9% (58.6%)
I want a system to detect when I need it and present it then (O3)	64.4% (65.5%)	70.1% (71.3%)	61.2% (59.9%)	52.2% (54.1%)
I want it to be delivered to me at regular intervals (O4)	44.6% (44.4%)	42.6% (43.0%)	48.0% (48.5%)	46.8% (44.3%)
Maximum 95% CI	2.60%	3.3%	5.6%	5.5%

Table 6. Preferences on When to Receive Security Training/Education

Select if you would be most likely to listen to, and make use of, password tips given to you	**All (n=1452)**	**Sweden (N=834)**	**UK (N=304)**	**Italy (N=314)**
When you are about to create a password (O1)	68.0% (69.2%)	72.7% (73.1%)	68.4% (69.3%)	55.4% (56.6%)
When you are at work reading your e-mail (O2)	43.0% (42.1%)	41.6% (40.9%)	38.5% (37.2%)	51.3% (51.2%)
When you are at home (O3)	48.3% (49.4%)	42.2% (43.9%)	59.5% (60.9%)	53.5% (53.3%)
At work as part of an employee day or similar (O4)	40.6% (39.4%)	43.5% (42.1%)	33.6% (32.5%)	39.8% (38.9%)
Maximum 95% CI	2.60%	3.3%	5.5%	5.5%

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.

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 7. Preferences on Level of Information Received

Select what level of information you prefer	All (n=1452)	Sweden (N=834)	UK (N=304)	Italy (N=314)
I want to receive the most important bullets and options for more and deeper information (O1)	73.2% (73.3%)	77.9% (77.5%)	71.4% (73.0%)	62.4% (60.7%)
I want to receive only the most important bullets (O2)	69.8% (71.3%)	74.9% (75.5%)	65.5% (67.5%)	60.2% (62.3%)
I do not want any security related information (O3)	18.2% (17.9%)	16.5% (16.7%)	19.1% (19.0%)	21.7% (20.5%)
I want to receive all information on a subject (O4)	38.8% (37.5%)	30.6% (30.3%)	44.1% (40.5%)	55.7% (56.6%)
Maximum 95% CI	2.50%	3.1%	5.6%	5.5%

Table 8. Preferences on Medium to Receive Security Training/Education in

Select in what mediums you prefer to access information security training	All (n=1452)	Sweden (N=834)	UK (N=304)	Italy (N=314)
Written text (O1)	66.0% (67.0%)	68.5% (69.8%)	63.8% (64.6%)	61.5% (60.7%)
Video (O2)	57.7% (57.5%)	59.0% (58.2%)	54.6% (55.1%)	57.3% (57.8%)
Audio (O3)	17.7% (17.0%)	12.6% (12.4%)	22.4% (21.9%)	26.8% (25.8%)
Interactive Video/Game (O4)	29.0% (28.7%)	30.6% (29.6%)	25.7% (26.6%)	28.0% (28.3%)
Face to Face (e.g. Lecture or one-on-one) (O5)	29.6% (29.8%)	29.4% (29.9%)	33.6% (31.8%)	26.4% (27.5%)
Maximum 95% CI	2.50%	3.3%	5.6%	5.5%

Table 9. Summary of Survey Results

Aspect	Summary
How training is delivered	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.
When the user is trained	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.
What **level of information** that is presented	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.
What medium it is presented in	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.

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.

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 second 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.

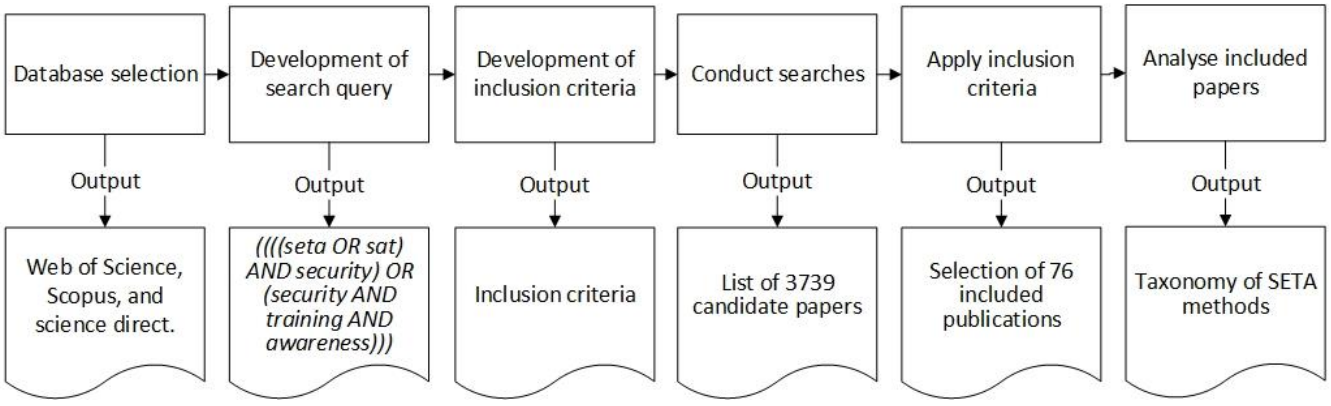

Figure 2. Overview of SLR Process

Table 10. SLR Inclusion Criteria

Inclusion criteria	Justification
Published in a peer-reviewed conference or journal	Ensures quality of included papers
Written in English	Ensures that included papers can be understood by the researchers
Not a duplication of another included paper	Ensures that publications are only included once
Describes SETA methods intended for end-users	Limits the review's scope to publications describing SETA methods rather than just presenting or mentioning it
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	

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.
    a. If the SETA method was not previously identified, it was added as a new method.
    b. If the SETA method was previously identified, the paper was connected to that SETA method.
    c. 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 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.

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.

Table 11. Identified SETA Methods and Papers They Appear in

Method	Sources
Out-of-bands simulation	(Aldawood & Skinner, 2019; Burris, Deneke, & Maulding, 2018; Ntokas, Maratou, & Xenos, 2015; Yamin, Katt, & Gkioulos, 2020)
Attack simulations	(Aldawood & Skinner, 2019; Alwanain, 2020; Bakar, Mohd, & Sulaiman, 2018; Caputo, Pfleeger, Freeman, & Johnson, 2014; Carella, Kotsoev, & Truta, 2017; Dodge Jr, Carver, & Ferguson, 2007; Dodge & Ferguson, 2006; Higashino, Kawato, Ohmori, & Kawamura, 2019; Jansson & von Solms, 2013; Lee et al., 2019; Pirocca, Allodi, & Zannone, 2020; Styles & Tryfonas, 2009)
E-learning	(Abawajy, 2014; Aldawood & Skinner, 2019; Arain, Tarraf, & Ahmad, 2019; Charoen, Raman, & Olfman, 2008; Cooper, 2008; Cox, Connolly, & Currall, 2001; Dlamini & Modise, 2012; Dukarm, Dill, & Reith, 2019; Eminağaoğlu, Uçar, & Eren, 2009; Figueroa & Ayyagari, 2015; Furnell, Warren, & Dowland, 2003; Goluch et al., 2007; Gundu & Flowerday, 2013; Hagen & Albrechtsen, 2009; Hansche, 2001; He et al., 2020; Hepp, Tarraf, Birney, & Arain, 2018; Jenkins & Durcikova, 2013; Jensen, Dinger, Wright, & Thatcher, 2017; Labuschagne & Eloff, 2012; Mashiane, Dlamini, & Mahlangu, 2019; McCoy & Fowler, 2004; Oroszi, 2019; Power & Forte, 2006; Schürmann, Jensen, & Sigbjörnsdóttir, 2020; Shaw, Chen, Harris, & Huang, 2009; Shaw, Keh, Huang, & Huang, 2011; Smith, Mediavilla, & White, 2018; Tschakert & Ngamsuriyaroj, 2019; Younis & Musbah, 2020)
Interactive E-learning	(Alkhamis & Renaud, 2016; Kovačević & Radenković, 2020; Moul, 2019; Tan et al., 2020; Tsokkis & Stavrou, 2018)
Regular security updates	(He et al., 2020; Power & Forte, 2006)
Instructor-led lecture	(Albrechtsen & Hovden, 2010; Aldawood & Skinner, 2019; Carella et al., 2017; Charoen et al., 2008; Cox et al., 2001; Ding, Meso, & Xu, 2014; Dlamini & Modise, 2012; Eminağaoğlu et al., 2009; Ferreira, Correia, & Da Costa Pereira, 2005; Hansche, 2001; Heikka, 2008; Mashiane et al., 2019; McCoy & Fowler, 2004; McCrohan, Engel, & Harvey, 2010; Nogwina, Gumbo, & Ngqulu, 2019; Power & Forte, 2006; Tschakert & Ngamsuriyaroj, 2019)
Gamified training	(Abawajy, 2014; Aladawy, Beckers, & Pape, 2018; Aldawood & Skinner, 2019; Arachchilage & Cole, 2011; Cole, Pence, Cummings, & Baker, 2019; Cone, Irvine, Thompson, & Nguyen, 2007; Cone, Thompson, Irvine, & Nguyen, 2006; Dincelli & Chengalur-Smith, 2020; Dlamini & Modise, 2012; Ghazvini & Shukur, 2017; Gjertsen, Gjære, Bartnes, & Flores, 2017; Gokul et al., 2018; Harta, Margheri, Paci, & Sassonea, 2020; Holdsworth & Apeh, 2017; Huynh, Luong, Iida, & Beuran, 2017; Jayakrishnan et al., 2020; Labuschagne & Eloff, 2014; Le Compte, Watson, & Elizondo, 2015; Mashiane et al., 2019; Oroszi, 2019; Scholl, 2019; Tioh, Mina, & Jacobson, 2017; Tschakert & Ngamsuriyaroj, 2019; Wray, Massey, Medina, & Bolton, 2020; Younis & Musbah, 2020)
Game contests	(Endicott-Popovsky, Orton, Bailey, & Frincke, 2005)
Context-based	(Jenkins & Durcikova, 2013; Kävrestad & Nohlberg, 2015; Kävrestad & Nohlberg, 2020; Moul, 2019)
Written materials	(Abawajy, 2014; Figueroa & Ayyagari, 2015; Hansche, 2001)
Security awareness campaigns	(Aldawood & Skinner, 2019; Cox et al., 2001; Eminağaoğlu et al., 2009; Mashiane et al., 2019)

Table 12. Taxonomy of Identified SETA Methods

Method	**How** training is delivered	**When** the user is trained	What **level of information** that is presented	**What medium** it is presented in
Out-of-bands simulation	Digitally	On-demand or at a scheduled time	Unspecified leaning towards extensive	Unspecified interactive digital material
Attack simulations	Digitally but can include physical elements	Unspecified but commonly contextual or scheduled session	Unspecified	Unspecified
E-learning	Digitally	On-demand or on a regular basis	Unspecified leaning towards extensive	Unspecified digital material
Interactive E-learning	Digitally	On-demand or on a regular basis.	Unspecified leaning towards extensive	Unspecified interactive digital material
Regular security updates	Digitally	On a regular basis	Brief	Video or text
Instructor-led lecture	Physically	At a scheduled time	Extensive	Unspecified
Gamified training	Digitally	On-demand or on a regular basis.	Unspecified leaning towards extensive	Gamified material
Game contests	Digitally	At a scheduled time	Unspecified leaning towards extensive	Gamified material
Context-based	Digitally	Contextual	Brief	Unspecified digital material
Written materials	Physically	On-demand	Extensive	Text
Security awareness campaigns	Physically	Continuous	Brief	Unspecified physical material

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 material's 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 *Evaluate user preferences regarding SETA delivery and discuss the results in relation to existing methods for 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 *Evaluate user preferences regarding SETA delivery and discuss the results in relation to existing methods for 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

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology, 33*(3), 236-247.

Abbasi, A., Zahedi, F. M., & Chen, Y. (2016). *Phishing Susceptibility: The Good, the Bad, and the Ugly*. Paper presented at the 2016 IEEE conference on intelligence and security informatics.

Abraham, S., & Chengalur-Smith, I. (2019). Evaluating the effectiveness of learner controlled information security training. *Computers & Security, 87*.

Agarwal, R., & Prasad, J. (1998). The antecedents and consequents of user perceptions in information technology adoption. *Decision Support Systems, 22*(1), 15-29.

Al-Daeef, M. M., Basir, N., & Saudi, M. M. (2017). Security awareness training: A review. *Lecture Notes in Engineering and Computer Science.*

Al Neaimi, A., & Lutaaya, P. (2018) *The role of culture in the design of effective cybersecurity training and awareness programmes. A case study of the United Arab Emirates (UAE).* Paper presented at the International Conference on e-Infrastructure and e-Services for Developing Countries.

Aladawy, D., Beckers, K., & Pape, S. (2018). *PERSUADED: Fighting Social Engineering Attacks with a Serious Game.* Presented at the International Conference on Trust and Privacy in Digital Business.

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security, 29*(4), 432-445.

Aldawood, H., & Skinner, G. (2019). An academic review of current industrial and commercial cyber security social engineering solutions. *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*

Alkhamis, E., & Renaud, K. (2016). *The design and evaluation of an interactive social engineering training programme.* Paper presented at the 10th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2016.

AlSabah, M., Oligeri, G., & Riley, R. (2018). Your culture is in your password: An analysis of a demographically-diverse password dataset. *Computers and Security, 77*, 427-441.

Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2018). An exploratory study of current information security training and awareness practices in organizations. *Proceedings of the 51st Hawaii International Conference on System Sciences.*

Alwanain, M. I. (2020). Phishing Awareness and Elderly Users in Social Media. *International Journal of Computer Science and Network Security, 20*(9), 114-119.

Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., & Choudrie, J. (2020). Keeping customers' data secure: A cross-cultural study of

cybersecurity compliance among the Gen-Mobile workforce. *Computers in Human Behavior, 114*.

Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology*.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69*, 437-443.

Arachchilage, N. A. G., & Cole, M. (2011). *Design a mobile game for home computer users to prevent from "phishing attacks".* Paper presented at the International Conference on Information Society, i-Society 2011.

Arain, M. A., Tarraf, R., & Ahmad, A. (2019). Assessing staff awareness and effectiveness of educational training on IT security and privacy in a large healthcare organization. *Journal of Multidisciplinary Healthcare, 12*, 73-81.

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*.

Bakar, N. A., Mohd, M., & Sulaiman, R. (2018). Information leakage preventive training. *Proceedings of the 2017 6th International Conference on Electrical Engineering and Informatics: Sustainable Society Through Digital Innovation, ICEEI 2017.*

Boss, S., Galletta, D., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly (MISQ), 39*(4), 837-864.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology, 3*(2), 77-101.

Braunsberger, K., Wybenga, H., & Gates, R. (2007). A comparison of reliability between telephone and web-based surveys. *Journal of Business Research, 60*(7), 758-764.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly, 34*(3), 523-548.

Burris, J., Deneke, W., & Maulding, B. (2018) Activity simulation for experiential learning in cybersecurity workforce development. *Proceedings of the International Conference on HCI in Business, Government, and Organizations* .

Butler, R., & Butler, M. (2018). Some password users are more equal than others: Towards customisation of online security initiatives. *South African Journal of Information Management, 20*(1).

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2014). Going spear phishing: Exploring embedded training and awareness. *IEEE Security and Privacy, 12*(1), 28-38.

Carella, A., Kotsoev, M., & Truta, T. M. (2017). *Impact of security awareness training on phishing click-through rates.* Paper presented at the 2017 IEEE International Conference on Big Data, Big Data 2017.

Caulfield, T., Spring, J. M., & Sasse, M. A. (2019). Why Jenny Can't Figure Out Which Of These Messages Is A Covert Information Operation. *Proceedings of the New Security Paradigms Workshop.*

Charoen, D., Raman, M., & Olfman, L. (2008). Improving end user behaviour in password utilization: An action research initiative. *Systemic Practice and Action Research, 21*(1), 55-72.

Chowdhury, N. H., Adam, M. T., & Skinner, G. (2019). The impact of time pressure on cybersecurity behaviour: a systematic literature review. *Behaviour & Information Technology, 38*(12), 1290-1308.

Cole, J. R., Pence, T., Cummings, J., & Baker, E. (2019) *Gamifying Security Awareness: A New Prototype.* Paper presented at the International Conference on Human-Computer Interaction .

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers & Security, 26*(1), 63-72.

Cone, B. D., Thompson, M. F., Irvine, C. E., & Nguyen, T. D. (2006). Cyber security training and awareness through game play. *Security and Privacy in Dynamic Environments*.

Cooper, M. (2008). *Information Security training - Lessons learned along the trail.* Paper presented at the ACM SIGUCCS User Services Conference.

Cox, A., Connolly, S., & Currall, J. (2001). Raising information security awareness in the academic setting. *VINE, 31*(2), 11-16.

Cybint. (2020). 15 Alarming Cyber Security Facts and Stats. Retrieved from https://www.cybintsolutions.com/cyber-security-facts-stats/

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information systems research, 20*(1), 79-98.

Das, S., Dingman, A., & Camp, L. J. (2018). *Why johnny doesn't use two factor a two-phase usability study of the fido u2f security key.* Paper

presented at the International Conference on Financial Cryptography and Data Security.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319-340.

Desman, M. B. (2003). The ten commandments of information security awareness training. *Information Security Journal: A Global Perspective, 11*(6), 39-44.

Dincelli, E., & Chengalur-Smith, I. (2020). Choose your own training adventure: designing a gamified SETA artefact for improving information security and privacy through interactive storytelling. *European Journal of Information Systems, 29*(6), 669-687.

Ding, Y., Meso, P., & Xu, S. (2014). *Protection motivation driven security learning.* Paper presented at the 20th Americas Conference on Information Systems, AMCIS 2014.

Dlamini, Z., & Modise, M. (2012). *Cyber security awareness initiatives in South Africa: A synergy approach.* Paper presented at the 7th International Conference on Information Warfare and Security, ICIW 2012.

Dodge Jr, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers and Security, 26*(1), 73-80.

Dodge, R. C., & Ferguson, A. J. (2006). Using phishing for user email security awareness. *Security and Privacy in Dynamic Environments*.

Donalds, C., & Osei-Bryson, K.-M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management, 51*.

Dukarm, C., Dill, R., & Reith, M. (2019). *Improving Phishing Awareness in the United States Department of Defense*. Paper presented at the European Conference on Cyber Warfare and Security.

EC-Council. (2019). THE TOP TYPES OF CYBERSECURITY ATTACKS OF 2019, TILL DATE. Retrieved from https://blog.eccouncil.org/the-top-types-of-cybersecurity-attacks-of-2019-till-date/

Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). The positive outcomes of information security awareness training in companies – A case study. *Information Security Technical Report, 14*(4), 223-229.

Endicott-Popovsky, B., Orton, I., Bailey, K., & Frincke, D. (2005). *Community security awareness training.* Paper presented at the 6th Annual IEEE System, Man and Cybernetics Information Assurance Workshop, SMC 2005.

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks, 9*(17), 4667-4679.

Ferreira, A., Correia, R., & Da Costa Pereira, A. (2005). Teaching information security to medical students. *Technology and Health Care, 13*(5), 389-390.

Figueroa, N., & Ayyagari, R. (2015). *Training users on information security: Evidence from Java applets.* Paper presented at the 12th European, Mediterranean and Middle Eastern Conference on Information Systems, EMCIS 2015.

Furnell, S. M., Warren, A. G., & Dowland, P. S. (2003). Improving security awareness through computer-based training. *Security Education and Critical Infrastructures, 125*, 287-301.

Ghazvini, A., & Shukur, Z. (2017). A Framework for an Effective Information Security Awareness Program in Healthcare A Case Study of Computer Game in Hospital Universiti Kebangsaan Malaysia. *International Journal of Advanced Computer Science and Applications, 8*(2), 193-205.

Gjertsen, E. G. B., Gjære, E. A., Bartnes, M., & Flores, W. R. (2017). *Gamification of information security awareness and training.* Paper presented at the 3rd International Conference on Information Systems Security and Privacy.

Gokul, C. J., Pandit, S., Vaddepalli, S., Tupsamudre, H., Banahatti, V., & Lodha, S. (2018). *Phishy - A serious game to train enterprise users on phishing awareness.* Paper presented at the 2018 Annual Symposium on Computer-Human Interaction.

Goluch, G., Ekelhart, A., Fenz, S., Jakoubi, S., Riedl, B., & Tjoa, S. (2007). *CASSIS - Computer-based academy for security and safety in information systems*. Paper presented at the Second International Conference on Availability, Reliability and Security.

Gundu, T., & Flowerday, S. V. (2013). Ignorance to awareness: Towards an information security awareness process. *SAIEE Africa Research Journal, 104*(2), 69-79.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7).

Hagen, J. M., & Albrechtsen, E. (2009). Effects on employees' information security abilities by e-learning. *Information Management and Computer Security, 17*(5), 388-407.

Hansche, S. (2001). Information system security training: Making it happen, part 2. *Information Systems Security, 10*(3), 1-20.

Harrison, B., Vishwanath, A., & Rao, R. (2016). *A user-centered approach to phishing susceptibility: The role of a suspicious personality in protecting*

against phishing. Paper presented at the 49th Hawaii International Conference on System Sciences (HICSS).

Harta, S., Margheri, A., Paci, F., & Sassonea, V. (2020). Riskio: A Serious Game for Cyber Security Awareness and Education. *Computers & Security, 95*.

Hashim, A. S., & Mahamad, S. (2017). Factors affecting awareness on information security in internet banking among Universiti Teknologi Petronas (UTP) students. *Proceedings of the 6th International Conference on Computing and Informatics: Embracing Eco-Friendly Computing*.

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security, 73*, 102-113.

He, W., Ash, I., Anwar, M., Li, L., Yuan, X. H., Xu, L., & Tian, X. (2020). Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. *Journal of Intellectual Capital, 21*(2), 203-213.

He, W., & Zhang, Z. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce, 29*(4), 249-257.

Heikka, J. (2008). *A constructive approach to information systems security training: An action research experience.* Paper presented at the 14th Americas Conference on Information Systems, AMCIS 2008.

Henry, G. T. (1990). *Practical sampling* (Vol. 21): Sage.

Hepp, S. L., Tarraf, R. C., Birney, A., & Arain, M. A. (2018). Evaluation of the awareness and effectiveness of IT security programs in a large publicly funded health care system. *Health Information Management Journal, 47*(3), 116-124.

Hess, T. J., McNab, A. L., & Basoglu, K. A. (2014). Reliability generalization of perceived ease of use, perceived usefulness, and behavioral intentions. *MIS quarterly, 38*(1), 1-28.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS quarterly*, *28*(1) 75-105.

Higashino, M., Kawato, T., Ohmori, M., & Kawamura, T. (2019). *An Anti-phishing Training System for Security Awareness and Education Considering Prevention of Information Leakage.* Paper presented at the 5th International Conference on Information Management, ICIM 2019.

Hofstede, G. H., Hofstede, G. J., & Minkov, M. (2005). *Cultures and organizations: Software of the mind (Vol. 2):* Mcgraw-hill New York.

Holdsworth, J., & Apeh, E. (2017). *An effective immersive cyber security awareness learning platform for businesses in the hospitality sector.* Paper presented at the 25th International Requirements Engineering Conference Workshops, REW 2017.

Hu, S., Hsu, C., & Zhou, Z. (2021a). The impact of SETA event attributes on employees' security-related Intentions: An event system theory perspective. *Computers & Security, 109*.

Hu, S., Hsu, C., & Zhou, Z. (2021b). Security Education, Training, and Awareness Programs: Literature Review. *Journal of Computer Information Systems*, 1-13.

Huynh, D., Luong, P., Iida, H., & Beuran, R. (2017) Design and evaluation of a cybersecurity awareness training game. *Vol. 10507 LNCS. Lecture Notes in Computer Science.*

Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & Information Technology, 32*(6), 584-593.

Jayakrishnan, G. C., Sirigireddy, G. R., Vaddepalli, S., Banahatti, V., Lodha, S. P., & Pandit, S. S. (2020). *Passworld: A serious game to promote password awareness and diversity in an enterprise.* Paper presented at the 16th Symposium on Usable Privacy and Security, SOUPS 2020.

Jenkins, J. L., & Durcikova, A. (2013). *What, I shouldn't have done that?: The influence of training and just-in-time reminders on secure behavior.* Paper presented at the International Conference on Information Systems (ICIS 2013): Reshaping Society Through Information Systems Design.

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to Mitigate Phishing Attacks Using Mindfulness Techniques. *Journal of Management Information Systems, 34*(2), 597-626.

Jin, G., Tu, M., Kim, T.-H., Heffron, J., & White, J. (2018). *Game based cybersecurity training for high school students.* Paper presented at the 49th ACM Technical Symposium on Computer Science Education.

Joinson, A., & van Steen, T. (2018). Human aspects of cyber security: Behaviour or culture change? *Cyber Security: A Peer-Reviewed Journal, 1*(4), 351-360.

Khan, H., Hengartner, U., & Vogel, D. (2015). *Usability and Security Perceptions of Implicit Authentication: Convenient, Secure, Sometimes Annoying*. Paper presented at the Eleventh Symposium On Usable Privacy and Security, SOUPS 2015.

Kim, B.-r., Lee, J.-W., & Kim, B.-S. (2018). Effect of Information Security Training and Services on Employees' Compliance to Security Policies. *Informatization Policy, 25*(1), 99-114.

Kim, E. B. (2014). Recommendations for information security awareness training for college students. *Information Management and Computer Security, 22*(1), 115-126.

Kovačević, A., & Radenković, S. D. (2020). SAWIT-security awareness improvement tool in the workplace. *Applied Sciences (Switzerland), 10*(9).

Kävrestad, J., & Nohlberg, M. (2015). *Online fraud defence by context based micro training.* Paper presented at the 9th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2015.

Kävrestad, J., Skärgård, M., & Nohlberg, M. (2019). *Users perception of using CBMT for informationsecurity training.* Paper presented at the 13th International Symposium on Human Aspects of Information Security & Assurance, HAISA 2019.

Kävrestad, J., & Nohlberg, M. (2020). *Assisting Users to Create Stronger Passwords Using ContextBased MicroTraining.* Paper presented at the IFIP International Conference on ICT Systems Security and Privacy Protection.

Kävrestad, J., & Nohlberg, M. (2020) ContextBased MicroTraining: A Framework for Information Security Training. *Vol. 593 IFIPAICT. IFIP Advances in Information and Communication Technology* (pp. 71-81).

Labuschagne, W. A., & Eloff, M. (2012). *Towards an automated security awareness system in a virtualized environment.* Paper presented at the 11th European Conference on Information Warfare and Security 2012, ECIW 2012.

Labuschagne, W. A., & Eloff, M. (2014). *The Effectiveness of Online Gaming as Part of a Security Awareness Program*. Paper presented at the 13th European Conference on Cyber Warfare and Security ECCWS.

Lastdrager, E., Gallardo, I. C., Hartel, P., & Junger, M. (2019). *How effective is anti-phishing training for children?.* Paper presented at the Thirteenth Symposium on Usable Privacy and Security, SOUPS 2017.

Le Compte, A., Watson, T., & Elizondo, D. (2015). A Renewed Approach to Serious Games for Cyber Security. *Proceedings of the 7th International Conference on Cyber Conflict - Architectures in Cyberspace*.

Lee, H. S., Jeong, D. N., Lee, S. I., Lee, S. H., Kim, K. H., Lee, H. Y., . . . Ko, T. (2019) Result and effectiveness of malicious e-mail response training in a hospital. *Vol. 264. Studies in Health Technology and Informatics.*

Lee, Y., Kozar, K. A., & Larsen, K. R. (2003). The technology acceptance model: Past, present, and future. *Communications of the Association for Information Systems, 12*(1), 50.

Mashiane, T., Dlamini, Z., & Mahlangu, T. (2019). *A rollout strategy for cybersecurity awareness campaigns.* Paper presented at the 14th International Conference on Cyber Warfare and Security, ICCWS 2019.

Mashiane, T., & Kritzinger, E. (2018). *Cybersecurity Behaviour: A Conceptual Taxonomy.* Paper presented at the IFIP International Conference on Information Security Theory and Practice.

McCoy, C., & Fowler, R. T. (2004). *"You are the key to security": Establishing a successful security awareness program.* Paper presented at the ACM SIGUCCS User Services Conference.

McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security. *Journal of Internet Commerce, 9*(1), 23-41.

Moul, K. A. (2019). *Avoid phishing traps.* Paper presented at the ACM SIGUCCS User Services Conference.

Nogwina, M., Gumbo, S., & Ngqulu, N. (2019). *An Overview of the Eastern Cape eSkills Colab Training and Awareness Programmes.* Paper presented at the 2019 IST-Africa Week Conference.

Ntokas, I., Maratou, V., & Xenos, M. (2015). Usability and Presence Evaluation of a 3D Virtual World Learning Environment Simulating Information Security Threats. *Proccedings of the 7th Computer Science and Electronic Engineering Conference* (pp. 71-76).

Offermann, P., Levina, O., Schönherr, M., & Bub, U. (2009). *Outline of a design science research process.* Paper presented at the 4th International Conference on Design Science Research in Information Systems and Technology.

Onumo, A., Cullen, A., & Ullah-Awan, I. (2017). *An empirical study of cultural dimensions and cybersecurity development.* Paper presented at the 2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud).

Oroszi, E. D. (2019). *Security awareness escape room a possible new method in improving security awareness of users*. Paper persented at the 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA).

Paré, G., & Kitsiou, S. (2017). Methods for Literature Reviews *Handbook of eHealth Evaluation: An Evidence-based Approach [Internet]*: University of Victoria.

Parsons, K., Butavicius, M., Lillie, M., Calic, D., McCormac, A., & Pattinson, M. (2018). *Which individual, cultural, organisational and inerventional factors explain phishing resilience?.*

Paper presented at the Twelfth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2018).

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems, 24*(3), 45-77.

Petter, S., DeLone, W., & McLean, E. (2008). Measuring information systems success: models, dimensions, measures, and interrelationships. *European Journal of Information Systems, 17*(3), 236-263.

Pirocca, S., Allodi, L., & Zannone, N. (2020) A Toolkit for Security Awareness Training Against Targeted Phishing. *Vol. 12553 LNCS. Lecture Notes in Computer Science*.

Power, R., & Forte, D. (2006). Case Study: a bold new approach to awareness and education, and how it met an ignoble fate. *Computer Fraud & Security, 2006*(5), 7-10.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS quarterly*, *34*(4), 757-778.

Rahi, S. (2017). Research design and methods: A systematic review of research paradigms, sampling issues and instruments development. *International Journal of Economics & Management Sciences, 6*(2), 1-5.

Rahimi, B., Nadri, H., Afshar, H. L., & Timpka, T. (2018). A systematic review of the technology acceptance model in health informatics. *Applied Clinical Informatics, 9*(3).

Rahman, T., Rohan, R., Pal, D., & Kanthamanon, P. (2021). *Human factors in cybersecurity: a scoping review.* Paper presented at the 12th International Conference on Advances in Information Technology.

Reeves, A., Calic, D., & Delfabbro, P. (2021). "Get a red-hot poker and open up my eyes, it's so boring" 1: Employee perceptions of cybersecurity training. *Computers & Security*.

Reinheimer, B., Aldag, L., Mayer, P., Mossano, M., Duezguen, R., Lofthouse, B., . . . Volkamer, M. (2020). *An investigation of phishing awareness and education over time: When and how to best remind users.* Paper presented at the Sixteenth Symposium on Usable Privacy and Security, SOUPS 2020.

Renaud, K., & Zimmermann, V. (2018). Ethical guidelines for nudging in information security & privacy. *International Journal of Human-Computer Studies, 120*, 22-35.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security, 53*, 65-78.

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior, 57*, 442-451.

Scheaffer, R. L., Mendenhall III, W., Ott, R. L., & Gerow, K. G. (2011). *Elementary survey sampling*: Cengage Learning.

Scholl, M. C. (2019). Raising Information Security Awareness in the Field of Urban and Regional Planning. *International Journal of E-Planning Research, 8*(3), 62-86.

Schürmann, C., Jensen, L. H., & Sigbjörnsdóttir, R. M. (2020) Effective cybersecurity awareness training for election officials. *Vol. 12455 LNCS. Lecture Notes in Computer Science.*

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education, 52*(1),

Shaw, R. S., Keh, H. C., Huang, N. C., & Huang, T. C. (2011). Information security awareness on-line materials design with knowledge maps. *International Journal of Distance Education Technologies, 9*(4), 41-56.

Shin, Y. M., Lee, S. C., Shin, B., & Lee, H. G. (2010). Examining influencing factors of post-adoption usage of mobile internet: Focus on the user perception of supplier-side attributes. *Information Systems Frontiers, 12*(5), 595-606.

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*.

Siponen, M. (2001). Five dimensions of information security awareness. *SIGCAS Computers and Society, 31*(2), 24-29.

Siponen, M., & Baskerville, R. L. (2018). Intervention effect rates as a path to research relevance: Information systems security example. *Journal of the Association for Information Systems, 19*(4).

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & management, 51*(2), 217-224.

Smith, K. H., Mediavilla, F. A. M., & White, G. L. (2018). The Impact of Online Training on Facebook Privacy. *Journal of Computer Information Systems, 58*(3), 244-252.

Soare, B. (2020). Vectors of attack. Retrieved from https://heimdalsecurity.com/blog/vectors-of-attack/

Sombatruang, N., Onwuzurike, L., Sasse, M. A., & Baddeley, M. (2019). Factors influencing users to use unsecured wi-fi networks: Evidence in the wild. *Proceedings of the 12th Conference on*

Security and Privacy in Wireless and Mobile Networks.

Spencer-Oatey, H., & Franklin, P. (2012). What is culture. *A compilation of quotations. GlobalPAD Core Concepts*, 1-22.

Styles, M., & Tryfonas, T. (2009). Using penetration testing feedback to cultivate an atmosphere of proactive security amongst end-users. *Information Management and Computer Security, 17*(1), 44-52.

Tan, Z., Beuran, R., Hasegawa, S., Jiang, W., Zhao, M., & Tan, Y. (2020). Adaptive security awareness training using linked open data datasets. *Education and Information Technologies, 25*(6), 5235-5259.

Taneski, V., Hericko, M., & Brumen, B. (2015). *Impact of Security Education on Password Change*. Paper persented at the 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO).

Thomson, K.-L., Von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security, 2006*(10), 7-11.

Tioh, J. N., Mina, M., & Jacobson, D. W. (2017). *Cyber Security Training A Survey of Serious Games in Cyber Security*. Presented at the 2017 Ieee Frontiers in Education Conference.

Tschakert, K. F., & Ngamsuriyaroj, S. (2019). Effectiveness of and user preferences for security awareness training methodologies. *Heliyon, 5*(6).

Tsokkis, P., & Stavrou, E. (2018). *A password generator tool to increase users' awareness on bad password construction strategies.* Presented at the 2018 International Symposium on Networks, Computers and Communications.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management science, 46*(2), 186-204.

Wheelan, C. (2013). *Naked statistics: Stripping the dread from the data*: WW Norton & Company.

Wray, R., Massey, L., Medina, J., & Bolton, A. (2020) Increasing engagement in a cyber-awareness training game. *Vol. 12197 LNAI. Lecture Notes in Computer Science.*

Vredenburg, K., Mao, J.-Y., Smith, P. W., & Carey, T. (2002). *A survey of user-centered design practice.* Paper presented at the SIGCHI conference on Human factors in computing systems.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security, 23*(3), 191-198.

Wu, D., Moody, G. D., Zhang, J., & Lowry, P. B. (2020). Effects of the design of mobile security notifications and mobile app usability on users' security perceptions and continued use intention. *Information & Management, 57*(5).

Xiong, A. P., Proctor, R. W., Yang, W. N., & Li, N. H. (2019). Embedding Training Within Warnings Improves Skills of Identifying Phishing Webpages. *Human Factors, 61*(4), 577-595.

Yamin, M. M., Katt, B., & Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security, 88*.

Yang, W., Xiong, A., Chen, J., Proctor, R. W., & Li, N. (2017). Use of phishing training to improve security warning compliance: Evidence from a field experiment. *Proceedings of the hot topics in science of security: symposium and bootcamp.*

Yoo, C. W., Sanders, G. L., & Cerveny, R. P. (2018). Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. *Decision Support Systems, 108*, 107-118.

Younis, Y. A., & Musbah, M. (2020). *A framework to protect against phishing attacks.* Paper presented at the ACM International Conference Proceeding Series.

Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies, 131*, 169-187.

Zimmermann, V., & Renaud, K. (2021). The nudge puzzle: matching nudge interventions to cybersecurity decisions. *ACM Transactions on Computer-Human Interaction (TOCHI), 28*(1), 1-45.

About the Authors

Joakim Kävrestad is a senior lecturer of Informatics at the University of Skövde. His research interests are within cybersecurity and digital forensics, focusing on human and organizational aspects. While settled in academia for close to a decade, he previously worked as a forensic expert within law enforcement. Joakim is active in several forums in academia and industry, including ENISA ad-hoc working group on awareness raising.

Marcus Nohlberg is an Associate Professor of Informatics at the University of Skövde, Sweden. Most of his research has been within the human element of security, security management, and security culture/awareness. Before joining academia in 2003, Marcus worked for 10+ years as a consultant, and he is also an enthusiastic entrepreneur and a co-founder of a start-up company. Once upon a time, he was mistaken for Malcolm Gladwell on a flight to Tel Aviv;

while he did not get upgraded to business class, he still got to sign a book.

Steven Furnell is a professor of cyber security at the University of Nottingham. His research interests include usability of security and privacy, security management and culture, and technologies for user authentication and intrusion detection. He has authored over 350 papers in refereed international journals and conference proceedings, as well as various books, book chapters, and industry reports. Furnell is the UK representative to Technical Committee 11 (security and privacy) within the International Federation for Information Processing, and a Fellow and board member of the Chartered Institute of Information Security.

Appendix A

Table A.1. Example of Coding of One Included Paper

Paper	Method	How	When	Level	Medium	Description
Aldawood & Skinner, 2019	OOB simulation	Digital	On-demand or scheduled time		Interactive	Learners experience simulated attacks in a safe environment
Aldawood & Skinner, 2019	Attack simulations	Digital				Learners experience simulated attacks in the real environment, with or without the learners' knowledge.
Aldawood & Skinner, 2019	E-Learning	Digital	On-demand	Extensive	Video or text	Describes videos and governing documents that employees can access on-demand
Aldawood & Skinner, 2019	Instructor-led	Physical	Scheduled time	Extensive		Describes training in seminar or conference forms
Aldawood & Skinner, 2019	Gamified	Digital	On-demand	Leaning towards extensive		Games where learners encounter scenarios
Aldawood & Skinner, 2019	Campaigns	Physical		Brief	Text	Describes infographics and similar with basic information

Appendix B

Table B.1. Example of Coding for One SETA Method

Paper	Method	How	When	Level	Medium	Description
Aldawood & Skinner, 2019	Campaigns	Physical		Brief	Text	Describes infographics and similar with basic information
Cox et al., 2001	Campaigns	Physical	Continuous	Brief	Text	Describes a short "security checklist" to be circulated among users in an unspecified way.
Eminağaoğlu et al., 2009	Campaigns	Physical	Continuous	Brief	Text	Describes posted with slogans and graphics
Mashiane et al., 2019	Campaigns	Physical	Continuous	Brief	Text	Describes posters with short messages

Appendix C

Table C.1. Survey Questions and Answer Options

Item	Options	Sources
Select how you would prefer to receive information security training/education	In physical lectures/presentations that I attend at a specific time (O1)	Reinheimer et al. (2020). Kävrestad, Skärgård, and Nohlberg (2019).
	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)	
Select when you would prefer to receive information security training/education	I want it at a scheduled time (e.g. a planned session) (O1)	Reinheimer et al. (2020). Kävrestad, Skärgård, and Nohlberg (2019).
	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)	
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)	Reinheimer et al. (2020). He & Zhang (2019).
	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)	
Select what level of information you prefer	I want to receive the most important bullets and options for more and deeper information (O1)	Hu et al. (2021).
	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)	
Select in what mediums you prefer to access information security training	Written text (O1)	Reeves, Calic, & Delfabbro (2021). Tschakert and Ngamsuriyaroj. Gjertsen, Gjære, Bartnes, & Flores (2017).
	Video (O2)	
	Audio (O3)	
	Interactive Video/Game (O4)	
	Face to Face (e.g. Lecture or one-on-one) (O5)	