Computer literacy

Does a background in computer programming give you better cyber security habits?

MASTER THESIS WITHIN: Informatics
NUMBER OF CREDITS: 30
PROGRAMME OF STUDY: IT, Management and Innovations
AUTHORS: Bozhidar Ivanov and Joonas Vaino
JÖNKÖPING May 2018
Abstract

Background: Computers are everywhere around us today and skills must be acquired in order for a person to use them. However, the topic of computer literacy is not researched enough to specify basic computer skills to consider an individual computer literate. This thesis will contribute to the research gap by investigating the computer skills of the workforce in the IT sector.

Purpose: The purpose of this thesis is to examine the connection between computer programming and cyber security skills of the IT professional, e.g. is there a beneficial factor of this connection.

Method: For this study the quantitative research method was used to gather data. The authors decided that the best way to reach their target group and answer the research questions was to conduct a survey and pose questions on the topics of computer literacy and cyber security.

Conclusion: The results show that there is a statistical significance between the user’s security habits and his or her programming skills (or the absence of them). People who write code, defined as programmers, scored better on security skills survey, whereas their counterparts, the non-programmers, have some knowledge on the topic but they can never be absolutely sure of their cyber safety in the fast changing world of IT.
## Contents

1. Introduction ........................................................................................................................................iv  
   1.1. Problem ........................................................................................................................................1  
   1.2. Purpose and research questions ......................................................................................................7  
   1.3. Delimitations ...................................................................................................................................8  
   1.4. Definitions .....................................................................................................................................9  
      1.4.1. Computing device ......................................................................................................................9  
      1.4.2. IT sector ....................................................................................................................................9  
      1.4.3. Computer literate ......................................................................................................................9  
      1.4.4. Computer programming ...........................................................................................................9  
      1.4.5. Cyber security ........................................................................................................................10  
      1.4.6. Cyber security habits ............................................................................................................10  
  
2. Theoretical background ......................................................................................................................11  
   2.1. Computer literacy ..........................................................................................................................11  
   2.2. IT sector .......................................................................................................................................12  
   2.3. Basic computer skills ....................................................................................................................12  
   2.4. Cyber security ..............................................................................................................................15  
   2.5. Computer programming ..............................................................................................................19  
   2.6. Comparison with base study .........................................................................................................20  
  
3. Methods ............................................................................................................................................23  
   3.1. Research philosophy .....................................................................................................................23  
   3.2. Research approach ........................................................................................................................24  
   3.3. Research design ...........................................................................................................................26  
   3.4. Research group and setting ...........................................................................................................29  
   3.5. Research credibility ......................................................................................................................30  
   3.6. Ethical considerations ...................................................................................................................33  

4. Results.................................................................................................................................34

4.1. Personal description .....................................................................................................34

4.2. Security habits ..............................................................................................................36

4.2.1. Personal protection ..................................................................................................36

4.2.2. Internet use .............................................................................................................36

4.2.3. Passwords .................................................................................................................36

4.2.4. Use of external storage .............................................................................................37

4.2.5. Carefulness .............................................................................................................37

4.3. E-mail credibility ..........................................................................................................38

4.3.1. Compromised Google account ...............................................................................38

4.3.2. US Green card competition .....................................................................................39

4.3.3. Microsoft terms of use update .................................................................................39

4.3.4. Western union bank transfer ....................................................................................39

4.4. Your opinion is important to us ..................................................................................41

4.4.1. Criticism ..................................................................................................................41

4.4.2. Gratitude ................................................................................................................41

4.4.3. Suggestions ............................................................................................................41

4.4.4. Future considerations ...............................................................................................42

5. Analysis .............................................................................................................................43

5.1. Security score ..............................................................................................................46

5.2. Password score ..........................................................................................................48

5.3. Self-evaluation .............................................................................................................49

6. Conclusion .......................................................................................................................50

7. Discussion ........................................................................................................................52

7.1. Methods and results discussion ..................................................................................52

7.2. Security awareness .....................................................................................................53

7.3. Future research ..........................................................................................................54
8. References..............................................................................................................................55

Appendix I - The survey ..............................................................................................................1

Appendix II - Results from the survey: section “Security habits”.............................................1
List of tables

Table 1 - Table comparison between two studies ................................................................. 21
Table 2 - Types of validity .................................................................................................. 31
Table 3 - Personal description summary ........................................................................... 34
Table 4 - E-mail credibility section summary ...................................................................... 38
Table 5 - Example of coding an answer set ......................................................................... 44
Table 6 - Model Summary output from SPSS Statistics for Security score regression ........ 46
Table 7 - Anova output from SPSS Statistics for Security score regression ....................... 46
Table 8 - Coefficients output from SPSS Statistics for Security score regression ............... 47
Table 9 - Model Summary output from SPSS Statistics for Password score regression ...... 48
Table 10 - Anova output from SPSS Statistics for Password score regression .................... 48
Table 11 - Correlation output from SPSS Statistics between Self-evaluation and Security score ..................................................................................................................................... 49

List of figures

Figure 1 - Types of literacies ............................................................................................... 2
Figure 2 - Types of cyber-attacks ....................................................................................... 16
Figure 3 - Four paradigms for organisational analysis ....................................................... 23
Figure 4 - Process of data collection ................................................................................. 24
Figure 5 - Top 10 e-mail clients ......................................................................................... 27
Figure 6 - Representation of a credible research ............................................................... 30
Figure 7 - Representation of analysis process ..................................................................... 43
1. Introduction

1.1. Problem

Nowadays technology is everywhere around us, aiding in everyday tasks. Communicating, studying, working, learning, traveling, entertaining, even sleeping, almost every aspect our lives involves using a computing device to ease, track or observe a given process. (Rodríguez-de-Dios, van Oosten and Igartua, 2018). This ease comes with a precondition, of course, which would be the knowledge and skills needed to use these devices. To use a computer one must learn it, study it, have an understanding of its functionalities and assess for what and how is it best suited for. In this paper we will summarize this needed knowledge into one word and that is “literacy”.

New technologies are invented every day and from that new literacies emerge. As Tuominen et al. describe it: “We seem to live in the middle of a literacy boom, and new literacies are invented continuously. Examples include computer literacy, media literacy (mediacy), science literacy, mathematical literacy (numeracy), visual literacy, digital literacy, and info-media literacy. The list of new literacies seems nearly endless, extending to esoteric concepts such as moral literacy, dance literacy, and ancient literacy” (Tuominen et al., 2005, pp. 329-345). The researchers encapsulate all the given examples into a single term “information literacy”. Figure 1, below, is a representation of this term.

It turns out that giving a definition for this concept is no small task. Regarded from different perspectives it can mean different things. The first articles dedicated to clear out the confusion date back to the 1960s but one of the earliest definitions was given by Paul Zurkowski. During his presidency at the Information Industry Association in 1974, he stated that information literacy (IL) is “an individual’s capacity to use information tools and primary sources to address problems” (cited in Tuominen et al., 2005, pp. 329-345). Considering that at the time the main source of information were libraries, it does not come as a surprise that the definition of IL associates with the skill of using libraries. However, at the dawn of the computer age, the processes of storing and searching evolved quickly, and so did the skills, required to do so. Information was saved not in books or sheets of paper but in bytes and indexing was not done by shelves but by memory cells in a hard drive. This meant that the old ways of dealing with information were fading away and new practices had to be learned. Tuominen et al. (2005)
described in detail the evolution of the term from 1960 till 2005, defining it as a sociotechnical practice and linking it to technology development. They conclude that there is no clear definition of information literacy because, like technology, it is constantly changing.

*Figure 1 - Types of literacies*

After the authors deepened their research on the term “computer literacy”, new sources of information were taken into consideration while conducting this study. The authors found useful knowledge from the topics discussed on the annual European Conference on Information Literacy (ECIL). It is organized by the Department of Information Management of Hacettepe University and Department of Information and Communication Sciences of Zagreb University.

“Oh Information Literacy, Media Literacy and Lifelong Learning being the main themes, ECIL aims to bring together researchers, information professionals, media specialists, educators, and policy makers from around the world to exchange knowledge and experience and discuss current issues, recent developments, challenges, theories, and good practices” (European Conference on Information literacy, 2018).
One of these papers is a study of IL awareness in academia. Three professors from three different universities conducted interviews with their colleagues to find out if IL is a known term in the world of academics, what is the attitude towards it and if is it taught to their students. The participants were from three academic fields and from three universities: business administration (Graz University, Austria), information science (Tallinn University, Estonia) and information systems (University of Zagreb, Croatia). As mentioned above, IL is a broad term, so in order to yield conclusions Kirinić et al. narrowed it down by defining five topics related to IL:

- awareness of IL (e.g. nature and definition of IL, components of IL including knowledge/skills/abilities);
- attitudes towards IL (importance for education, professional development, and lifelong learning);
- motivation for IL facilitation (motivation for incorporating/facilitating IL in courses/programs, and involving students in it);
- IL experience in courses the academics teach;
- IL requirements expected from students;

At the end, “the results of our study highlight that it cannot be taken as granted that IL is well known outside of the information science community” (Kirinić, Schlögl & Virkus, 2015). So, the term is not taught (in some cases not even mentioned) in universities unless it is a field of study. It is the same case for computer literacy (CL), it is not taught outside its field of study (Reed, 2005), which the writers of this thesis consider as a major drawback for any education system. This behavior by the universities yields an unproductive workforce on the labor market, especially in the IT sector.

But what about schools? Is computer literacy (CL) a known term there? Do high-school graduates gain skills, abilities or knowledge of CL? The authors of this thesis studied a blog post from a teacher from England. Marc Scott talks about how CL is wrongly taught to the younger generation. His post titled “Kids can't use computers... and this is why it should worry you” is more of a rant about the cognitive bias the author sees in people which states that the young are digital natives and thus know how to use a computer. He emphasizes that most people’s knowledge about computers is on a very basic level, that people know how to use pre-programmed containers like programs, apps, operating systems, but lack the understanding on
how these containers work. Scott. M. (2013) brings out four key points as to why this has happened:

- That the mentioned generation of kids has grown up with tech savvy parents who have fixed technical problems rather than let children figure those problems out on their own, which was the case for the previous generation.
- Our primary school systems IT curriculum teaches children about using containers (for example Microsoft products), rather than basic overall IT knowledge.
- School networks, where children are thought, are kept closed, sites are restricted and only authorized applications are installed on school computers. These restrictions deny access to additional knowledge, like the system settings and the command line, to both students and teachers.
- Computers have gone mainstream, which in return have produced better working solutions for problems in the form of different programs and apps. Which, yet again, are more containers for the end user’s disposal, thus removing the need for the end user to understand the processes behind using a computer.

The blog post concludes with: “The truth is, kids can't use general purpose computers, and neither can most of the adults I know” (Scott, 2013) or to explain the statement in other words students are not computer literate enough to really understand what a computer does. By only teaching students to use pre-programmed containers they are stuck in limbo, where one lacks any idea if their selected solution to a problem (being it writing documents, doing calculations or just browsing the web) is the optimal way to do it, because they would lack the knowledge to judge the case. Because of the nature of computing devices, this affects the usage of any one of them as they all boil down to ones and zeros, which makes the lack of computer literacy a major drawback to anyone who works with computing devices. So, going back to the comparison between a computer and a library as a source of information, previously, this brings the authors to the conclusion that CL is not taught well enough in schools giving students who choose IT at the university a competitive edge over their peers.

Further research is needed to specify what skills and knowledge make an individual computer literate. Many writers list different abilities like word processing, web-browsing, simple hardware usage and connectivity, keyboard commands and etc. (Li & Hung, 2010; James, 2012; McKay, 2018). Yet, the most common ability, present in all listings, is staying protected
while using a computer, e.g. cybersecurity. In fact, many studies show that this very important skill is highly and worryingly ignored in the ever growing world of IT.

Furnell and Clark (2012) write that today’s IT services are more focused on ensuring the user’s ease-of-use, than securing his or her personal data. Safeguards have been reduce in order to ensure the user’s attention. Mylonas et al. (2013) criticize that people download, install and give privileges to apps on their smartphones, giving access to personal information, without even considering the risks. Security awareness is terrifying low for the average user when it comes to access of online data. However, this is not the case for physical data. Öğütçü et al. (2016) conclude that an individual is aware that he or she must keep his citizenship number protected, so it would not be abused, but the authors do agree that there is an absence of security habits when it comes to the place where the number is stored, like an online community database, for example. Even the so called “digital-natives [students]” (Scott, 2013), discussed earlier, do not have the necessary skills to stay safe online (Tioh & Mina, 2015). Furthermore, they have the tendency to ignore messages for security breaches, like an antivirus or firewall warning and a required security update notification. Considering, that the older generation is uneducated on the topic to teach the younger one, the outcome is no surprise. Furnell and Moore’s research (2014) conclude that “The younger generation were seen to perform tangibly worse than an adult population who were not exactly ideal in the first place. Thus, it would certainly seem that without some additional effort, security literacy is not going to advance by itself”.

This lack of security knowledge has long been recognized by both academia and industry (Öğütçü et al., 2016). There are ways of ensuring protection on a software and on a hardware level, but the weakest link remains - the user (Tioh & Mina, 2015). The only way to ensure safety is to have an educated person behind the screen and raise the bar of security. When it comes to the workplaces, it is expected to have the highest level of protection of the company’s and the clients’ data. Despite that, Furnell and Moore (2014) argue that “there is a notable gap between where organisations think they need to be and where they actually are” in terms of security. Most jobs in first world countries require the use of computing devices in one of its many forms. This should raise a big concern about security literacy among employers, as we can quite clearly take away from the four points, mentioned by Scott (2013) above, that employees’ computer usage skill level may vary by a lot. The various computer abilities, the lack of education in the field of online safety and the overall picture of today’s cybersecurity habits intrigues the authors of this thesis.
This brings us to the motivation behind this thesis. The authors agree that the knowledge gap of cybersecurity is real and the more it is overlooked, the more dangerous it becomes in the growing world of computers. This is why they want to study the field and focus more attention to the problem. Sadly, there are not many research papers on the topic of computer security in the office, however this creates a knowledge gap which makes room for field to study.
1.2. Purpose and research questions

The purpose of this thesis is to examine the connection between computer programming and cyber security skills of the IT professional, e.g. is there a beneficial factor of this connection. To fulfil the purpose, the authors first must specify the scope in which this study will be conducted. To begin with, this investigation is looking for people who are considered computer literate and who would fit this category better than the employees of the IT sector, the daily users of software and hardware in its many forms (Dictionary, 2018). This study focuses on the IT industries of Bulgaria and Estonia, both proven to have high-ranking solid infrastructure and educated workforce in the field (Ivanova & Castellano, 2012; Grier and Dumbacher, 2011; Hasanli, 2018). This leads to the first research question of this thesis:

What are the basic skills for an employee in the IT sector?

Afterwards, the terms “computer literate” and “computer programming” must be defined in order to frame the basic skills. Both concepts have detailed definitions in chapter 1.4. They allow a separation of the research group into two sub-groups: programmers and non-programmers. From this partition we can define the second research question and fundamental problem:

What affects a user’s computer literacy more: having an education in programming, being employed as a programmer or having programming experience?

The authors of this thesis are also interested to compare the self-evaluation for computer literacy of an individual and his or her actual knowledge. This is the reason to pose an additional question:

How do people from the IT sector assess their computer literacy?

The goal of the last research question is not to analyze the way the participants assess themselves, but to what extent their personal evaluation is correct. The answer will not only deepen the research, but it will show if there is a significant difference between what the IT community knows about computing devices and what it really is. The purpose of this thesis is to examine the connection between the knowledge of writing code and the other computer skills of the IT professional, e.g. is there a beneficial factor of this connection. The authors regard cyber security as one of the most crucial of these abilities. This is further explained in section 3.4.
1.3. Delimitations

While conducting their research, the authors of this thesis faced a lot of difficulties for properly presenting their point of view. The first one was the obscure topic, namely information literacy that was hard to handle for the given time. So, they focused their attention on computer literacy to narrow down the problem. Further investigations revealed that is hard to evaluate computer skills and knowledge because there are too many subsets of abilities in the world of computing devices (Doyle, 2017). Thus, we reach the biggest drawback of this thesis, the single examined topic in the research survey - cyber security. The authors have failed to identify more than one common subject to examine in the survey. To be computer literate may be an obscure term but that means there are more common grounds which can be examined (James, 2012).

In addition, the research was conducted in only two countries - Bulgaria and Estonia. While they might have good IT infrastructures (Ivanova and Castellano, 2012; Grier and Dumbacher, 2011; Hasanli, 2018), the writers could have broadened their work in other and bigger countries, which would have brought knowledge about more aspects of IT (Crotti, 2014).

A third delimitation of this thesis is the fields it is written in: information technologies (IT). As stated in the start, new technologies are invented every day and are constantly changing, and it is hard to make an assessment of something so complex. Hence, it must be pointed out that the conclusions made in this thesis will be valid for the current state of the IT industry with the currently available skills, abilities, tools and knowledge for it.
1.4. Definitions

1.4.1. Computing device

By definition a computing device can be “any electronic equipment controlled by a CPU, including desktop and laptop computers, smartphones and tablets. It usually refers to a general-purpose device that can accept software for many purposes in contrast with a dedicated unit of equipment such as a network switch or router” (PC Encyclopedia, 2018). The authors use “computing device” as a general concept to avoid constant repetition of the above mentioned devices.

1.4.2. IT sector

In the scope of this thesis the concept IT sector or IT field describes an industry which uses computers, software, networks, servers and other technologies to manage and store data (Doyle, 2017). It is specified as a concept because the respondents of this study are the people, working in the IT sector.

1.4.3. Computer literate

For an individual to be considered “computer literate” or “computer savvy” (James, 2012) he or she must possess certain knowledge and skills. James (2012) describes ten abilities that make a person computer literate: to use search engines (1), to have word processing skills (2), to interact with spreadsheets (3), to have basic browser skills (4), to be able to scan for viruses (5), to know common keyboard commands (6), to be able to identify basic hardware components (7), to know basic networking (8), to differentiate various types of cables (9) and to have security habits (10). For this research, the authors recognise only two abilities: to be able to scan for viruses and to have security habits. A detailed description and argumentation of this decision is presented in chapter 3.1. For the purpose of this study, the concept will define an individual who has security habits and knows how to protect him- or herself from cyber-attacks.

1.4.4. Computer programming

Computer programming or programming knowledge is the ability to use a machine-understandable language “for expressing a set of detailed instructions for a digital computer. Such instructions can be executed directly when they are in the computer manufacturer-specific numerical form known as machine language, after a simple substitution process when
expressed in a corresponding assembly language, or after translation from some higher-level language” (Computer programming language, 2018). The writers use this term to make a separation in the research group to people who have this kind of ability and people who do not. For easier reference these two groups are named sequentially “programmers” and “non-programmers”.

1.4.5. Cyber security

Jacobson and Idziorek (2012) specify cyber security as “the process of protecting information from threats”. The term is used in the same sense for this article as well. The authors define it as the common skill for all employees, working in the IT sector. For an IT professional it is essential to “know how to protect yourself from attackers on the Internet and keep your personal data private” (James, 2012).

1.4.6. Cyber security habits

“...we, the users, play the most significant part in determining the security of our information by the decisions we do or do not make” (Jacobson & Idziorek, 2012). Simply put, to be assured of our privacy and security, the everyday user is the last line of defence in cyber security and the legitimacy and accuracy of the information given to us must be always checked before used. The authors of this thesis would like to encapsulate these required types of everyday security actions with the phrase “cyber security habits”.

2. Theoretical background

2.1. Computer literacy

As stated in chapter 1.1, computers are everywhere around us today and skills must be acquired in order for a person to use them. We have become so used to computing devices in our everyday tasks, that it is hard not to learn to use them (Rodríguez-de-Dios, van Oosten and Igartua, 2018). Above was also mentioned Justin James (2012) from TechRepublic who presented in his article ten skills which make an individual to be considered computer literate: use of search engines (1), word processing skills (2), interaction with spreadsheets (3), basic browser skills (4), performing a virus scan on a computer (5), knowledge of common keyboard commands (6), identifying basic hardware components (7), knowledge of basic networking (8), differentiating various types of cables (9) and possession of security habits (10). However, “Being able to do simple tasks [with a computer] does not mean the person is computer literate, but simply proficient in those simple tasks. This leads to the argument that computer literacy means being able to understand how the computer works.” (Childers, 2003). Hence the focus of this study is not if people are able to use computing devices, but rather the manners in which they are using them. Do they really understand what, how and why happens in the background, when using them? This leads to the separation of two groups: people who “regard the computer as a proverbial black box” (Childers, 2003) and those who not only use it but know how the “black box” functions. This difference in the computer literacy of the two groups intrigues the authors of this thesis, so they set off to find if this difference is justifiable and what are the benefits of it.

In order to answer the research questions, the authors specify that they define the above mentioned two groups as “programmers” and “non-programmers” with computer programming knowledge as the main differentiator. “People who program can communicate with computers, which is becoming more and more important now that computers have a hand in almost everything.” (Woodward & Fayed, 2016). Hence, because the ability to “communicate” with computers is an essential skill in the modern world, people who know programming should have an advantage over those who do not.
2.2. IT sector

In order to conduct this study and prove that computer programming skills affect computer literacy, the authors need to find a suitable research group. This group must include both programmers and non-programmers and the numerous job titles in the IT sector seem to be a good fit - “People with jobs in the career field of information technology (IT) use computers...” (Doyle, 2017). So, the sector is represented by people who can be considered computer literate, yet not all of them need to know programming. In the IT sector there are job titles like software developer who “design, run, and test various computer programs and applications. They usually have a bachelor’s degree in computer science or a related field. They also have strong programming skills.” (Doyle, 2017) as well as digital marketeer who only uses the programs and applications developed to perform his or her job. Simply said, the IT field is an excellent source of data for this study because it contains representatives from the programmers’ and non-programmers’ groups, both proven to be computer literate.

For this thesis the IT sectors of Bulgaria and Estonia were selected. Except being home-countries of the authors, both have fast growing infrastructures in the field, which allowed the use of already established connections with the IT workforce.

“The Bulgarian IT market has shown a steady growth over the years; [...] The advantages of Bulgaria as an outsourcing destination come from low-cost, highly educated workforce, combined with solid infrastructure, economic and political stability, geographic proximity and fewer security concerns. Based on the structure of the growth rates and the most sought IT skills, the organizations in Bulgaria are in the final stage of building their IT infrastructures (ICT Media 2008).” (Ivanova & Castellano, 2012).

“[Estonia] has become a leader in e-government services as well as an active participant in the global information and communications technology business. With its aspirations to be a leader in IT and telecommunications, Estonia somehow encourages turning instinctively to these technologies in times of crisis, great or small.” (Grier and Dumbacher, 2011).

2.3. Basic computer skills

Now, with the test subjects determined, the researchers need to think of the way they are going to conduct the research to yield results proving their case study, e.g. to make a comparison of the computer literacy between the programmers and the non-programmers. In order to achieve
this, they have to define the basic computer skills to allow a scale for comparison. Justin James (2012) writes in his article “10 things you have to know to be computer literate” the following:

- Search engines - the ability to use Google, Yahoo, Bing not only as searching keywords but also the usage of advanced search and Boolean operators;
- Word processing - writing and formatting texts not only in documents but in emails as well have been an essential skill for computer literate people;
- Spreadsheets - the power of analysis, the ability to input data in cells and use formulas, references, and macros to edit and transform that data;
- Browser basics - skills here include not only to differentiate the search bar from the URL bar but also opening links in new windows or tabs, using bookmarks, editing URLs to perform navigation, clearing the browser’s cache and understanding common error messages;
- Virus/malware scanning - modern antivirus programs are automated processes which keep you safe during the day but it is still important to know how to trigger a manual virus/malware scan, as well as how to use alternative systems, spot signs of an infection, and other similar tasks;
- Common keyboard commands - the use “shortkeys” saves time and efforts if the user knows how to use them;
- Basic hardware terminology - knowing the different hardware in and around your computer. While it is not important to know how to fix a given hardware problem, identifying the problematic piece and contacting the right person for it, can be regarded as computer literacy;
- Simple networking diagnostics - Connecting to a network (wired or wireless) has become an everyday activity and also a must-have skill to be computer literate;
- How to hook it up - the ability to differentiate the ports and cables your computer uses, at least charger;
- Security/privacy 101 - knowing how to check a link before you click it, to verify that encryption is being used to transmit sensitive data and overall protection of your privacy on- and offline;

Certainly, James’ top ten list is not exhaustive and there are other researchers who have made their conclusions on the term “basic computer skills” but the struggle here is with the fact that there are tons of jobs available in IT (Doyle, 2017). Each job specification requires a different set of computer skills. While a web developer needs programing skill to write a program and
some word processing abilities to document this program, a computer support specialist needs not only excellent word processing skills for contacting clients, but also good user interface knowledge of the chosen support system. Needless to say, programming skills are of no use for this work position (McKay, 2018).

To battle this entanglement of definitions and job descriptions, the investigators seek a core ability, a must-have skill among all employees, who work in the field of IT. The answer was found in Grier and Dumbacher’s (2011) article, which talks about Estonia’s growing vulnerability to cyber-attacks due to its growing cyber-infrastructure. Since, the only way to protect against cyber-attacks is to ensure that all individuals involved have solid security habits, the need for cyber security skills exists for both, the programmers and non-programmers, working in the IT sector. Thus, the authors of the thesis chose cyber security skills as the common ground in computer literacy that allows them to evaluate programmers’ and non-programmers’ knowledge in CL.
2.4. Cyber security

Cyber security is the “the process of protecting information from threats” (Jacobson & Idziorek, 2012). These threats come in many forms and different solutions have been implemented to oppose them but “It has long been recognized that the user is in fact is the weakest link in the security chain” (Jacobson & Idziorek, 2012). Users are not aware of the risks in using a computing device. “A likely reason for this is that security issues were not dealt with in the laptop classes [in school], while hardware and operating system, office software and the use of the Internet (particularly for information retrieval) where explicitly covered within the subjects' curricula.” (Schaumburg, 2008).

There are many frameworks to categorize security threads. For example, C. P. Pfleeger and S. L. Pfleeger split cyber security threats into two categories: nonhuman (e.g. natural causes: fires, floods, failure of a component) and human threats. Human threats can be split into benign intent (e.g. human error: unintentionally deleting something, typing the wrong thing) and malicious intent. Malicious intent can also be split into random and direct. Random attacks do not pick their targets and are executed on masses, an example of this could be malicious code on a website that could be visited by any person. Direct attacks are targeted on specific computers or a group of computers (e.g. all computers in a company, all computers using a specific program) (Pfleeger & Pfleeger, 2011). Shirey (2000) divides attack types into active, passive, inside and outside. Where active attacks try to change the system and its operation and passive attacks try to get hold of information on the system, not affecting its operations (Shirey, 2000). Inside attacks are launched from inside the security perimeter of a device by someone who has authorized access to the system and outside attacks are launched from the outside perimeter of a device: e.g. over the internet (Shirey, 2000). There are more ways to categories threats, depending on the needs of users, although most models are quite similar to each other.
Threat categorization is useful to understand what type of an attack has happened, where it could have come from and what part of the system it affects. Having knowledge of threat categorization also helps mitigate threats, as it helps users predict cyber dangerous action they might take. Any type of an attack a user has witnessed usually fits into one or more category in a threat model. So, knowing where your system was compromised could help the user figure out the attack they have fallen victim to and vice versa. This helps to raise security awareness and to fix the problem.

As with threat categories there are also many different attack types. Different attacks can also be used in combination with each other. The following is partial list of most well-known attacks:

- **Port scanning**: Port scanning is not malicious by itself but is rather used to find potential targets. A port scanner is a program which tries to connect to random servers and ports to see if there are services running on them to later exploit their vulnerabilities (Shirey, 2000).

- **Denial-of-service attack (DoS)**: With a DoS attack the attacker simply tries to block out other traffic from the target, this is achieved by the hacker’s machine by making so many requests to the target that the target fails to serve others (Nsfocus, 2014).
- Distributed denial-of-service attack (DDoS) - Same as a DoS attack, but the attacker uses multiple devices to achieve their goal. Therefore, it is a lot harder to stop as the attacking traffic is coming from more than one place (Nsfocus, 2014).

- Man in the middle attack - The attacker relays information between two parties. This can be achieved multiple ways e.g. getting access to the victim’s router, computer or specific service used, but the attacker must have access to the information sent between two parties. The attacker can just be passively monitoring information sent, known as eavesdropping, or even change the message the receiving end gets (Wang & Wyglinski, 2016).

- Malware attack - Short for malicious software attack, the attacker tries to plant their malicious software on the victim's computer. Malware comes in different types or in a combination of the following (Moir, 2003):
  - Viruses - Malware that tries to modify other programs (Moir, 2003).
  - Worms - Malware that can replicate itself and infect other devices (Moir, 2003).
  - Trojan Horses - Malware which tricks the user into thinking it is used for something else then infecting their computer (Moir, 2003).
  - Spyware - Malware which tries to collect data about the victim without them knowing (Moir, 2003).
  - Ransomware - Malware which duplicates or locks down the victim’s data for the use of extortion (Liska & Gallo, 2017).
  - Scareware - Malware which tries to scare or cause panic in the victim, usually for the purpose to make the victim buy unneeded software (Ince, 2013).
  - Adware - Malware which tries to show the victim specific online advertisements (Ince, 2013).

- Spoofing - The attacker presents an attacker-controlled copy of a valid website, e-mail, network etc. to get access to the victims data (Ince, 2013).

- Phishing - The attacker presents himself/herself as a trustworthy source to acquire sensitive user information (Ince, 2013).

When used correctly, most computers have security software that is capable to fend off most attacks. These softwares are known as antivirus software or anti-malware and firewalls. Antivirus software is capable of detecting and removing of malware. This is achieved by scanning your system for malicious patterns and cross referencing them with known viruses and attacks (Koret & Bachaalany, 2015). A firewall is a network security system, that monitors
traffic going through the user’s computer, based on predefined security rules. A firewall typically blocks data movement between the user’s computer and untrusted networks (Butterfield & Ngondi, 2016). However, these all require that the user of the computing device has had the habit of updating and maintaining the necessary security software.

As mentioned before, in cyber security the last line of defense are still the users (Jacobson & Idziorek, 2012). They can always veto the work of an antivirus program or a firewall and choose not to keep them up to date. User activities can also increase or decrease the risk of cyber-attacks. For example, by having “strong” passwords that are as long as possible and use the whole spectrum of available symbols (uppercase letters, lowercase letters, numbers, symbols) (Schloman, 2004) and by not using the same password multiple times (Curran et al., 2011) one could significantly reduce the risk of his or her password being hacked. Also, by opening attachments only from trusted sources and by recognizing when they are being tricked (Schloman, 2004) the risk of falling a cyber-attack victim is reduced. Finally, not your usual everyday activities such as shredding or wiping an old hard drive are beneficial as possible remnants of old information are still present on them (Millard, 2013).

Sadly, research shows that most people are not completely aware of the risks associated with computer usage. Arlitsch & Edelman (2014) describe the world today as a technology-driven environment, all connected to and communicating through Internet. All of the devices around us store and share our personal information, making our lives easier, but this comes at a price. It seems the use of technology comes hand to hand with the cyber security threats.

Hall (2016) has studied the weakest link in the world of cyber security - people. In his work he evaluates the consequences for the employers by inspecting the weakness at a personal and at an organizational level. On a personal computer people are careless of their security. The researcher regards the biggest threat to personal information to be the social media websites, giving as an example Facebook. Willingly sharing his personal details to the social network, an individual increases the risk of a hacker to impersonate them. Using the victims name to extract valuable information through colleague contacts. At work this carelessness is transferred, luckily it is overlooked by the company’s security system. However, this system cannot prevent an employee to open a phishing e-mail. Hall (2016) considers that organizations must focus more resources on security because there are users who do not know about the risks out there. “After all, even the most secure of companies is only as strong as its weakest link.” (Hall, 2016).
2.5. **Computer programming**

Heretofore, the authors of this paper have revised what it is to be computer literate and emphasized on the most important skill of this set - security habits. Now they want to study if there is a way to enhance these habits: to make a computer literate person more secure. Both authors have higher education in Computer Science and computer programming was thought up as a way to enhance security knowledge.

One of the biggest advantages of learning programming is that it teaches logical thinking (Porter, 2016; Creighton, 2017; Engel, 2014). A program consists of multiple small problems. Each problem is tackled by the programmer the best way possible, building strength and complexity with every solution. Once gotten used to, this approach is easily transferable in everyday work, big complex problems are transformed to small accessible tasks. Coding teaches us to be more focused, have more logical and structured thoughts, sharpening “your reasoning and problem-solving skills” (Engel, 2014).

John R. Woodward and Marwan Fayed (2016) compare computer programming to Latin but “unlike Latin, it is anything but dead”. They are advocates of the idea that programming should be part of every school’s curriculum. The young generation is surrounded by computers and they must know how they function and be aware of the risks and threats using them. The writers make a step even further by saying that: “Errors sometimes occur when documents outlining in English how a program should work are translated into computer code. Those who have an appreciation of a programming language can write these more clearly. Indeed, businesses usually have to employ specialist analysts as intermediaries to help with this translation process. As computers become more dominant, those who don’t know how to think in this [logical] way risk being increasingly left behind.” (Woodward and Fayed, 2016).

The ability to code has become a big advantage on the labor market because of the wild spread of computers. Paraphrasing Scott Childers’s words: “computer literacy means being able to understand how the computer works” the authors state that: “to be able to protect your data means to know how attacks on that data work”. This ascertainment has lead the authors of this thesis to believe that computer programming can improve a person’s cyber security skills as well.
2.6. Comparison with base study

Before conducting their research, the authors examined previous studies on computer literacy in the workplace. An extensive search was conducted, using Jönköping University’s online library services, like Primo and other databases for academic papers. Unfortunately, it was hard to find appropriate sources on the topic because the field is not researched enough. The closest and most useful article found was written by Li and Hung and published in 2010. They investigate how information literacy can enhance job performance in the workplace setting.

In this thesis, the authors wanted to replicate Li and Hung’s methodology, by performing a research about computer literacy in the scope of the IT sector. Their hypothesis is that computer programming has a beneficial influence on the computer skills of the employee from the sector. To do this a replication strategy must be implemented.

In their book, DePoy and Gitlin (2015) describe three types of reasoning strategies for replication: deductive, inductive and abductive. Deductive reasoning is used when an existing and accepted theoretical framework is used to explain a specific case. Inductive reasoning uses the reverse logic of the deductive one. It is present when researchers draw rules or patterns from specific observations to define a framework. Lastly, abductive reasoning is positioned in the middle of the first two. It is used in studies where the observations do not fully apply to a specific framework but still have common concepts with it.

For this study an abductive approach was chosen. The authors have reached the understanding that to be able to conduct correctly their research a combination of deductive and inductive reasoning is required. The research is considered deductive because it replicates to some extend Li and Hung’s (2010) work. However, at the same time it uses an inductive approach because it includes new concepts and excludes some of the existing ones from the developed framework. The abductive reasoning is followed because it is a way to choose the most accurate explanation among different alternatives (Dudovskiy, 2018). Table 1 presents a comparisons between the two studies.
<table>
<thead>
<tr>
<th><strong>Table 1 - Table comparison between two studies</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field of study</strong></td>
</tr>
<tr>
<td><strong>Country</strong></td>
</tr>
<tr>
<td><strong>Publishing year</strong></td>
</tr>
<tr>
<td><strong>Title</strong></td>
</tr>
<tr>
<td><strong>Subjects</strong></td>
</tr>
<tr>
<td><strong>Sector</strong></td>
</tr>
<tr>
<td><strong>Data collection strategy</strong></td>
</tr>
<tr>
<td><strong>Data analysis strategy</strong></td>
</tr>
</tbody>
</table>

Li and Hung (2010) start off by stating the problem they have acknowledged - there is a research gap on studies focusing on IL in a workplace environment, so they decide to evaluate the connection between information literacy and the work outcome. They examine IL in three dimensions: traditional literacy, Internet literacy and computer literacy. “Traditional literacy describes the degree of knowledge, skill and ability of printed sources use. Internet literacy denotes the degree of knowledge, skill and ability of web use. Computer literacy refers to the knowledge, skill and ability of computer use” (Li & Hung, 2010). For the work outcome variable, they use the person-job (PJ) fit concept, which is the extent for an individual’s capability to reach specific job requirements. Subsequently, they create their hypothesis by assuming the positive relations between the examined variables and create a survey with questions for each dimension of IL. As for the research group, they have investigated the benefits of IL in the financial sector of Taiwan. The empirical results prove that IL (including computer literacy) has a significant positive influence on PJ fit, e.g. this knowledge helps the worker to be more informed about and, from that, to feel more comfortable at his/her workplace (Li & Hung, 2010).

This thesis will follow the research process, outlined by Li and Hung (2010) with a few changes along the way. The writers of this document also acknowledge the same research gap and want to contribute to reduce it. They decide they want to investigate further by conducting their study in a different research setting - the IT sector. After, a similar hypothesis was thought of -
computer programming has a positive relation to computer skills. At this point it was logical to use the same questionnaire from the Taiwan study, however upon a deepened review of the basic computer skills in the IT sector, changes had to be made. The researchers stumbled upon an obstacle that impedes their progress - they did not have a scale for measuring an individual’s computer literacy. Therefore, they set off to find such a scale. Research shows that literacy is the possession of knowledge and skills on a given topic (Tuominen et al., 2005, pp. 329-345). This is where the authors encounter their second difficulty - the IT sector has a wide range of abilities (Doyle, 2017) to be considered computer literate. If they attempted to evaluate all of the discovered basic computer skills, the final questionnaire would be too long and people would be reluctant to give their time to answer it. This would result in limited responses and a lot of time for conducting the research. Thus, the authors decided to use one of the many computer abilities to create a measuring scale. They turned to the most common item in the lists of computer skills - security (Creighton, 2017; Engel, 2014; Porter, 2016). This new base topic required a change in the questions of the survey, to evaluate the participants’ security habits. Now, the authors have the means to conduct their research, resulting in change of the main framework. A needed action in order to gather adequate results to make an evaluation of the competence of the current workforce in the IT field and contribute to the research gap on information literacy in the IT sector.
3. Methods

3.1. Research philosophy

As stated by Duignan (2016), the research philosophy is a concept in which new knowledge is developed. This concept is influenced by each contributor’s point of view and their assumptions about reality and personal values. The research philosophies can be categorized in four distinct and rival paradigms (set of basic assumptions): radical humanist, radical structuralist, interpretive and functionalist (see Figure 3). The authors will not go into details for each paradigm, only the one which this research applies to.

Figure 3 - Four paradigms for organisational analysis

A key-assumption in the functionalist paradigm is rationality. Rational problems are resolved by using rational explanations presented by rational people. Usually, research done using this paradigm aligns itself with the positivist research philosophy (Saunders et al., 2009). From the literature review and personal experience the researchers have developed a logical hypotheses to test out in a realistic environment - the IT sector. They have tried to remain neutral and detached to produce an uninfluenced new knowledge. Furthermore, they have strived to keep this research as transparent as possible so it can be replicated in the future. These are the reasons to consider this research aligned with the positivist standpoint.
3.2. Research approach

For this study the deductive approach was chosen. Saunders (2009) describes this approach as suitable for explaining the casual relationship between two (or more) variables. In the scope of this thesis, these two variables are the ability to computer program and the level of a security the person possess.

The quantitative research methodology was used to gather data. The authors decided that the best way to reach their target group and answer the research questions was to conduct a survey and pose questions on the topics of computer literacy and cyber security. While giving more precise results, the qualitative methodology involves a demanding analysis process later (Saunders, 2009). The authors were reluctant to find sources of information on the basis of which to conduct this analysis. This is why the qualitative methodology has been overlooked.

Keeping in mind that an individual must be able to use a computer to take part in this study, the researchers can freely use the conveniences of web-based questionnaires, or as Thomas (2004) describes them “E-mail invitation link to URL (or Web address) questionnaires invite the participant to respond to the questionnaire by either clicking on an embedded URL or copying and pasting the URL into their Web browser. The participant responds to the questionnaire on the Web”.

Figure 4 - Process of data collection

![Google Forms Process](http://www.forms.google.com)

Source: Adapted from “Google Forms”, by www.forms.google.com.

The survey was generated using Google Forms - an online platform for creating, styling and dispersing web surveys and gathering the participants’ answers in one table (see Figure 4). The platform allows answering surveys on mobile devices as well, which allowed the respondents to reply immediately no matter which computing device they were using (Google Forms, 2018). Limited time for conducting the research was one of the complications the authors struggled with. This is the main reason for them to use the convenience sampling technique. Links were not only distributed by e-mail. Social messaging applications such as Facebook Messenger, Viber and Skype were used to connect to as many people in the IT sector as
possible. Also, the participants were asked to send out the link to colleagues, creating a snowballing effect and expanding the research group even more. The sample selection process was kept running as long as possible. The writers do acknowledge that this sampling technique is prone to bias, this is why they were strict on keeping the variation of the population as low as possible (Saunders, 2009).
3.3. Research design

As discussed earlier, this study uses a quantitative research method to gather data, therefore, a survey was created. The questions in it were inspired by an extensive literature review and the administrators of two IT companies (one from Bulgarian and one from Estonian). Firstly, the authors searched for similar surveys and the closest match to this kind of research was the work of Chung-Kai Li and Chia-Hung Hung in 2010, who studied the work environment in financial institutions in Taiwan. They proved that “there is a positive relationship between dimensions of traditional literacy and computer literacy toward person-job fit”, or in other words, computer literacy helps an individual to be better at his job. As pointed out above, the authors consider cyber security as important knowledge in order to be computer literate, making an individual more protected and a better professional in the world of IT. Thus, Li and Hung’s work was considered only as a starting point for the questionnaire. Secondly, more questions were added on the topic of cyber security, plus personal question for the participants to be able to differentiate the programmers and non-programmers (Lankshear & Knobel, 2008; Jacobson & Idziorek, 2012). A final source of information were the administrators of the companies. They were asked to revise the questionnaire and evaluate if there were any missed scenarios. The questions themselves (see Appendix I) were separated into four sections: Personal description, Security habits, E-mail credibility and Your opinion is important to us.

The goal of the first section is to acquire a description of the participant. Therefore, it contained questions about his or her age, sex, higher education, programming skills and work position. The answers allow the authors to specify to which of the two groups the contributor fits: programmer or non-programmer, and if he or she is in the first group, what is the experience he or she has. An additional question is added in this section for self-evaluation to determine if the participant considers him- or herself computer literate enough to be secure from cyber-attacks when using a computing device.

The security section is the main part of the survey. The questions in it are about security and privacy habits, focusing the participant’s attention on different ways of how one could prevent cyber-attacks. The end-goal of this section is to evaluate these habits of the contributor. Most of the questions are in single selection form, making it easier to make a comparison scale between the programmers and non-programmers.

The authors of this thesis wanted to also examine if people do notice a phishing attack when they encounter one. This is why the last section contains screenshots of four e-mails. To be
more realistic, they were created in a Gmail-looking web interface. Being one of the most popular mail clients (Email Client Market Share, 2018), most of the participants will have seen the interface before and will thus immediately focus on the content of the email itself. A list of the top ten most used e-mail clients is presented on Figure 5:

*Figure 5 - Top 10 e-mail clients*

![Bar chart showing the top 10 e-mail clients.](image)

Source: Adapted from “Email Client Market Share”, by www.emailclientmarketshare.com and “2018 Email Client Market Share Trends From 11+ Billion Opens” by Kevin Mandeville.

The four e-mails examine the ability of the survey respondent to recognise e-mail spoofing attempts. They are asked if they would interact with each specific e-mail (e.g. respond to it, click links in it, follow instructions from it) and to argue their choice with a few words. The first example (see Appendix I) presents a fake electronic letter from Gmail’s support team for a compromised account. The hint here is represented in the suspicious link indicated to fix the problem and the suspicious address the warning is coming from. More educated Google users would also point out that Google does not send an e-mail in case of a breach but uses online interfaces to ensure security. The second e-mail is the well-known fake green card visa scam, asking you to send money and documents to obtain the US border pass. A red flag for the keen eye should be the spelling mistakes, bad grammar and strange e-mail addresses (Stahl, 2011).
To keep the reader’s attention on the screenshots, the third one was taken from a real Microsoft service agreement update letter. There was no phishing involved here but the aim of this one is to examine do the participants spot the real e-mail. The last one is from Western Union. The user is asked to click on a link to unlock his transaction. A warning in this case would be the strange domain the message is send from, a missing transaction identification number or a person to contact over the phone or directly in an office.

The last section contains only one open-ended question. The goal here is to collect feedback and other ideas on the subjects of Computer literacy and Cyber security, not asked about in the survey.
3.4. Research group and setting

As previously mentioned, the focus group of this study are the people qualified to work with computers. Regarded as the professional computer users, the authors regard them as the best subjects for this research. Therefore, the best candidates are the workforce of the IT sector.

Before sending out the survey the researchers wanted to make sure everything was clearly written and understandable. A test group was formed consisting of the thesis coordinator and three IT specialists. Their task was to go through the survey and evaluate the work done. There were a few remarks and corrections, but overall the survey was exhaustive and well-structured.

The survey was sent out to every connection the authors had in the IT sector. Links were generated using the Google Forms functionality and distributed by e-mail and social messaging applications such as Facebook Messenger, Viber and Skype. Also, the participants were asked to send out the link to colleagues, expanding the research group even more. Results were collected for 4 weeks and the number of responses was 105.
3.5. Research credibility

In order to consider this study as credible, the authors strived to explicitly outline its research philosophy, approach, design and delimitations. Also, it must meet two measures of quality: validity and reliability. The first one examines how accurate is the concept measured in the quantitative study and the second one - the accuracy of the instrument. Giving an assessment with the two measure will prove further the credibility of the study (Heale & Twycross, 2015).

Figure 6 shows a representation of the outcomes of a credibility test, the most desired one being the most-right one.

*Figure 6 - Representation of a credible research*

There are three types of validity: content validity, construct validity and criterion validity. A short description for each of them is provided in Table 2. In the scope of this study, the construct is computer literacy or more accurately, cyber security. The aspects of cyber security are presented in chapter 3.4. Not all aspects were included in the survey, but the authors argue that based on the literature review, the well-known security threats are acknowledged. Also, the survey was first presented to a test group, which were asked to make an assessment as a whole. “This is called establishing face validity, because respondents are judging whether the instrument looks valid to them.” (Muijs, 2010). Therefore, the research is content valid.

As stated above, Chung-Kai Li and Chia-Hung Hung’s research “An examination of the mediating role of person-job fit in relations between information literacy and work outcomes” was used in the basis of this thesis. E.g. there are similarities between the two instruments, which is an existing convergence between the two studies. Being one of the types of evidence (Heale & Twycross, 2015), the convergence makes this study’s construct valid.
Table 2 - Types of validity

<table>
<thead>
<tr>
<th>Type of validity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content validity</td>
<td>The extent to which a research instrument [survey] accurately measures all aspects of a construct</td>
</tr>
<tr>
<td>Construct validity</td>
<td>The extent to which a research instrument (or tool) measures the intended construct</td>
</tr>
<tr>
<td>Criterion validity</td>
<td>The extent to which a research instrument is related to other instruments that measure the same variables</td>
</tr>
</tbody>
</table>

Source: Adapted from “Validity and reliability in quantitative studies”, by Heale, R., & Twycross, A., 2015, Evidence-based Nursing, 50(2), p. 179.

To examine the final measure of validity, criterion validity, the Pearson Correlation was used to evaluate each survey variable. All of the answers were coded and transferred into SPSS Statistics. There a total score was calculated by summing all the variables. Sig. (2-tailed) was a significance level of 5%, while N, the total of survey respondents, is close to 100 people. Comparing the total score value with the r table product moment the validity of each variable (SPSS Statistics, 2017; SPSS tests, 2015). 25 out of 30 variables were greater than the value from the table, making them valid. Thus, the writers of this thesis conclude the research is 83% criterion valid.

Reliability measures the consistency of the survey, e.g. if this research is run again, would it yield the same results. It is hard to evaluate precisely reliability of a study; it can be estimated using two measuring attributes: repeated measurement and internal consistency.

Repeated measurement regards the consistency of the survey upon repeating runs of the research with the same environment variables, known as the test-retest method. Unfortunately, this survey has been distributed only once and this type of reliability test cannot be assessed without an additional set of results. And being anonymous there is no way to reach the exact same research group. Sadly, this research fails the repeated measurement attribute.

Internal consistency can be assessed using Cronbach’s alpha. This is one of the most used reliability test instruments with a high degree of evaluation. The test calculates a coefficient, which between 0 and 1. If the coefficient is greater than 0.600 then the questionnaire items dictate reliable, if it is less than 0.600 - they dictate unreliable (SPSS Statistics, 2017; SPSS tests, 2015). For this research, the case processing summary showed that all the data was valid, and no records were excluded. From the output of Reliability Statistics, the obtained
Cronbach's alpha value was 0.712 which is greater than 0.600, making this research instrument statistically reliable.
3.6. Ethical considerations

It is important to acknowledge that not every participant was willing to answer all the questions in the survey. The authors tried to keep the questions and examples as short as possible, but it was hard to maintain that, especially in the E-mail credibility section, where half of the examples were very long texts. Probably, most of the participants were impatient and did not read through the whole e-mail. Feedback from one interviewee showed that he or she did not read the e-mails at all, writing “tl;dr” (Internet slang for “too long; didn’t read” (Wikipedia, 2018)) in the comments after them. Overall it was a risk worth taking to present a real-life case scenario.

Also, being a survey on security habits, there were questions linking to personal data, like passwords, use of bank cards, knowledge and so on. To ensure people that giving this information is safe, the survey was made anonymous, e.g. no name, e-mail or login was required to identify the participant. Also, to the most sensitive questions the answer option “Prefer not to answer” or “I am not sure” was added to skip them but still collect answers for the rest.

One of the participants actually contacted one of the researches of this thesis, stating that it is controversial to be asked questions about cyber security and after that to request information for the participant’s password (length, wording, content). In his opinion, people who would be willing to answer the questions in this order would be considered naive. However, except this single negative opinion, all other participants were happy to test their security knowledge. Some even wanted feedback on how well they scored.

To battle the uneasiness of participants and researchers, a long period of data collection was allocated - one month. The survey was distributed via e-mail and social media during the active part of the day. Participants were asked to answer the questions in a convenient for them moment, not pressuring them with time restrictions. Additionally, short descriptions were added to every section to provide information about the survey and to ensure that the results will be used only for this study and will not be misused in any way.
4. Results

This section presents the results from the survey. For easy comprehensibility of the 105 responses, this chapter is divided in four parts, representing each section in the survey.

4.1. Personal description

The answers from the “Personal description” section describes the research group the study was conducted in. All of the questions in this section were required, so all of them were answered. A summary of the collected data is presented in Table 3.

Table 3 - Personal description summary

<table>
<thead>
<tr>
<th>Question text</th>
<th>Answers</th>
</tr>
</thead>
<tbody>
<tr>
<td>How old are you?</td>
<td>Minimum value: 15</td>
</tr>
<tr>
<td>You are: (sex)</td>
<td>Men: 67.6%</td>
</tr>
<tr>
<td>Your higher education...</td>
<td>Count of unique values: 66</td>
</tr>
<tr>
<td>Do you have any experience in computer programming (e.g. writing code)?</td>
<td>None 23.8%</td>
</tr>
<tr>
<td>What is your current work position?</td>
<td>Count of unique values: 66</td>
</tr>
<tr>
<td>Do you agree with this stat...</td>
<td>Minimum value: 3</td>
</tr>
</tbody>
</table>

The youngest participant was 15 years old, while the oldest - 56. Most of them were between 23 and 29 years, which makes for a relatively young research group. The majority was male, 67.6% which is normal for a still male-dominant sector, but the female numbers have a significant growth in the last years (Hope, 2018).
The question about education resulted in 66 unique education programmes, with Computer programming being the most common one (27 responses). By chance, the work position question yielded also 66 unique professions. 12 respondents indicated that they work as C#/NodeJS developer, which makes it the most common job title for this study.

There is a real variety of answers when the participants were asked if they had programming skills. Almost half, 48.6%, stated “I have worked/am working as a professional programmer”. Close to a quarter, 23.8%, had no experience at all and the rest are little experienced with the language of computers.

When asked about security habits, in the last question of this section, most participants were reluctant to strongly agree with the given statement. The most commonly selected value was 8 and only 16 participants were 100% sure of their security skills to answer 10.
4.2. Security habits

This section presents the gathered data from which the writers of this thesis made their conclusions. All of the questions are single selection, except one: question 15: “Passwords strength - content”, which is multiple selection. Also, most of the questions have answer type “Other”, so additional comments can be added. A summary of the collected data is presented in Appendix II. To make a short discussion about the results of this section, the questions are separated in 5 groups, categorized by topic.

4.2.1. Personal protection

The first group evaluates the participants’ personal security. It includes the following questions: 7. Antivirus program, 8. Network security system (firewall), 9. Network connectivity 10. Home wireless network. Around 75% of the participants have found a reason to have an antivirus program installed on their computer and a firewall to protect their network. When it comes to public WiFi networks, a little less than two-thirds of the users connect considering the risk. On the other hand, almost 50% have the optimal security on their home networks, including changing default username and password of the router, as well as the use of encryption of the network.

4.2.2. Internet use

Internet is widely spread in modern society and it is one of the main doors for security threats, this is the reason this category is spread throughout the whole survey. It focuses on the participants behaviour online. The questions about 11. Hypertext Transfer Protocol Secure (HTTPS), 12. Downloading data, 18. 2-step verification and 28. Bank card details are in this group. Around 66% of the examined population claim to prefer the use of HTTPS and download data from trusted sources only. The same percentage goes to the use of the 2-step verification. 57.1% never save bank card details online, in websites nor browsers.

4.2.3. Passwords

This category had the goal of acquiring information on people’s habits in creating passwords. It contained 13. Passwords diversity, 14. Passwords strength - length, 15. Passwords strength - content, 16. Passwords strength - wording and 17. Passwords strength - security. For ethical reasons the “Prefer not to answer” option was added, so not all of the 105 participants reply. A
little over of 65% of the participants have thought of passwords which are considered safe. There is room for improvement, but the overall score ensures a good security level.

4.2.4. Use of external storage

This group includes questions 19. Encryption - hard drives, 20. Encryption - Cloud, 21. Old hard drives and 22. Flash drives. It evaluates the participants’ security when storing information on external storage, such as flash drives, hard drives and online (cloud structures). For external storage a safest way to go is the use of encryption. Around 35% of the interviewed use this precaution for their personal hard drives. The percentage is higher for online storage because the responsibility of encryption falls to the company, offering the service and the user chooses to use it. Lastly, the flash drives are regarded as a security risk, around 67% would use only trusted sources or would at least scan them before use.

4.2.5. Carefulness

As stated before, the computer user is the last line of defense in the cyber security war, that is why this last section is devoted to the participants’ attention to security risks. The questions in this section are: 23. Updates, 24. Unauthorized access - hardware, 25. Unauthorized access - software, 26. Wireless connectivity - WiFi and 27. Wireless connectivity - Bluetooth. More than 53% of the questioned users have excellent security habits when it comes to authorized access. These individuals lock their computers when they are not using them and have a dedicated user account for software manipulation. The results from this section also suggest that people would turn off wireless devices like WiFi and Bluetooth, if they are not in use, which minimizes the risk of security breach.
4.3. **E-mail credibility**

This was the last section of the survey and about one-fourth of the participants did not answer the open not required questions. The researchers anticipate that the interviewees would be annoyed if the open questions at the end were required and the answers would not be useful. Nevertheless, most of them submitted useful comments. A summary of the number of responses in the E-mail credibility section is presented in Table 4:

*Table 4 - E-mail credibility section summary*

<table>
<thead>
<tr>
<th>E-mail topic</th>
<th>Real e-mail</th>
<th>Participants answered “Yes”</th>
<th>Participants answered “No”</th>
<th>Participants answered “I am not sure”</th>
<th>Participants justified their answers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compromised Google account</td>
<td>fake</td>
<td>2 (1.9%)</td>
<td>102 (97.1%)</td>
<td>1 (1%)</td>
<td>79 (75.2%)</td>
</tr>
<tr>
<td>US Green card competition</td>
<td>fake</td>
<td>3 (2.9%)</td>
<td>100 (95.2%)</td>
<td>2 (1.9%)</td>
<td>79 (75.2%)</td>
</tr>
<tr>
<td>Microsoft terms of use update</td>
<td>real</td>
<td>51 (48.6%)</td>
<td>39 (37.1%)</td>
<td>15 (14.3%)</td>
<td>71 (67.6%)</td>
</tr>
<tr>
<td>Western union bank transfer</td>
<td>fake</td>
<td>6 (5.7%)</td>
<td>86 (81.9%)</td>
<td>13 (12.4%)</td>
<td>71 (67.6%)</td>
</tr>
</tbody>
</table>

4.3.1. **Compromised Google account**

97.1% of the participants would not interact with this e-mail. Only two individuals answered ”Yes” and one answered ”I am not sure”. Not justifying their answers in the next question, brings the assumption that these three participants have ignored this type of questions. As for the part who answered ”No”, the most obvious warning signals were the suspicious link in the e-mail and the domain it was send from. 57 participants found this signal. The second popular red flag was that people are used to Google’s services and know that the big IT company will not send e-mails without giving more information about the problem at hand, or without styling the letter for a more personal appeal (username, personal e-mail, a link to a specific settings page). The number of interviewees keen on Google was 14. Other indication for phishing included suspicious text, bad design and there were 2 responses from users who already dealt with these kinds of attacks.
4.3.2. US Green card competition

This e-mail had surprisingly 3 positive answers, 2 of which were again ignored because of missing reason for answering this way. However, 1 participant supported his decision on the bases of the reference number in the letter and the ability to contact a specific person via phone. 2 participants responded, “I am not sure”, because they have not applied but would consider following the instructions in the e-mail if they did. Moving on with the “No” answers, again the most noticed warnings were the suspicious links in the text and the shady domain - 23 participants. These signs were closely followed, in number of responses, by the claim of other users that they have not entered the competition at all - 22 participants. Many find the content suspicious, others preferred to contact the local embassy than to interact with the e-mail, some ignored it out of experience. Sadly, only 3 interviewees read through the text carefully (certainly), because they found spelling and grammar mistakes, which made them to be sure of their choice not to interact.

4.3.3. Microsoft terms of use update

About one-third of the respondents (27) felt sure enough that this was a real e-mail from Microsoft. Some (7) still preferred to check the links before clicking them but overall, they felt secured interacting. The uncertain “I am not sure” had highest count from all of the examples and the most doubtful signs were again the domain address and the hidden links in the text. Most of the confident “No”-ers (15) replied that this e-mail is only informative, and no interaction is needed, so they would just ignore it. Only 4 people in this segment believed the e-mail was a fake and did not want to interact with it.

4.3.4. Western union bank transfer

Yet again, the suspicious e-mail addresses the message was sent from was the biggest giveaway the participants have noticed. 24 of them would not interact because of this. Other 14 write that they have not made a transaction, or they do not use Western union at all to receive such an e-mail, so for sure they ignored it. The third most popular warning (9) were the missing of personal details: no design of the e-mail, no transaction number, no personal client name, or even an official way to contact the company. Another 8 participants wrote they preferred to contact the company the official way, e.g. via online banking in the official site, call over the phone or directly in an office. 4 comments from the “Yes” (1) and the “I am not sure” (3)
groups stated that they would consider following the link in the e-mail with caution, provided they have made a transaction in advance.
4.4. Your opinion is important to us

In the final question of the survey participants were asked to say a few words on the topics of “Computer literacy” and “Cyber security”. The responses were 33 in count and they ranged from criticism to encouragement about the survey as a whole. The researchers have managed to group the essential answers in 4 groups:

4.4.1. Criticism

As noted in the Ethical considerations chapter, some participants were reluctant to give answers to the questions concerning their passwords. A user gave feedback that these type of questions will not yield valid answers in this survey. Another has failed to understand the purpose of the survey, criticizing that the survey is missing priorities: “That’s the info that is lacking the most I think. Is it more important to have a safe password or antivirus program installed?” (Anonymous comment, 2018). The creators of the survey should have anticipated this and provided information to educate the user before his participation in the study.

4.4.2. Gratitude

Of course, the comments did not include only criticism. Some participants were grateful for drawing their attention on the topic of cyber security. Many have noticed a gap in their knowledge on security skills and claim that they have gained useful information on how to be more secure. Entering courses on online security has also risen as a topic for discussion. “There are too many people who want to take advantage of unaware users.” (Anonymous comment, 2018).

4.4.3. Suggestions

Participants gave suggestions on how to become more secure. One option is to have a complexity scale for your passwords which corresponds to the amount of personal data in the given profile. Other options like password generators and savers, like LastPass, makes it easier to remember one password and not all of them. There are also different types of hardware and software prevention techniques which render a computer useless until a password is entered. One is disabling all IO ports, like USBs, until login, comments one of the participants. Unfortunately, if it comes to the worst and personal information has leaked out, knowing your rights and how to react are important security skills as well. Overall, cyber security revolves around the balance between convenience and securing your data, there is just “No
system/account [can be] 100% secure” (Anonymous comment, 2018). One user suggested that to be able to have the optimal security you have to do one thing - “stop using the Internet” (Anonymous comment, 2018).

4.4.4. Future considerations

There were commentators who wrote their thoughts on cyber security of the future. One suggested that when quantum computers emerge hacking the “so called secure passwords” (Anonymous comment, 2018) will be done with ease. This is why security measures must evolve as well. A participant commented a solution for this problem - “hardware encryption devices which are in the form of usb stick with fingerprint sensor” (Anonymous comment, 2018). While secured and easy to use, they are still not common to the public.
5. Analysis

When the provided time for data collection ran out, the next step was to analyse the data. Google Forms possess a useful export function, that generates a Google Sheet file (www.sheets.google.com) with all of the results in a table. From there the data can be manipulated for easier processing. To make the process clear and easy to read, each manipulation was in a separate sheet.

Firstly, the participants had to be separated in the programmer and non-programmer groups. In order to be considered as a programmer, an individual had to have either an education in programming, a job in the field of programming or experience in programming. For each of these options there was a question in the survey. An index was assigned to each group: programmer – 1 and non-programmer – 0. These indexes are later used in the additional sheets.

Figure 7 - Representation of analysis process

All of the unique answers (66) for the education question, number 3 in Appendix I, were copied in the Education sheet and an index was assigned to each of them. This splits the participants to programmers and non-programmers according to their field of study. It must be noted, that not all university programs are the same. For example, there is no proof that studying informatics in an economics university is the same as in a technical university in terms of programming. However, the research does not focus on the high level skills in the field, but more on the knowledge of them. Studying the field for 3 years or more is reason enough to believe that an individual should have acquired at least basic programming skills.
All of the unique answers (again 66) for the work position question, number 5 in Appendix I, were copied in the Work position sheet and an index was assigned to each of them, as well. This splits the participants to programmers and non-programmers according to their job title. Like the programs in education, the job descriptions in the IT sector can vary greatly in specifications and responsibility from company to company. As pointed out earlier, people writing code can be described as programmers, or as developers. However, this research does not focus on the description of the job title but the skills it brings, e.g. programming skills.

The experience question, all of the items in the Security habits and half of the E-mail credibility sections were categorical, so they were coded together in the Points sheet. All of the answers were coded with numbers from 0 to 4, depending on the level of security each answer describes (see Table 5 for an example). Codes can be repeated in the same answer set if they carry the same weight/information for the research.

Table 5 - Example of coding an answer set

<table>
<thead>
<tr>
<th>Question: Bank card details</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>I always save my card details online, it is easier to use it this way</td>
<td>0</td>
</tr>
<tr>
<td>I only save my card details online, if I feel the site is trustworthy</td>
<td>1</td>
</tr>
<tr>
<td>I only save my card details on my browser, I trust my browser's development team</td>
<td>2</td>
</tr>
<tr>
<td>I never save my card details online</td>
<td>3</td>
</tr>
<tr>
<td>I do not use bank cards</td>
<td>4</td>
</tr>
<tr>
<td>I am not sure</td>
<td>0</td>
</tr>
</tbody>
</table>

Additionally, the other half of the questions in the E-mail credibility section were open-ended, so they had to be grouped and coded. The E-mails sheet was divided in four sections for each question and this group was divided into sub-groups with short descriptions. Each of them have a code from 0 to 10 and the count of answers that apply for that description. The greater the count the more users agree to that description. This sheet will be mostly used in the Discussion chapter.

Lastly, all of the coded values were transferred into the Coded sheet, where Password and Security scores were calculated. The Password score summed the codes of the questions about the passwords and the Security score - all of the other questions. This yielded in fewer variables
to compare in SPSS Statistics. This separation was made because of “Prefer not to answer” answers in the password questions. Some participants did not want to give this personal information, so the points from these variables had to be excluded from the Security score to ensure correct calculations. Afterwards, the records were filtered from the unwanted answers and Password score was summed. At the end, the two segments were imported into SPSS Statistics. The segment for the Security score included all the 105 records, while the filtered one for the Password score contained 65 items. Figure 7 gives a representation of the whole process until this point.

The authors ran a multiple regression comparing the survey participants scores against their answers determining if they were in the programmers’ or non-programmers’ group. This had to be done twice because of the two segments, mentioned before. The regression with the Security score showed how well the survey participants did in security questions (105 participants) and the one with the Password score - how well the survey participants did in password strength related questions (65 participants).
5.2. Security score

The authors ran multiple regressions using SPSS Statistics with the dependant variable being Security score - integer between 0 and 54 based on the participants answers from the survey and the predictor variables being:

- IsProgrammerEducation - Programming experience from education - boolean value
- IsProgrammerWork - Programming experience from work - boolean value
- IsProgrammerExperience - Programming experience from self taught sources - boolean value

If a participant did not have any programming experience the values off all the predictor variables would have been 0.

*Table 6 - Model Summary output from SPSS Statistics for Security score regression*

<table>
<thead>
<tr>
<th>Model</th>
<th>R</th>
<th>R Square</th>
<th>Adjusted R Square</th>
<th>Std. Error of the Estimate.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>.378</td>
<td>.143</td>
<td>.117</td>
<td>6.673</td>
</tr>
</tbody>
</table>

*Table 7 - Anova output from SPSS Statistics for Security score regression*

<table>
<thead>
<tr>
<th>Model</th>
<th>Sum of Squares</th>
<th>df</th>
<th>Mean Square</th>
<th>F</th>
<th>Sig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regression</td>
<td>749.610</td>
<td>3</td>
<td>249.870</td>
<td>5.612</td>
<td>.001</td>
</tr>
<tr>
<td>Residual</td>
<td>4496.904</td>
<td>101</td>
<td>44.524</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>5246.514</td>
<td>104</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The received R Square value is 14.3% (Table 6) which is low. This is considered normal, because the authors are measuring human behaviour. The conclusions are that the Security score is affected from the predictor variables but to a small degree. Nevertheless, the analysis show that there is statistical significance.

The p value of the regression model is 0.001 (Table 7). The authors’ chosen margin of error is 5%, as the p value 0.001 < 0.05 from this they take away that the regression model statistically significantly predicts the outcome variables.

Looking at the coefficients output (Table 8) the researchers conclude that only the programming experience from self-taught sources contributes statistically significantly to the model as it was the only predictor variable with a p value less than 0.05. IsProgrammerExperience has a p value of 0.001 < 0.05, IsProgrammerEducation has a p value of 0.924 > 0.05 which makes it insignificant and IsProgrammerWork has a p value of 0.956 > 0.05 which also makes it insignificant. From the values in the B column we can take away that people who were in the programming experience from self-taught sources group had higher security score of 5.848 on average.
5.3. Password score

Using SPSS Statistics, a multiple regression was run with the dependent variable being the Password score - integer between 0 and 12 based on the participants answers from the survey and the predictor variables being:

- IsProgrammerEducation - Programming experience from education - boolean value
- IsProgrammerWork - Programming experience from work - boolean value
- IsProgrammerExperience - Programming experience from self-taught sources - boolean value

If a participant did not have any programming experience the values off all the predictor variables would have been 0.

Table 9 - Model Summary output from SPSS Statistics for Password score regression

<table>
<thead>
<tr>
<th>Model</th>
<th>R</th>
<th>R Square</th>
<th>Adjusted R Square</th>
<th>Std. Error of the Estimate.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>.250</td>
<td>.062</td>
<td>.016</td>
<td>1.801</td>
</tr>
</tbody>
</table>

Table 10 - Anova output from SPSS Statistics for Password score regression

<table>
<thead>
<tr>
<th>Model</th>
<th>Sum of Squares</th>
<th>df</th>
<th>Mean Square</th>
<th>F</th>
<th>Sig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Regression</td>
<td>3</td>
<td>4.391</td>
<td>1.354</td>
<td>.265</td>
</tr>
<tr>
<td></td>
<td>Residual</td>
<td>61</td>
<td>3.243</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td>64</td>
<td>3.243</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The regression returned 0.062 for the R square value (Table 9), meaning the Password score is influenced by 6.2% by the three predictor variables. This value is considered extremely low by the authors. At the same time, the p value of the regression model is 0.265 (Table 10) which does not fit into the authors chosen error margin of 5%, as 0.265 > 0.05. From this the authors take away that the regression model does not statistically significantly predict the outcome variables and that there is no significant correlation between the password score and the predictor variables.
5.4. Self-evaluation

Table 11 - Correlation output from SPSS Statistics between Self-evaluation and Security score

<table>
<thead>
<tr>
<th>Correlation</th>
<th>Variable</th>
<th>Property</th>
<th>SelfEvaluation</th>
<th>SecurityScore</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SelfEvaluation</td>
<td>Pearson correlation</td>
<td>1</td>
<td>.466</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sig. (2-tailed)</td>
<td></td>
<td>.000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>N</td>
<td>105</td>
<td>105</td>
</tr>
<tr>
<td></td>
<td>SecurityScore</td>
<td>Pearson correlation</td>
<td>.466</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sig. (2-tailed)</td>
<td>.000</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>N</td>
<td>105</td>
<td>105</td>
</tr>
</tbody>
</table>

Table 11 shows a correlation between the Self-evaluation and Security score variables: \( r = 0.466 \). It is based on \( N = 105 \) participants and its 2-tailed significance, \( p = 0.000 \), which is less than the chosen margin of error \( (0.000 < 0.05) \), thus the correlation is statistically significant. This indicates that if the Security score rises, so will the self-assessment. The people from the research group have a good idea of their security knowledge. However, from the weak correlation the authors presume that the participants are not so keen on their abilities to consider themselves secure.
6. Conclusion

This chapter is going to present the final conclusions of this thesis and answer the research questions, posed in chapter 1.2.

What are the basic skills for an employee in the IT sector?

Through an extensive literature review, the authors of this thesis have found out that basic skills in the IT sector cannot be defined easily because of the variety of job responsibilities. The problem exists because in the field of IT there are numerous job descriptions that require different skill sets and levels of computer skills are extremely different. However, this research has proved that every IT professional must have security skills. The computer users must know how to protect themselves from threats and how to react, if information has leaked out. Protection habits, like antivirus scans of the system, firewall on the network, checking external drives for viruses, recognizing phishing attempts in e-mails and etc. are all important and fundamental abilities for the modern user. Being the last line of defence in the world of cyber security, the users must possess security literacy to be able to bear this responsibility.

What affects a user’s computer literacy more: having an education in programming, being employed as a programmer or having programming experience?

In this research two variables were used to measure computer literacy: Security score and Password score. As for examining the programming knowledge, the writers of this thesis recognize three ways of acquiring it: by studying it in an university, by working in the designated field or by being self-taught. The research findings show an increase of the Security score if the participant has programming skills. This proves there is a positive outcome from having programming knowledge. The Password score was barely affected by the programmer variables in the analysis. This means programmers do not have any advantage over the typical user when creating a password. This can be explained with the tightened security of today’s sites and platforms. Most of them, if not all, require long passwords (at least 8 characters) with a combination of small letters, capital letters, numbers and symbols. This could be the reason for evening up the field of password security between the two groups. From this, the authors deduce that learning programming has a significant positive effect on computer literacy, in the field of cyber security.

How do people from the IT sector assess their computer literacy?
In chapter 6.3 the authors acknowledged a positive connection between the security skills people have and their self-evaluation of those skills. The higher the score of the security skills the higher people assess themselves. It is noted that the connection is not strong, but this can be explained again with the ambiguous IT sector which is constantly changing. Overall, the researchers conclude that people have a good estimation of their computer literacy when it comes to security and this slight hesitation is useful for future considerations.
7. Discussion

7.1. Methods and results discussion

Initially, this study had to be done on a bigger scale, evaluating not only security habits but also hardware maintenance, simple document and spreadsheet manipulation and other types of computer skills. Sadly, upon exploring the so-called basic computer skills, the researchers came to the realization that (1) the scope in which they wanted to perform the research was immense and (2) the skills they wanted to assess cannot be considered basic for every person. Both had to be limited in some way in order to make them measurable.

Therefore, the research group was narrowed down from the initial scope, Estonians and Bulgarians (from any field), to the IT sectors of the two countries. The authors wanted to examine computer literacy on the best representatives there is, so they turned to the experienced users, the employees of the IT sector.

Next, the basic computer skills needed to be defined. Upon further investigation, all the sources on the topic pointed out that security is really an important part of the IT world. Every examined article included the importance of online and offline protection.

Thus, the authors of this thesis performed a quantitative research, surveying people from the IT sector about security habits. Thanks to platforms like Google Forms, creating the questionnaire and collecting data was easy and fast, but the authors struggled with the analysis of the data. Sadly, the analysis did not yield concrete results on which to back up the answers for the research questions. The connections between the Security/Password score and the programmer variables was expected to be higher, but it only showed statistical significance. The programmer variables affected the Security score by 14.3% and the Password score by only 6.2%, values which are not high enough for a 100% conclusive research. Nevertheless, the authors have contributed to the research gap of computer literacy and future studies may build up on it.
7.2. Security awareness

As discussed earlier, most computer users are not aware of the security threats in today’s technological world, both at home and at work (Hall, 2016). Each new service or product an individual uses acquires information about him or her. The problem here is that most do not know what kind information is acquired and how it is used (Arlitsch & Edelman, 2014). This creates possibilities for misuse from the service provider or for abuse from a hacker.

The authors of this thesis have not found a way to evaluate if people have become more cybersecurity aware or not. However, the comparison between the programmers’ and non-programmers’ groups show that the first group is more educated on the matter, making them more vigilant for suspicious activity. Overall, studies show that the IT sector itself has tightened security to ensure the users’ safety. Precautions like online safety awareness campaigns, enforced use of stronger passwords and periodic changing, 2-step verification, antivirus programs, security protocols, encryption, etc. (Valcke et al., 2011; Donovan & Bernier, 2009) keep you safe but a breach is always possible in the ambiguous world of IT.
7.3. Future research

After the authors conducted a self-evaluation, there was a realization of a model which they followed, writing this thesis:

1. Find a measurable field - find at least one right way to go about a field and that right way is measurable.
2. Find a representative of this field, who is considered to have the most knowledge in it.
3. Learn the representative’s knowledge.
4. Teach the representative’s knowledge to the regular users to raise their skill level.
5. Repeat step 1-4 in different fields to raise computer literacy level.

This thesis covered points 1 to 2. The authors chose the topic of security as it was not individually based and has truths that work overall, which can be measured and managed to statistically prove that the people who were observed to have programming experience had better security habits. To build on the work done in this paper, the logical next step would be to figure out more in detail what makes the people with programming skills better at their security habits than their counterparts. Segmenting down on this should lead to a more precise description of a power user e.g. it might be that a back-end developer has better security habits than a front-end one or a person who works with a specific programming language has a higher security skill.

When that power user is better identified the authors would suggest a goal to find out what parts of their knowledge leads to a higher security score. In hopes to generate a short list of knowledge fragments which could be thought to a non-power user in a reasonable time to produce maximum positive affect on their security habits. From here again the logical next step would be to test if that short list of knowledge fragments actually raises the security level of a regular user.

The authors also believe that the research done in this paper could be easily be replicated on a different computer literacy topic other than security. The key problem they faced was how to measure the effects as by definition computer literacy is meant to satisfy an individual’s personal needs and as the needs are individual some criteria has to be found to judge what is good or bad in a specific field. But the authors believe more topics that would suit this type of a research surely exist.
8. References


9. Appendix I - The survey

The live survey can be found on this link: https://goo.gl/forms/6cqavNrW44id5ZH83

Computer literacy - do you have what it takes to be cyber secure?

Thank you for participating in this survey. It is absolutely anonymous and will take about 15 minutes.

Your answers are going to be used to make an assessment of the participants' computer literacy, more specifically their knowledge, skills and habits in cyber security.

The goal of this study is to evaluate if people are educated enough to discover, reduce and protect themselves from online threats and other breaches. Also, we aim to find out if some background in programming (writing code) helps to be more educated in the field of security. The end results depend on your honest answers.

* Required

Personal description

In this section we want to know a little about you, so we are going to ask you few personal questions.

1. How old are you? *

Example: 25

2. You are: *

Mark only one oval.

- Male
- Female
- Prefer not to say

3. Your higher education is/was in the field of: *

Example: Computer science, Business administration, etc. (multiple inputs are possible)

4. Do you have any experience in computer programming (e.g. writing code)? *

Mark only one oval.

- None
- I have worked on a few side projects, for myself
- I have worked on a few side projects, that are published and open for the public
- I have worked/am working as a professional programmer
- Other:

5. What is your current work position? *

Example: WEB developer, Business services specialist, IT project manager, etc. (multiple inputs are possible)
6. Do you agree with this statement: "I am aware of the security risks using a computing device (e.g. computer, smartphone, tablet, etc.) and I have good computer security habits to prevent them"? *

\[ \text{Mark only one number.} \]

1 2 3 4 5 6 7 8 9 10

Strongly disagree Strongly agree

Security habits

In this section we would like you to answer with the statement that best describes your current behavior regarding the topic in question.

7. Antivirus program *

\[ \text{Mark only one oval.} \]

- I do not have one
- I do not have one and I know that I do not need one
- I have it
- I have it and I know what it does
- I have it and I know how it works
- I am not sure

8. Network security system (firewall) *

\[ \text{Mark only one oval.} \]

- I do not have one
- I do not have one and I know that I do not need one
- I have it
- I have it and I know what it does
- I have it and I know how it works
- I am not sure

9. Network connectivity *

\[ \text{Mark only one oval.} \]

- I use most WiFi networks without hesitation (even if I do not know who the owner is)
- I use public WiFi networks only after I have verified them
- I use public WiFi networks only with a VPN
- I use only private WiFi networks
- I am not sure

10. Home wireless network *

\[ \text{Mark only one oval.} \]

- I do not use a wireless network at home
- My wireless network name and/or password are the factory defaults
- I have set my own name and password for my home wireless network
- I have set my own name and password for my home wireless network and I know my router uses encryption
- I am not sure

11. Hypertext Transfer Protocol Secure (HTTPS) *

\[ \text{Mark only one oval.} \]

- I do not know what HTTPS is and how to know if I am currently using it
I do not know what HTTPS is but I know when I am using it
I know what HTTPS is but I am not sure when I am using it
I know what HTTPS is and using it is essential for me

12. Downloading data *

Mark only one oval.

I do not pay attention from where and from whom I download data from the Internet
I download data from non-trusted sources but scan it for security threats
I only download data from trusted sources
I only download data from a trusted source and I try to verify the legitimacy of the source and sender

13. Passwords diversity *

Mark only one oval.

I use the same password for most services
I use an array of passwords for most services (different passwords with same structure)
I use a different password for every service
I use a password manager (auto-generated password)

14. Passwords strength - length *

Mark only one oval.

My passwords are mostly less than 8 characters
My passwords are mostly between 9 - 16 characters
My passwords are mostly over 17 characters
Prefer not to answer

15. Passwords strength - content *

Check all that apply.

☐ My passwords contain small letters
☐ My passwords contain capital letters
☐ My passwords contain numbers
☐ My passwords contain symbols (if possible)
☐ Prefer not to answer

16. Passwords strength - wording *

Mark only one oval.

My passwords are mostly composed of human readable words
My passwords are mostly composed of human encrypted words (e.g: password is written as pa??w0rd)
My passwords are described as gibberish (completely random characters)
Prefer not to answer
Other:

17. Passwords strength - security *

Mark only one oval.

I have my passwords written down in a physical form but I am not sure where
I have my passwords written down in a physical form and I know where they are
I have all my password memorized
Prefer not to answer

18. 2-step verification *

Mark only one oval.

I do not know what 2-step verification is
● I know what 2-step verification is but I do not use it
● I use 2-step verification wherever it is possible

19. Encryption - hard drives *

*Mark only one oval.*

● Most of my devices' hard drives are not encrypted
● Most of my devices' hard drives are encrypted
● I am not sure

20. Encryption - Cloud *

*Mark only one oval.*

● Most of the cloud services I use, do not use encryption
● Most of the cloud services I use, use encryption
● I am not sure

21. Old hard drives *

*Mark only one oval.*

● I do not know where my old hard drives are and in what condition they are
● I have stored my old hard drives in a safe place
● I have wiped or destroyed all my old hard drives
● I do not have any old hard drives
● I am not sure

22. Flash drives *

*Mark only one oval.*

● I just use flash drives, I do not consider them as a security risk
● I just use flash drives and believe my antivirus program will protect me
● I always check the flash drive for malware before I use it
● I only use flash drives from trusted sources
● I am not sure

23. Updates *

*Mark only one oval.*

● I do not update my operating system and programs/apps
● I update my operating system and programs/apps from time to time
● I update my operating system and programs/apps as soon as possible
● I am not sure

24. Unauthorized access - hardware *

*Mark only one oval.*

● When I leave my computer unattended, I do not lock it, log out or turn it off
● When I leave my computer unattended, I lock it, log out or turn it off only in public places (e.g. work, university, cafe)
● When I leave my computer unattended, I always lock it, log out or turn it off
● I am not sure

25. Unauthorized access - software *

*Mark only one oval.*

● On most of the devices, I only use one account with administrative privileges
● On my device, I only use a personal account for daily use and a separate one with administrative privileges
● On my device, I only use a personal account which does not have administrative privileges
● I am not sure

26. Wireless connectivity - WiFi *

*Mark only one oval.*

● My devices do not support WiFi/I do not use WiFi
● My WiFi is always turned on
● My WiFi is turned on only when I need it
● I am not sure

27. Wireless connectivity - Bluetooth *

*Mark only one oval.*

● My devices do not support Bluetooth/I do not use Bluetooth
● My Bluetooth is always turned on
● My Bluetooth is turned on only when I need it
● I am not sure

28. Bank card details *

*Mark only one oval.*

● I always save my card details online, it is easier to use it this way
● I only save my card details online, if I feel the site is trustworthy
● I only save my card details on my browser, I trust my browser's development team
● I never save my card details online
● I do not use bank cards
● I am not sure

E-mail credibility

In this section we will show you a few e-mails. Would you consider to interact to these e-mails (e.g. reply, follow the instructions in it or click a link from it)?

29. If you receive this e-mail, would you interact with it? *

Bigger size image (opens in new tab):
https://drive.google.com/open?id=1gE6Hpz9rB9SppDM_AAoWnCynf_YmfAe
Mark only one oval.

- Yes
- No
- I am not sure

30. Please explain your choice with a few words.


31. If you receive this e-mail, would you interact with it? *

Bigger size image (opens in new tab):
https://drive.google.com/open?id=17tEzVO42DDF8iM3xg6MxZxo2P9IdPaJT

Mark only one oval.

- Yes
- No
- I am not sure

32. Please explain your choice with a few words.


33. If you receive this e-mail, would you interact with it? *

Bigger size image (opens in new tab):
https://drive.google.com/open?id=1CnZnfHWKBM4D70Y9R20mawvgpxfjXjc4
Mark only one oval.

- Yes
- No
- I am not sure

34. Please explain your choice with a few words.

35. If you receive this e-mail, would you interact with it? *

Bigger size image (opens in new tab):
https://drive.google.com/open?id=1dopFiMXA_lhYDb9DMpV91DDPRPOqWovH
Mark only one oval.

- Yes
- No
- I am not sure

36. Please explain your choice with a few words.

Your opinion is important to us

Lastly, we want to know if we have mist to ask you something.

37. Is there anything more you would like to say on the topics of Computer literacy or Cyber Security?
10. **Appendix II - Results from the survey: section “Security habits”**

<table>
<thead>
<tr>
<th>Question</th>
<th>Answers</th>
<th>Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>7. Antivirus program</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I do not have one</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(12.4%)</td>
</tr>
<tr>
<td></td>
<td>I do not have one and I know that I do not need one</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(13.3%)</td>
</tr>
<tr>
<td></td>
<td>I have it</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(12.4%)</td>
</tr>
<tr>
<td></td>
<td>I have it and I know what it does</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(31.4%)</td>
</tr>
<tr>
<td></td>
<td>I have it and I know how it works</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(25.7%)</td>
</tr>
<tr>
<td></td>
<td>I am not sure</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(4.8%)</td>
</tr>
<tr>
<td></td>
<td><strong>8. Network security system (firewall)</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I do not have one</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(11.4%)</td>
</tr>
<tr>
<td></td>
<td>I do not have one and I know that I do not need one</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(1%)</td>
</tr>
<tr>
<td></td>
<td>I have it</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(14.3%)</td>
</tr>
<tr>
<td></td>
<td>I have it and I know what it does</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(29.5%)</td>
</tr>
<tr>
<td></td>
<td>I have it and I know how it works</td>
<td>37</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(35.2%)</td>
</tr>
<tr>
<td></td>
<td>I am not sure</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(8.6%)</td>
</tr>
<tr>
<td></td>
<td><strong>9. Network connectivity</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I use most WiFi networks without hesitation (even if I do not know who the owner is)</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(31.4%)</td>
</tr>
<tr>
<td></td>
<td>I use public WiFi networks only after I have verified them</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(29.5%)</td>
</tr>
<tr>
<td></td>
<td>I use public WiFi networks only with a VPN</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(2.9%)</td>
</tr>
<tr>
<td></td>
<td>I use only private WiFi networks</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(34.3%)</td>
</tr>
<tr>
<td></td>
<td>I am not sure</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(1.9%)</td>
</tr>
<tr>
<td></td>
<td><strong>10. Home</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I do not use a wireless network at home</td>
<td>4</td>
</tr>
<tr>
<td>wireless network</td>
<td>(3.8%)</td>
<td>(11.4%)</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>--------</td>
<td>---------</td>
</tr>
<tr>
<td>My wireless network name and/or password are the factory defaults</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>I have set my own name and password for my home wireless network</td>
<td>37</td>
<td></td>
</tr>
<tr>
<td>I have set my own name and password for my home wireless network and I know my router uses encryption</td>
<td>51</td>
<td></td>
</tr>
<tr>
<td>I am not sure</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>11. Hypertext Transfer Protocol Secure (HTTPS)</th>
<th>(7.6%)</th>
<th>(8.6%)</th>
<th>(18.1%)</th>
<th>(65.7%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>I do not know what HTTPS is and how to know if I am currently using it</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I do not know what HTTPS is but I know when I am using it</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I know what HTTPS is but I am not sure when I am using it</td>
<td>19</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I know what HTTPS is and using it is essential for me</td>
<td>69</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>12. Downloading data</th>
<th>(10.5%)</th>
<th>(23.8%)</th>
<th>(44.8%)</th>
<th>(21%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>I do not pay attention from where and from whom I download data from the Internet</td>
<td>11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I download data from non-trusted sources but scan it for security threats</td>
<td>25</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I only download data from trusted sources</td>
<td>47</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I only download data from a trusted sources and I try to verify the legitimacy of the source and sender</td>
<td>22</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>13. Passwords diversity</th>
<th>(16.2%)</th>
<th>(41%)</th>
<th>(21.8%)</th>
<th>(21%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>I use the same password for most services</td>
<td>17</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I use an array of passwords for most services (different passwords with same structure)</td>
<td>43</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I use a different password for every service</td>
<td>23</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I use a password manager (auto-generated password)</td>
<td>22</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>14. Passwords strength - length</th>
<th>(14.3%)</th>
<th>(52.4%)</th>
<th>(15.2%)</th>
<th>(19%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>My passwords are mostly less than 8 characters</td>
<td>15</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>My passwords are mostly between 9 - 16 characters</td>
<td>55</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>My passwords are mostly over 17 characters</td>
<td>16</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prefer not to answer</td>
<td>19</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15. Passwords strength - content (multiselection)</td>
<td>My passwords contain small letters</td>
<td>83 (79%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>My passwords contain capital letters</td>
<td>78 (74.3%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>My passwords contain numbers</td>
<td>83 (79%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>My passwords contain symbols (if possible)</td>
<td>55 (52.4%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Prefer not to answer</td>
<td>14 (13.3%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16. Passwords strength - wording</td>
<td>My passwords are mostly composed of human readable words</td>
<td>27 (25.7%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>My passwords are mostly composed of human encrypted words (e.g: password is written as pa??w0rd)</td>
<td>17 (16.2%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>My passwords are described as gibberish (completely random characters)</td>
<td>34 (32.4%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Prefer not to answer</td>
<td>21 (20%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Other</td>
<td>6 (5.7%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17. Passwords strength - security</td>
<td>I have my passwords written down in a physical form but I am not sure where</td>
<td>1 (1%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I have my passwords written down in a physical form and I know where they are</td>
<td>15 (14.3%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I have all my password memorized</td>
<td>71 (67.6%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Prefer not to answer</td>
<td>18 (17.1%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18. 2-step verification</td>
<td>I do not know what 2-step verification is</td>
<td>9 (8.6%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I know what 2-step verification is but I do not use it</td>
<td>24 (22.9%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I use 2-step verification wherever it is possible</td>
<td>72 (68.6%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19. Encryption - hard drives</td>
<td>Most of my devices’ hard drives are not encrypted</td>
<td>49 (46.7%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Most of my devices' hard drives are encrypted</td>
<td>36 (34.3%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I am not sure</td>
<td>20 (19%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20. Encryption - Cloud</td>
<td>Most of the cloud services I use, do not use encryption</td>
<td>14 (13.3%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Most of the cloud services I use, use encryption</td>
<td>50 (47.6%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I am not sure</td>
<td>41 (39%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21. Old hard drives</td>
<td>I do not know where my old hard drives are and in what condition they are</td>
<td>18 (17.1%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I have stored my old hard drives in a safe place</td>
<td>1 (1.1%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I have wiped or destroyed all my old hard drives</td>
<td>27 (25.7%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I do not have any old hard drives</td>
<td>38 (36.2%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I am not sure</td>
<td>21 (20%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>22. Flash drives</td>
<td>I just use flash drives, I do not consider them as a security risk</td>
<td>7 (6.7%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I just use flash drives and believe my antivirus program will protect me</td>
<td>27 (25.7%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I always check the flash drive for malware before I use it</td>
<td>11 (10.5%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I only use flash drives from trusted sources</td>
<td>50 (47.6%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I am not sure</td>
<td>10 (9.5%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>23. Updates</td>
<td>I do not update my operating system and programs/apps</td>
<td>3 (2.9%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I update my operating system and programs/apps from time to time</td>
<td>44 (41.9%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I update my operating system and programs/apps as soon as possible</td>
<td>56 (53.3%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I am not sure</td>
<td>2 (1.9%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>24. Unauthorized access - hardware</td>
<td>When I leave my computer unattended, I do not lock it, log out or turn it off</td>
<td>7 (6.7%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>When I leave my computer unattended, I lock it, log out or turn it off only in public places (e.g. work, university, cafe)</td>
<td>33 (31.4%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>When I leave my computer unattended, I always lock it, log out or turn it off</td>
<td>64 (61%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I am not sure</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>25. Unauthorized access - software</td>
<td>On most of the devices, I only use one account with administrative privileges</td>
<td>68 (64.8%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>On my device, I only use a personal account for daily use and a separate one with administrative privileges</td>
<td>16 (15.2%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>On my device, I only use a personal account which does not have administrative privileges</td>
<td>13 (12.4%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I am not sure</td>
<td>8 (7.6%)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| 26. Wireless connectivity - WiFi | My devices do not support WiFi/I do not use WiFi | 0 (0%) |
| | My WiFi is always turned on | 46 (43.8%) |
| | My WiFi is turned on only when I need it | 58 (55.2%) |
| | I am not sure | 1 (1%) |

| 27. Wireless connectivity - Bluetooth | My devices do not support Bluetooth/I do not use Bluetooth | 10 (9.5%) |
| | My Bluetooth is always turned on | 14 (13.3%) |
| | My Bluetooth is turned on only when I need it | 79 (75.2%) |
| | I am not sure | 2 (1.9%) |

| 28. Bank card details | I always save my card details online, it is easier to use it this way | 3 (2.9%) |
| | I only save my card details online, if I feel the site is trustworthy | 30 (28.6%) |
| | I only save my card details on my browser, I trust my browser's development team | 7 (6.7%) |
| | I never save my card details online | 60 (57.1%) |
| | I do not use bank cards | 4 (3.8%) |
| | I am not sure | 1 (1%) |