Hermanni Mäkitalo

MEASURING USERS' LEVEL OF INFORMATION SECURITY AWARENESS – RESEARCH AND DEVELOPMENT OF SAMPLE QUESTIONS

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2017

TIIVISTELMÄ

Mäkitalo, Hermanni
Measuring users' level of information security awareness – research and development of sample questions
Jyväskylä: Jyväskylän yliopisto, 2017, 60 s.
Tietojenkäsittelytiede, pro gradu -tutkielma
Ohjaaja: Siponen, Mikko

Tämän gradun tarkoituksena on käsiteanalyysin avulla hahmottaa tärkeimpiä omaisuuksia tietoturvatietoisuudesta ja tavoista levittää sitä, tutustua niihin tarkemmin, ja muodostaa näistä perusteltuja ja käyttäjille olennaisia kysymyksiä joilla selvittää käyttäjän tietoturvatietoisuutta. Aiheen tarkempi läpikäynti on tärkeää, sillä aiemmissa tutkimuksissa on havaittu, että käyttäjät kertovat noudattavansa tietoturvapolitiikoita, vaikka tarkemmin tutkittaessa eivät tienneet tai ymmärtäneet tietoturvapolitiikoiden sisältöä. Kysymysten muodostamisessa otetaan huomioon myös muita käsiteanalyysi vaiheessa selvinneitä piirteitä, joilla tehdä kysymyksistä parempia. Tuloksena esitetään 20 esimerkkikysymystä, sekä ehdotuksia kysymysten muodostamiseen sekä niiden käyttämiseen.

Asiasanat: Tietoturvatietoisuus, tietoturva, käsiteanalyysi

ABSTRACT

Mäkitalo, Hermanni
Measuring users' level of information security awareness – research and development of sample questions
Jyväskylä: University of Jyväskylä, 2017, 60 p.
Information Systems, Master's Thesis
Supervisor: Siponen, Mikko

The purpose of this thesis is to develop questions to measure level of users' understating of information security awareness. Researching the subject is important, because earlier studies have discovered that users who respond positively to questions about whether they follow information security policies might not actually even know what those policies consist of, which may be result of not understanding them. This is achieved by using concept analysis to identify features of information security awareness, which are then studied further to gain better understanding of whether they are relevant for users or not, and to make well-argued questions. We will also utilize other identified ways to make questions better. Thus, we will present 20 example questions, and suggestions on how to develop them to achieve best results.

Keywords: information security awareness, information security, concept analysis

FIGURES

TABLES

TABLE OF CONTENTS

1 INTRODUCTION

According some predictions, world will change more and faster than it has changed in the past. Insight by Accenture predicts that retail will change more in next 5 years than it has changed it past 50 years (Donnelly & Scaff, 2016), and chairman of Lloyds Banking Group stated that banking industry will face more changes in next 10 years than in past 200 years (Treanor, 2014). Banking and retail have both moved Internet. It is common these days to do your purchases and handle all your banking needs online. Teens spend about 9 hours a day using social media (Common Sense, 2015) and almost everyone in western world has smart phone today. In 4 years from 2011 to 2015, amount of Americans who own smartphone has risen from 35% to 64% (Pew Research Center, 2015).

Internet, digitalization and security walk hand in hand. Modern day bank robbers don't march to bank guns blazing, but instead they rob millions to billions from central banks (Telegraph Reporters, 2016) or use banking trojans to steal credentials from common people (Criscione, Bosatelli, Zanero, & Maggi, 2014). Banking credentials are not the only valuable information asset that the criminals are after. Even normal everyday information such as names, addresses, phone numbers and family information can help criminals to create fake identities to create credit cards and take loans under victims' identity, or even to shift blame to some innocent person by using their identity to break the law.

Where banks have task to keep their online banking systems running and secure, users should keep their end up too. Information security affects us all. It can be most easily seen only as creating strong and secure passwords and running anti-virus software, but it is much more than that. Every decision we do online is affected by our knowledge and understanding of information security.

Purpose of this research is to research the topics information security (IS) and information security awareness (ISA), analyze those two key terms, find related concepts that are most relevant to users, and finally develop list of 12 preliminary questions that could be used to measure users' information security awareness. Information security is ample topic, so in this research we focus on topics that users can commonly encounter and may have problems with. We try

to keep discussed aspects relevant to users, but still address the important issues.

Information security awareness training and education is argued to be essential for organizations to be stable and secure (Brodie, 2009). There is always room to improve reliability and validity when measuring complicated concepts such as information security or information security awareness. We argue that by studying previous research and identifying topics and notably studied subjects, we can identify the most hazardous pitfalls of the users', and by studying those more profoundly, we can create questions that may help to verify if such gap in knowledge or understanding exists. This can then provide information about users' knowledge about the most critical and severe aspects of information security that they can affect. For example, if we ask user whether their password is strong, and they answer yes, does that tell us anything about the actual strength of the password, or just about users understanding of what the good are passwords made of? They could think that their mother's maiden name is good password, because who in their right mind would guess that. They don't know, or fail to understand, that passwords are being cracked with programs guessing possibly millions of possibilities per second, instead of some shady person typing guesses one by one at some basement with green glow.

1.1 Research problem

The main research problem is to develop questions to measure users' level of information security awareness. The sub problem is to identify topics that would be most relevant for users' while also being critical enough to pose danger for the users themselves and the organization they belong to. To achieve this, we will utilize concept analysis that is described in chapter 2.

While we will most likely unravel many subjects by researching previous studies, we aim to focus on most relevant and dangerous issues, and write them open clearly. There are dozens of potential dangers that users face every day that we must choose from, and we aim to justify our selections in each sub chapter. There is thin line between explaining issue thoroughly and going unnecessarily deep in subject, which is something we must keep in mind. For example, we explain why connecting to WEP protected Wi-Fi network is bad practice, and why WPA2 protected networks are more secure. We must go quite deep to explain the differences, but explaining things to the depth of Open Systems Interconnection model (OSI model) would be superfluous in this context.

1.2 Prior research

While a lot of studies have been made concerning information security awareness, we found very few papers about developing questions to measure users' information security awareness. A lot of research has been done concerning issues related to ISA, for example concerning passwords, their memorability (Vu et al., 2007; Yan, Blackwell, Anderson, & Grant, 2004), how to get users to use better passwords (Campbell, Kleeman, & Ma, 2011; Gehringer, 2002; Shay et al., 2010), handling multiple passwords (Gaw & Felten, 2006; Grawemeyer & Johnson, 2011) and password security in general (Barton & Barton, 1984; Florencio & Herley, 2007; Florêncio, Herley, & Coskun, 2007; Klein, 1990). We found one paper about developing users' information security awareness questionnaire (Velki, Solic, & Ocevcic, 2014), but the paper was still titled as an ongoing work. We found also paper about determining level of information security awareness level in an organization by Bashorun, Worwui and Parker, in which they found and suggest, among other things, that ISA education should be tailored for the audience. (Bashorun, Worwui, & Parker, 2013) They end their study by stating that "In conclusion, the major steps for any organization in terms of good information security are awareness, awareness and awareness.", which we take as a need to study the information security awareness further.

Many companies offer information technology security awareness training, and SANS, PCI Security Standards Council, and NIST all have documents explaining how to build an information technology security awareness and training program (Brodie, 2009; NIST, 2003; Security Standards Council, 2014). We argue that there exists need for research to analyze of which components the questions should be formed from to maximize that they more comprehensively measure what they are supposed to be measuring, instead of asking random technical questions. This will help training to be more precise and results of testing users understanding more reliable.

The main point of information security awareness training is to namely raise awareness about information security. This is achieved through information, education, and training. Simple example is that without awareness about different types of scams, and that there even exist scams, classical Nigerian prince –scam might sound very alluring, sending 5,000.00 euros to royal person and to receive millions for helping them. No matter what their cause to give the money would be, be it greed or willingness to help person in distress, they would end up scammed out of their money. There has been studies about information security awareness approaches and raising methods (see e.g., Puhakainen, 2006; Wood, 1995), and about how to improve users' information security awareness through different approaches (see e.g., Albrechtsen & Hovden, 2010; Amankwa, Loock, & Kritzinger, 2016; Jama, Siraj, & Kadir, 2014; Monk, Van Niekerk, & Von Solms, 2010). Studies about ISA have also been made in field of determining ISA level in an organization (see e.g., Bashorun, Worwui, & Parker, 2013), the need for ISA programs (see e.g., Aloul, 2010;

Straub & Welke, 1998), and about users' individual factors (see e.g., Farooq, Isoaho, Virtanen, & Isoaho, 2015).

1.3 Motivations

There is need for study to develop better questions to measure whether users understand to what they are answering on. In 2014, Siponen and Vance surveyed employees and found that many agreed to questions like "I comply with information security policies", even though when tested, they failed to answer multiple-choice questions correctly (Siponen & Vance, 2014). This can result in distorted results in questionnaires and studies if not taken in account.

Knowledge and expertise gained in work seems to transfer to home (Talib, Clarke, & Furnell, 2010), which in turn leads little by little to a more secure society. It is important for scholars and practitioners to understand what users don't understand, to better adjust their training to fit their shortcomings. We already know that training should be relevant to users interests and tasks (Siponen & Puhakainen, 2010; Talib et al., 2010), but it should be great help when designing training to know how well the audience generally understands about information security, so the training can be adjusted to be more advanced or elementary.

We have also personal interest in this subject, as we are coming from software development field, and have seen that even those who normally might be perceived as technically savvy users, may have strange gaps in their knowledge and understanding. We are looking forward to take the results back in to the field.

1.4 Defining important keywords

When we speak about information security awareness, it is useful to first define what we mean when we speak of information security. Information security is often pictured to consist of confidentiality, integrity, and availability. This is commonly referenced as CIA-triad. According to Cherdantseva and Hilton, CIA-triad was coined by Johnson Space Center, USA in 1986-1987, but it was first presented by Saltzer and Schroeder back in 1975. (Cherdantseva & Hilton, 2013a) In this context, confidentiality can be defined as protection from unauthorized information release, integrity as protection from unauthorized information modification, and availability as protection from unauthorized denial of use. This or similar definition is used by many scholars (e.g., Fuchs, Pernul, & Sandhu, 2011, p. 748; Reid & Van Niekerk, 2014, p. 2). The same CIA-triad and similar definition is also used in jurisprudence and law (e.g., *44 U.S. Code § 3542*, n.d.) NIST glossary of key information security terms defines information security as "the protection of information and information systems from unauthor-

ized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."(NIST, 2013), which also bases on CIA-triad and is very similar to other definitions. Cherdantseva and Hilton define Information Security as "a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security countermeasures of all available types (technical, organizational, human-oriented and legal) in order to keep information in all its locations (within and outside the organization's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destructed, free from threats."(Cherdantseva & Hilton, 2013b), which is also in line with previous definitions. Information security awareness itself is defined and gone through carefully in chapter 2.

Rootkits are malicious programs, that try to try to hide malware in different ways and sustain the access to the system through various means. (NIST, 2013) Rootkits can operate on multiple different levels, basically either on user level or kernel level, where user level rootkits have less rights than kernel level, and are easier to detect and remove. While kernel level rootkits are much harder to detect, and have much more capabilities than user level rootkits, they are also harder to develop and may cause operating system to become unstable, and thus possibly exposing the rootkit.

Heuristic scans are additional scanning method commonly used by anti-malware applications with regular fingerprint scanning to detect viruses and other malwares. Heuristic detection engines use data mining and machine learning to learn the behavior of the file. (Bazrafshan, Hashemi, Fard, & Hamzeh, 2013) They look for patterns in behavior, which means they can identify malware that has never even been seen before, if it behaves closely enough like another existing malware. This however may result in false alarms, as some legitimate programs may have some similar characteristics as some malware.

Human interface devices (HID) are devices that take input from humans and direct it to the computer. HID here will more specifically refer to USB-HID specification, since it is most common for normal users, and modern computers have been moving from PS/2 ports to USB-ports. Most common HID's associated with computers are keyboard and mouse, which are at present generally connected by universal serial port (USB) port.

2 CONCEPT ANALYSIS

This chapter goes through the selected research method, the objective of the analysis, history and actual analysis of the main concept, and identification of the related concepts. The process of concept analysis is explained in chapter 2.1, while the actual analysis can be found on chapter 2.4. Keeping the research problem in mind, the main concept was chosen to be information security awareness, as it was deemed to be most relevant and descriptive when thinking about how much users understand about information security. Concept analysis gives us some freedoms to focus more on the parts that are more essential in terms of research problem, so for example, we will focus more on the identification of features and examining the related concepts, than steps 5, 7, and 8. All the steps can be seen on the figure 1.

2.1 About concept analysis

As stated before, in this research we will utilize concept analysis as research method. The main paper used as guidance in this research is a paper by Puusa (2008), in which she describes the history and significance of the concept analysis as scientific method, as well as the actual steps and phases of the method. The steps or phases are not her handwriting, but from a book by Walker and Avant from 1988, in which they reformed steps originally developed by Wilson (1969). While concept analysis is often used in business studies and in nursing sciences, it is can be used in other fields of study as well, if the subject is mature enough and there is enough material to study.

FIGURE 1 Steps of the concept analysis

The concept analysis was selected because it was deemed most befitting, as there exists good amount of research relating the main concept, the researcher had existing knowledge about the research of the topic of this research, and had an interest in the topic, which are all benefitting this research method. As for other methods that might have also resulted in interesting results, we considered generic meter development and validation method as described by

Mackenzie, Podsakoff, & Podsakoff (2011), but this was found as unfitting as method for a master's thesis, as it would have been way too laborious and large-scale, and the we did not possess needed extensive knowledge about quantitative research methods to fully utilize its potential. Concept analysis if of course not the only suitable method for this purpose, and we would very much welcome other researchers to approach the same issue with other methods, such as grounded theory to see whether their results would vary from ours.

The concept analysis method used in this research has basically 8 steps as seen in figure 1. While all steps are important, bearing in mind what we aim to have as the result, we consider the step 6 to be of utmost importance, as the questions we aim to develop are to be based on these identified related concepts.

2.2 Objective of the analysis

By studying our main concept, we aim to build better understanding of it, as well as identify related concepts to be able to build better questions to measure more relevant and critical aspects of information security awareness. We hope to identify enough related concepts, since the more we identify categories (related concepts), the more comprehensive and pervasive the questionnaire has potential to be. After identifying the related concepts, we will select some of them based on how much research about the related concept can be found, how much user can affect it or how much it affects user, and how critical it is in terms of security.

The materials used in this study were searched from online journal databases and scientific material libraries. The databases used were AIS Electronic Library, ACM Digital Library, Emerald Insight, IEEE Explore, IGI Global, JSTOR, SAGE Journals, Elsevier ScienceDirect, and Springer Link. These were chosen because of they have large amount of studies and papers from information systems field, and because the university provides elevated access for students to those databases. Besides research papers, studies, and conference proceedings, some reports and standards from National Institute of Standards and Technology (NIST), ENISA, and PCI Security Standards Council were used, since they are supposedly used by practitioners, and commonly cited by researchers (for example Kim, 2012; Puhakainen, 2006; Tsohou, Karyda, Kokolakis, & Kiountouzis, 2012, 2010; Tsohou, Kokolakis, Lambrinoudakis, & Gritzalis, 2010).

2.3 Selection of the main concept

The main concept was chosen because of its importance in the information systems field, and because it has been highly used in many studies, standards, and

training programs. It has been attributed as a crucial aspect in corporate security (NIST, 2003), and should be studied further to improve our understanding of how it is used, how it has been used, how it should be used, and what should it contain.

2.4 The main concept in the literature

While searching about research papers about our main concept, it is apparent that the information security awareness has gained more interest in recent years in research field. For example, searching with term "information security awareness" gives 252 results at Elsevier's ScienceDirect.com, of which nearly half (122) have are written on 2012 and after. The focus of the awareness has shifted from computer and software security towards information security, which can we believe can be explained by the Internet becoming more common and popular among the normal citizens instead of being just tool for researchers, making Internet more compelling for corporations, resulting in more available online services, which again in turn resulted more data being generated. The shift from computer security and information security is also noted by Whitman and Mattord, who wrote that CIA-triad has been as a conceptual model first for computer security, and later on for information security. (Whitman & Mattord, 2012). Same can be seen with NIST Special Publications, of which the 800-16 from 1998 is titled to be about computer security, while another publication that is commonly cited in same context, 800-50 from 2003, is about information security. This combined with the advancement of technology, e.g., disk space and computers in general becoming more inexpensive and faster, and Internet connections becoming more common, resulted in more and more data being generated, which eventually has gained interest of security researchers and legal systems, resulting in things such as data protection and data privacy laws. As more and more data moved from paper to digital format, and espionage and other threats also moved to digital world, companies had need to educate their employees about the new dangers.

Thomas Peltier wrote in article in Computer Fraud & Security Bulletin (1992) titled "Information Security Awareness - Selling IS to the employees", in which they went through reasoning about why the information security is needed, and why ISA plays an essential role on securing the information. Martin Smith wrote book called "Commonsense Computer Security – Your Practical Guide to Information Protection (2nd Edition)" in 1993, in which part 2 was titled "Responsibilities for Computer Security", which was about who should handle what and which duties should be assigned to whom in the enterprise environment, and the part 3 of the book contained discussion about information security awareness programs. Charles Wood wrote article in Computer Fraud & Security Bulletin in 1995 about information security awareness raising methods, in which they went through approximately 50 possible efforts companies could

enroll (Wood, 1995). While the list is in part image of its time, with few tweaks it could have been written today.

Siponen (2000) wrote "The term 'information security awareness' is used to refer to a state where users in an organization are aware of – ideally committed to – their security mission (often expressed in end-user security guidelines).", and "Similarly, information security awareness is of crucial importance, as information security techniques or procedures can be misused, misinterpreted or not used by end-users, thereby losing their real usefulness.". This first quote differs from NIST's definition, as in the NIST's glossary of key information security terms publication, information security awareness is defined as "Activities which seek to focus an individual's attention on an (information security) issue or set of issues." (NIST, 2013). This definition is also used by Enisa in their guide on how to raise information security awareness. (Enisa, 2010) However, this has been noted by Puhakainen (2006) in their dissertation, where they categorized 59 information systems security awareness approaches into two categories. In the first category, the ISA is considered as a means to attract users' attention to information security issues, and in the second category, ISA is considered as users' understanding of information systems security. (Puhakainen, 2006) This study will focus more on the aspects of users' understanding of information systems security rather than the actions used to improve it, as it we want to focus on the knowledge aspect of this issue, as in what should the users know and understand in order to be able to act and behave securely, and to be able to follow security standards and rules.

Farooq and Kakakhel performed study about comparing perceptions and training preferences, where at one part, to better understand the ISA level of their respondents, they asked questions regarding security threats faced by users in everyday life. (Farooq & Kakakhel, 2013) They don't however open how did they end on those specific topics, and why they were selected instead of other topics that people may face. Their topics were zero day attacks, denial of service, botnets, security incidents, pharming, phishing, social engineering, spam, Trojan horse, and Virus/Worms.

Albrechtsen and Hovden aimed to improve information security awareness and behavior through dialogue, participation, and collective reflection in their intervention study. They argue that their selected indexes cover a broad range of aspects of information security awareness and training, but no further arguments for the selected items are given. Their topics were responsibility (contains questions about virus infections, maintaining information security, and complying information security requirements), motivation (contains questions about writing passwords down and locking computer), information security vs. functionality (contains questions about information security being bothersome, and whether information security is foremost a technical issue), importance of specific information security measures (questions about safe use of e-mail, anti-virus tools, locking computer, usage of internet, non-disclosure), importance of generic security and safety measures (reporting incidents, keeping ID-card visible, following guidelines, occupational accident prevention, and

fire protection), reporting (willingness to report observed or suspected information security incidents), perceived skills and knowledge (having enough skills and knowledge to handle the information security of their working station), locking the computer, carrying id-cards, checking unfamiliar persons without ID-cards, and manual virus-check. (Albrechtsen & Hovden, 2010)

McCoy and Fowler explain in their paper how they implemented campus-wide security awareness program, their methods of delivery, and their perceived importance of establishing a flexible program that can meet demands and still be relevant to their users. (McCoy & Fowler, 2004) The topics they used in their training programs consisted password safety and security, workstation security, internet and email security, and physical security.

Al-Hamdani in his paper about assessment of need and method of delivery for ISA program lists possible topics to use in ISA training program. The list contains following items: password construction, password management, authentication, Internet usage, telephone fraud, physical e-mail usage and security, private information, virus protection and detection, PC Security, software licensing, backups, building access, social engineering, identity theft and home office security. (Al-Hamdani, 2006)

NIST Special Publication 800-50 lists potential awareness topics. The list contains items from following topics (topic may include multiple items): passwords, malware, policies, e-mails, data backup and storage, social engineering, web usage, incident response, physical access to devices, handheld and mobile devices, wireless security issues, usage of encryption, updates, software usage and licenses, access control, and information confidentiality. (NIST, 2003, pp. 24–25) Many researchers have used the items from the NIST 800-50 publication as their main topics from which they then have produced their questions or training topics (e.g., Awawdeh & Tubaishat, 2014; Kim, 2012).

From those listed in NIST Special Publication 800-50, Kim generated items from following topics to their questionnaire: anti-virus programs, updating virus definitions, regularly scanning computer and storage devices, use of firewall, installing software patches, using pop-up blockers, understanding the risk of downloading programs or files, understanding the risk of peer-to-peer file sharing, understanding the risk of clicking on e-mail links, understanding the risk of e-mailing passwords, understanding the risk of e-mail attachments, regularly backup important files, understand the risk of smartphone viruses, need of anti-virus for a smart phone, knowing the strong password characteristics, using different passwords for different systems, and changing passwords regularly. (Kim, 2012)

Enisa's how to raise information security awareness guide states that "identifying topics related to information security that are critical for the organization and the target audience is the first step of many while organizing an awareness initiative". They also list topics that should be considered for topics to information security awareness program: information security policies and procedures (which includes e.g., passwords), workstation security, website policies, e-mail security, social engineering, third-party and partner security, iden-

tity verification, technical security mechanisms, information classification and controls, incident response, asset management (e.g., USB flash drives, printing devices, PDA, mobile phones). (Enisa, 2010)

2.5 Identifying features of the main concept

Inherent features are attributes that are typical for the main concept, and appear regularly in research materials. Identifying inherent features helps researcher to differentiate the main concept from the related concepts. (Puusa, 2008) To better serve the purpose of this study, as inherent features, we focus on identifying topics and subjects that commonly are attached to information security awareness and its training programs instead of listing everything that we possibly can find. However, besides the previously mentioned topics, we would like to mention some descriptive features we found. While discussing information security awareness, it was often mentioned that awareness training programs should be flexible (McCoy & Fowler, 2004), be targeted (Enisa, 2010, p. 29; NIST, 2003, p. 20), and be relevant (for the targeted group) (NIST, 2003, p. 11).

In chapter 2.4 while going through the studies, we found many topics that are commonly used in ISA training programs or are commonly attached to the concept. There are many topics that are very close to each other (e.g., virus protection, anti-virus tools, and malware can all be gone through under the topic of malware), or are subtopics to some topic that may also be used (password management and password generation are subtopics of passwords). Because of this, we will categorize similar features under one title where possible without altering the topic. For example, "spam" and "e-mailing passwords" are both problems that can be categorized under the title "e-mail". We will now go through the identified features that we argue to be most crucial and relevant for the users, and which we should study further. All the identified features are listed on figure 1.

Passwords were notably most discussed feature. The topics were about whether users know what are secure passwords, how to manage multiple passwords, can passwords be written down, and do they know they should use different passwords for different systems. Comparing what we read for this study to what we have read in previous courses, we found some controversial issues (e.g., writing passwords down), so we will be paying extra attention to this topic in next chapter.

E-mail is the second feature we will study further, because while it is old technology while comparing for example to smartphones, it very widely used in corporate field, and is important way of communication. It is also used to spread malware, used in (spear)phishing, and in social engineering, so it deserves more study.

Third feature we will go through more carefully is physical access. The topics of physical access were about locking computer, building access, physical access to devices, and handheld and mobile devices. This topic is also important

to handle thoroughly, because another feature that we identified is social engineering, and one skill of good social engineer is that they can talk or tailgate themselves through locked doors.

Besides passwords, e-mail, physical access, social engineering, other features we selected to be more carefully studied are wireless networks, removable media, websites, updates and alerts, phone security, malware, and social engineering.

TABLE 1 Identified features of the main concept

Identified feature	**How it appeared in the literature**
Passwords	Password creation, password storage, password management, authentication, identity verification, writing passwords down, strong passwords, different password for different systems, changing passwords
E-mail	Phishing, spam, safe use of e-mail, physical e-mail usage and security, e-mails, e-mail links, e-mail attachments, e-mailing passwords
Wireless networks	Wireless security issues, handheld and mobile devices, technical security mechanisms, use of personal firewall
Physical access	Locking computer, checking unfamiliar persons without id-cards, building access, home office security, physical access to devices, handheld and mobile devices, access control, technical security mechanisms
Removable media	Asset management, workstation security, PC Security, scanning computer and storage devices
Websites and social media	Website policies, pharming, usage of internet, internet usage, web usage, using pop-up blockers
Updates and alerts	Software usage and licenses, updating virus definitions, installing software patches
Phone security	handheld and mobile devices, telephone fraud, asset management, understand the risk of smartphone viruses, need of anti-virus for a smartphone
Malware	Zero day attacks, Trojan horse, virus/malware, virus protection and detection, malware, anti-virus tools, PC Security, manual virus-check, botnets, regularly scanning computer and storage devices, anti-virus programs
Social engineering	social engineering, third-party and partner security, checking unfamiliar persons without ID-cards, reporting, information confidentiality, telephone fraud, identity theft
Backups	backups, data backup and storage, regularly backup important files

2.6 Identifying related concepts of the main concept

This chapter goes through identified related concepts of information security awareness. Information security awareness is an abstract concept, so identifying

whether the concept at hand is either related concept or inherent feature can be problematic. This is in part because some concepts such as network security can be understood as level of the security of the network in question, action and methods to secure the network, or as synonym for information assurance, which is defined as "Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation" (NIST, 2013). By identifying the related concepts, we aim to focus on clarifying the main concept and the difference to related concepts.

Arguably most important related concept is the concept of information security. Whole concept of information security awareness bases on this concept, and it is also of utmost importance for the other related concepts. Information security was defined back in 1.4.1 while going through important keywords.

Information security training programs and information security awareness programs are different things, even though they are often discussed about together. Information security awareness programs main purpose is to raise the awareness about the issues and increase interest in the issue, whereas information security training programs are intended to train users so they can work securely and avoid dangers. NIST 800-50 states "The most significant difference between training and awareness is that training seeks to teach skills, which allow a person to perform a specific function, while awareness seeks to focus an individual's attention on an issue or set of issues." (NIST, 2003)

Information security education is yet another concept that was seen a lot. The difference between training and education per NIST 800-50 is "An example of education is a degree program at a college or university. Some people take a course or several courses to develop or enhance their skills in a particular discipline. This is training as opposed to education." (NIST, 2003).

3 REVIEW OF IDENTIFIED RELATED CONCEPTS

This chapter is dedicated to going through studies and practices of the features identified in chapter 2.5. Taking the suggested size of master's thesis and to keep the amount of studying needed about the topics reasonable, we will limit our examination to 10 topics we reckon to be commonly most crucial. This is not, and is not supposed to be, a complete list containing everything. As stated in many studies, one size does not fit all. We repeat the recommendation of customizing the contents of information security awareness training programs to the targeted audience, as well as using carefully selected delivery methods, which also should be chosen to best reach the targeted audience.

3.1 Passwords

Text-based passwords have long been the most used authentication mechanism (Shay et al., 2010), and while there exist alternative methods e.g., image- based password systems (Chiasson, Oorschot, & Biddle, 2007) and biometric authentication systems (Mahto, 2015), text-based passwords still prevail as most used and supported method for authentication. Text-based password authentication systems are easy to implement (Tsai, Lee, & Hwang, 2006) and do not require additional hardware, while e.g., facial recognition systems require camera and biometric systems require e.g., fingerprint reader.

While text-based passwords have aforementioned desirable aspects, they also have major issues. It would be very slow for humans to try and guess all the possible exactly 6 characters long passwords, because just with numbers and case sensitive alphabets, there are 56,800,235,584 possibilities. Reality, however, is that with computing power is cheap and there are free open source programs available for use to crack the hashed passwords. These are reviewed in chapter 2.1.2

Passwords are usually stored in hashed format. Hashing is one-way encryption function, which means that the function is supposed to be irreversible.

For example, SHA1-hash of a word "cat" is 9d989e8d27dc9e0ec3389fc855f142c3d40f0c50. Hashes are case sensitive, which means that "cat", "Cat" and "CAT" all have different hashes. Hashes are fixed in length, but the length depends on function, e.g., all SHA-1 hashes are 40-characters in length. Good hashing algorithms are also collision resistant, meaning that no known two different inputs to hashing function produce same output. MD5 is known to have collisions (Black, Cochran, & Highland, 2006; Klima, 2006) and is generally considered to be broken (Dougherty, 2008), as well as SHA-1 (Stevens, Karpman, & Peyrin, 2015). Instead of aforementioned broken functions, Stevens et al. (2015) suggest using SHA-2 or SHA-3 when possible. As mentioned before, hashes are supposedly irreversible, which means that cracking them by reversing them per se is impossible. When we talk about cracking, we mean practice of taking a word, hashing it with the same function as the password we are trying to crack was hashed, and checking whether the word we hashed produced the same hash as the one we are trying to crack is. This process is repeated until match is found or attacker gives up. Cracking passwords is discussed more in depth in chapter 2.1.2.

3.1.1 Common insecure password habits

Using short passwords is one of biggest mistakes users can make. Given the possible character set of 95 different characters (upper- and lowercase letters, numbers and 33 special characters), resulting in even the most complex 6 characters long password being cracked in bit under 24 minutes. Another pitfall is to use names and other proper nouns, e.g., Oxford or Lagavulin. It is reasonable to expect that all natural language words and names of people, teams, and brands can be found from massive wordlists.

It is known by makers of cracking tools (Openwall, 2010) and scholars (Shay et al., 2010) that users tend to use predictable patterns on passwords. Common password structure is to use capital letter at the beginning, followed by lower case letters, and lastly append numbers and special characters at the end. In study by Shay et al. (2010) 43.4% of respondents answered to question "When you created your current password, which of the following did you do?" with answer along lines "Word/name w. numbers/symbols added to beginning/end". 61.2% of special characters used by respondents came from under the numbers 1, 2, and 3 (!, @, and #). Using special characters is great step forward from not using them, but using them in predictable manner diminishes their benefits.

Reusing passwords is another major issue. In study by Shay et al. (2010) 80% of respondents answered positively on whether they were reusing passwords or not. Most of them also reused one password with minor modifications on multiple accounts. Password reuse is coping mechanism for users against having too many accounts, but reuse should be avoided, as it can cause domino-effect, which means that breach in one of the services can compromise users accounts in other services (Ives, Walsh, & Schneider, 2004).

While not necessarily a habit, sharing passwords is also considered to be insecure practice. One third of teens admitted to have shared their password with someone (Lenhart et al., 2011), which is among the lines of study by Shay et al. (2010), where they found that 33% of respondents under 22 had shared their passwords, whereas with older users the percentage was. Sharing password has multiple problems. First of all, when sharing personal password with co-workers, if one of these said co-workers gets laid off or hired to competitor, they can leak the password and cause serious damage to company. Another problem is that sharing password can cause trust issues between people, e.g., if John shares his password to Jane, and attackers gain access to that said password somehow unrelated to Jane and cause damage to John, it will still raise suspicions between the two people.

3.1.2 How passwords are cracked

John the Ripper, Hashcat, Cain and Abel, L0phtCrack and RainbowCrack are some of the most popular password cracking applications. Cain and Abel is freeware password recovery application made for Microsoft Windows, but also possesses some other features, for example VoIP conversation recording, ARP spoofing and revealing password boxes (Montoro, 2014). L0phtCrack is proprietary password auditing and recovery application for Microsoft Windows, and it features dictionary, brute-force and hybrid attacks, and can utilize rainbow tables (L0pht Holdings LLC, 2012). RainbowCrack is, as its name suggests, password cracking application that utilizes rainbow tables. It supports Windows and Linux operating systems. (RainbowCrack Project, 2015) Hashcat is cross-platform password recovery tool, that has two different versions: oclHashcat and hashcat (hashcat, 2015a). Hashcat uses computers central processing unit (CPU) for processing speed, while oclHashcat uses graphical processing unit (GPU), which, depending on GPU-card, can offer performance up to 5-20 times higher than CPU (Yu & Huang, 2015). oclHashcat has two versions depending on users GPU: cudaHashcat for NVidia GPUs and oclHashcat for AMD GPUs. (hashcat, 2015b) John the Ripper multi-platform password cracker that has support for multiple CPUs and support for GPUs (CUDA and OpenCL). It can automatically detect the type of common hash functions, and can perform dictionary- and brute force attacks. (Openwall, 2015)

Brute force attack is type of an attack, where program guesses password blindly with given set of rules. Rules can for example specify that program tries all lowercase combinations of alphabets that are under 6 characters long, or all exactly 8 character long passwords consisting of upper- and lowercase alphabets and numbers. Brute force attack can theoretically crack any password imaginable if given enough time. In practice, however, e.g., Hashcat using CPU benchmarked on a two years old computer to be able to crack 34.05 million SHA1 hashes per second. Precisely 8-characters long password consisting of upper- and lowercase letters and numbers yields 218 340 105 584 896 possible combinations, meaning it would take bit over 74 days with aforementioned

speed to crack them all. If we try to crack all exactly 12-characters long passwords with the same speed, it would take bit over 3 million years. However, GPU-farm with 8 units of GeForce GTX Titan X can achieve speed of 48867.2 million SHA1 hashes per second. With the higher end GPU-farm, 8-characters long password would be cracked in 74 minutes, but even with it, cracking all the hashes of 12-characters long passwords would take over 2093 years. (Gosney, 2015)

Dictionary attack is special case of brute force attack. It utilizes existing dictionaries or wordlists instead of blindly guessing every possibility. Dictionary attacks are fast way to crack the most trivial and used passwords, since as mentioned before, users tend to use passwords that either can be found from dictionary or are based on words in dictionary. Many password lists consisting of hacked databases can also be found online, of which few of the well-known are RockYou, Yahoo Voices, eBay and Adobe. (Cubrilovic, 2009; Ilyin, 2014; Krebs, 2013; Lunden, 2012) Dictionary attack is only as useful as the dictionaries it uses. Larger dictionaries increase chance of finding the password, but also increase the time that the attack takes.

Hybrid attack (e.g., on John the Ripper) takes dictionary words and uses custom rules to create new words. For example, it can try to capitalize all letters, only the first letter, only the last letter, reverse the word, duplicate it, or append characters or numbers to word. John the Ripper can also use grammatical rules, such as pluralizing word, transforming nouns to verbs (“speak” -> “speaking”), and mimic things that user might do e.g., shifting fingers one button to left or right (“nouns” => “biyba”), and uppercasing consonants or vowels and lowercasing the other. (Openwall, 2010) Hashcat team has also build an option to perform fingerprint attack, that basically automates rule generation by finding patterns from cracked passwords and applies them to words in given dictionaries or word lists. Newest addition to hashcat program is Prince attack-mode. It starts by checking given password hashes against wordlists, then if not all passwords are found, switches to hybrid mode, and then to keyboard walks and passphrases. Lastly it moves to brute force with Markov-chains. (Steube, 2014)

3.1.3 Generating good passwords

Good password is something that is hard for cracking software to guess, but easy for human to remember. Longer password increase complexity very fast, but common phrases and well known sentences are not necessary much more secure than common shorter passwords. Maximum length of password should not be limited (Scarfone & Souppaya, 2009), and that no characters should be prohibited from being used. (Gehringer, 2002) Scarfone & Souppaya (2009) explain effects of increasing character set and length of the password in NISTs Guide to Enterprise Password Management draft:

> Increasing the character set from 26 characters to 95 characters on a four character-length password increases the keyspace almost 200 times. However, if the length of the password is increased from four to 12, given a character set of only 26 characters, the keyspace increases by almost 200 billion times. Although both have significant effect on the overall strength of a password in resisting brute force attacks, outside of cryptographic attacks, length seems to be the dominating factor in determining password strength. (Scarfone & Souppaya, 2009, 19)

Minimum length of password is suggested to be somewhere between 6 and 14 characters (Microsoft, 2016; Vu et al., 2007; Zhang & McDowell, 2009). However, given the rise in computation power over the years, 6-characters long passwords should not be considered strong or adequate anymore. Considering that password would consist of upper- and lowercase letters, numbers and special characters, user most likely would like cracking of their password to take at least longer than they are alive, so to be on safe side, minimum of 100 years. With 95 possible characters, and with set of 8 modern GPUs, this would mean at least 11 characters long password, which would yield over 3690 years. Noting, that this calculation only includes passwords exactly 11 characters long, but not those of 10 characters and less. Given that GPUs are likely to become stronger in future, we would suggest using minimum of 15 characters long password, in which case it would take over 300 billion years to crack all possible 15 characters long passwords with today's high-end technology.

Generating and remembering a 15-characters long complex password consisting of lower- and uppercase letters, numbers and special characters is an immense task for anyone to perform. Study found that users have about 25 accounts, but use only 6.5 different passwords. (Florencio & Herley, 2007) Studies have also shown that users will reuse passwords more as the amount of accounts increase (Gaw & Felten, 2006). Using mnemonics, users should be able to generate passwords that are as memorable as randomly chosen ones, but as memorable as naively chosen passwords (Yan et al., 2004). However, Adams and Sasse (1999) state that four or five regularly used password are maximum that users can be expected to cope with (Adams & Sasse, 1999). Password management software, such as 1Password, LastPass or KeePass, can theoretically solve the problem of remembering secure passwords, as they can generate long and secure passwords, and store them highly encrypted, so that user has to remember just one password to access the rest. (Scarfone & Souppaya, 2009) This method, however, is highly vulnerable to malware. In recent years, multiple families of malware have gained an ability to search and steal master password and encrypted password file from password management software, compromising all stored passwords (Goodin, 2015; Tamir, 2014).

3.2 Email

Email is fast and easy way of communication that has deeply integrated into our society (Ayodele & Adeegbe, 2013; W. Z. Khan, Khan, Bin Muhaya,

Aalsalem, & Chao, 2015). However, as with all types of communication, email can be used for malicious purposes. Phishing, a homophone of a word fishing, is an act of sending bait that impersonates legit message in order to get sensitive information from the target, e.g., credit card information or account information. Phishing is often expanded as spear phishing if the phishing is targeted only to one or few selected individuals, and the message is personalized to maximize the chances of the receiver falling for the phishing. (Greitzer et al., 2014; Wang, Herath, Chen, Vishwanath, & Rao, 2012) Normal phishing campaigns usually utilize spamming techniques to reach as many potential victims as possible (Dhinakaran, Lee, & Nagamalai, 2009). For example, regular phishing might be mass spamming of a classical Nigerian Prince –scam, and spear phishing is message that appears to come from receiver's coworker, addresses them with their right name and asks them for door code to server room or something similar. Nigerian Prince –scam is type of phishing, where sender explains that they have large amount of something valuable, usually gold or money, hidden somewhere, and they need receiver to send them some amount of money to help them move their valuables to somewhere where they can access it, and afterwards they promise to give the target substantial amount of money. Phishing emails may also contain links to sites that attempt to infect receiver's computer with malware (Schatzmann, Burkhart, & Spyropoulos, 2009). To make phishing detection harder, it is possible to spoof e-mail header to make it look like it came from somewhere legit, meaning that the e-mail actually comes from different sender than it might appear for the receiver. (Mahadevan, Cangussu, & Dantu, 2009). There are some ways to defend against spoofed e-mails in corporate environment, but for the normal user best options is to enable spam filters, and be vary of everything they did not expect.

ENISA's ten security awareness good practices notes that confidential information should be encrypted when sent by email (ENISA, 2009). Additionally, NIST Guidelines on Electronic Mail Security Recommendations states that encryption should be used to securely send email messages containing sensitive information (Tracy, Jansen, Scarfone, & Butterfield, 2007). Moreover, said Guidelines also warns about sending sensitive information via email as it could be intercepted, and Cisco Best Practices for Business Class E-mail comparison of security characteristics of email and postcard sums that the similarity is disturbing (Cisco, 2009).

Emails may also contain attachments, which in turn may contain malware. Basic way of spreading malware is to use email to send it with message promising something that entices receiver to click the attachment (Heikkinen, 2006). Both NIST and ENISA also suggest that users shouldn't open unknown emails and attachments, and that users should use malware scanning software to scan all attachments even from known senders, as sender information could be faked. Not only the attachments are dangerous though, as the applications used to read the e-mail may be the target that the payload in the e-mail attacks against. For example, Microsoft Outlook has preview feature in their e-mail client,

which could be used as an attack vector for RTF vulnerabilities. (Chu & Florio, 2014)

3.3 Wireless networks

Nowadays wireless networks can be found in most places, e.g., homes, café's, libraries and shopping centers. We will focus on wireless networks based on IEEE 802.11 standards, as they are most commonly used in consumer electronics. IEEE 802.11 standards are commonly referred as wireless local area network (WLAN), or as Wi-Fi. Even though Wi-Fi and WLAN are often used as synonyms, Wi-Fi is registered trademark of Wi-Fi Alliance (Wi-Fi Alliance, 2016). WLAN's purpose is to share network access, usually Internet access, wirelessly to multiple devices in limited range. Access point (AP) is the device, e.g., WLAN router, that is connected to rest of the network, and to what users connect their devices, e.g., laptops and smart phones, to access the network.

WLANs are identified by services set identifier (SSID), which has maximum length of 32 characters. User might set their AP to stop broadcasting the SSID in order to hide the network and stop unwanted users from connecting to it, but this doesn't really provide any security, as the name is transferred unencrypted when connecting to network (Skracic, Petrovic, Pale, & Tralic, 2014), listening the network long enough for someone to connect to it will give out the name. User can also set AP to filter access by end devices media access control (MAC) addresses to allow access only for predefined devices. This too is trivial to bypass, as MAC addresses are too transferred as plaintext, attacker can listen network traffic long enough for someone to connect to the network, and then change their MAC address to match address of an allowed device. (Nagarajan, Arasan, & Huang, 2010; Shikha, Kaushik, & Gautam, 2013)

More advanced WLAN protection mechanisms exists, namely Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) of which latter has newer version (WPA2), which is also currently the most up to date authentication mechanism available for most common WLANs. WEP, however, should be considered broken and not be used (Stubblefield, Ioannidis, & Rubin, 2004). Wi-Fi Protected Setup (WPS) is another security measure that should be considered broken in most parts. WPS is not an encryption, but an option for users to connect their devices to WLAN by entering 8-digit PIN code instead of lengthy password. This feature has major flaw, where remote attacker may gain WPS PIN, and with that, WPA/WPA2 pre shared key (Viehböck, 2011). Enhanced edition of WPS that has fixed this problem has been introduced by scholars (Zisiadis, Kopsidas, Varalis, & Tassiulas, 2012), but it appears to not have been widely deployed.

WPA and WPA2 have two operation modes, pre-shared key (PSK) and enterprise. Enterprise mode requires remote authentication dial-in user service (RADIUS). PSK method is most common in homes and small offices, as it doesn't require server to authenticate users as enterprise mode does, but in-

stead requires users to know pre-shared secret between 8 and 63 characters to allow access to network. (Nakhila, Attiah, Jinz, & Zoux, 2015) PSK authentication can be bypassed by guessing the password, but since the passwords cannot be shorter than 8 characters, it can be very time consuming to crack the password.

Easiest and most likely the most common negligence related to wireless networks that users may be guilty of is connecting to insecure networks on public places without sufficient protection. Connecting to unsecured network exposes all traffic generated by user to anyone who listens the network traffic. Many tools exist that attacker can use to detect and analyze the network traffic, and even crack WEP or WPA/WPA2-PSK protected connections. Airmon-ng, airodump-ng, aireplay-ng and aircrack-ng are all tools from same suite designed for monitoring, analyzing and testing wireless IEEE 802.11 networks. Wireshark can also be used to monitor network traffic and even read contents of network packages.

Another type of negligence is to use the WLAN router with default settings. Many devices ship with preconfigured administrator and password combination, which may vary a bit, but there are sites that list default usernames and password for most common devices. This makes it possible for attacker to, for example, change gateway address to make all traffic go through their computer, so they may analyze and alter it as they want. Default settings may not also be the optimal settings. For example, WPS might be enabled, or WPA might be in use instead of WPA2, or wireless network password might be the same default password in all that model of devices. Default SSID names should also be avoided, since rainbow table attacks can be deployed against WPA protected networks. Changing the SSID of AP to something else than one of the most common SSID's renders this attack useless, since rainbow tables are pregenerated and thus can only be used against adequately named networks.

3.4 Physical access

Gaining physical access to targeted computer is basically "game over" – situation (Bookman, 2003; Trost, 2009). In some scenarios, it might be hard to access the files in the system even if physical access has been obtained, for example if the whole system is well encrypted and is not currently in decrypted format when attacker gains the physical access, but is e.g., powered off. In this scenario, attacker might insert key logger to steal users input and either report inputted characters back to attacker, or if attacker knows they can easily access the room again, key logger may be set to store input locally to minimize detectable suspicious network traffic, and attacker can pick it up later.

If the target machine is not a server, but a local workstation that doesn't embody full disk encryption, it is highly likely that attacker could access the files on that machine. They could use e.g., Linux live-cd or Windows recovery to bypass login of the installed operating system, then mount the local drive(s)

and access, delete or copy files. This can also be just a start, as attacker may use this method to e.g., create new account or reset password of existing account (Whitty, 2012). In situation where attacker can access the system, they could also install malware to gain access after they are no longer able to physically access the system, or because they know they don't currently have enough time to go through the computer before someone comes around.

Even if the system is normally encrypted, if it is unencrypted and running by the time attacker gains access to it, the keys are still stored in memory. This leaves system vulnerable against cold boot attack, which allows attacker to extract keys from the memory (Halderman et al., 2008; Lindenlauf, Hofken, & Schuba, 2015). Physical access also gives some opportunities that online attacks don't have. DMA attacks use physical ports that permit direct memory access (DMA), e.g., Thunderbolt, FireWire, Express Card and PCI Express. Rogue device with direct access to memory could then install malware or read passwords and encryption keys (Balogh & Mydlo, 2013; Stewin & Bystrov, 2012; Witherden, 2010).

One thing to consider here is that information security triad consists of confidentiality, integrity and availability. If attacker gains physical access to our server, integrity becomes questionable. Victim would have to check whole server for possible changes, and all areas attacker accessed against possible tools that may monitor or access the network traffic, and even after that, can the victim still be sure that attacker didn't access or alter anything? Attackers physical access could also mean end of availability. If attackers main purpose would be to cause damage or destruction, they could physically destroy the hardware, rendering data inaccessible.

3.5 USB flash drives

While this may partially be a subcategory of physical access, popularity of USB flash drives and their potential dangers deserve their own chapter. CD's and USB flash drives themselves are not dangerous, and are usually used for legitimate purposes, but they are easy to conceal, hard to notice, and it is easy to forget that even small USB flash drive can contain more than 512 GB of information, which is much more than generic malware requires. Lots of users use them on daily basis without issues, which may contribute to why people don't usually find USB flash drives suspicious or don't see them as potential threats.

Stuxnet, one of the most notorious modern malware, spread through USB flash drives and local networks (Cotroneo, Pecchia, & Russo, 2013; Langner, 2011), and in Black Hat USA 2014, security researchers Nohl & Lell demonstrated BadUSB, a full system compromise from USB flash drive, and self-replicating virus that was not detectable by anti-virus applications at the time (Black Hat USA, 2014). USB flash drives with intriguing nametag such as "private" or "classified" can used as a part of social engineering attack, and are usually highly successful (Hadnagy, 2010).

In recent study, researchers dropped 297 USB flash drives on university campus, and within six minutes first drive was connected, and in the end the total success rate was over 45% (Tischer et al., 2016). While majority of users reported that their intention was to find the owner of the drive to return it, the altruistic motivation does not protect against potential payloads and dangers of what the drives might have contained. In the same study, 68% of the users who had inserted the drive did not take any precautions, and of those who did, 16% scanned the drive with their anti-virus and 8% trusted their computers security features to be adequate. Had this case not been experiment but a malicious attack using aforementioned case of BadUSB or Ducky (Hak5, 2014), none of the aforementioned precautions would have worked.

ENISA's ten security awareness good practices recommend to not let anyone plug their USB drive into your computer, and to never connect any personal USB drives to your computer (ENISA, 2009). In some organizations, it is even a policy for employees to never insert devices from unknown sources to work devices, but even though users might say that they are complying the security policies, they might not even know what those policies say (Siponen & Vance, 2014).

Ways to defend against possible malicious USB flash drives are limited, but generally efficient. Most efficient way is not to use USB flash drives, and to block USB-ports from being easily accessible to by passers attackers in hurry. If attacker is not in hurry, they can possibly pick the locks and insert the USB flash drive, but this can be avoided by not allowing unnecessary people to lounge around computers without supervision. Enterprise users can also lower the risk by using sacrifice computer, which is device that is either strongly sandboxed and monitored, or device that can be easily reset to original state if it is suspected to have been infected. Even though anti-virus software does not detect everything, defense in depth is still best solution and anti-virus programs should be utilized.

3.6 Websites

The popularity of World Wide Web (WWW) has rocketed from early 2000, and from 2010 to 2015, the number of websites has risen from 200 million to 863 million (InternetLiveStats.com, 2016). Since then, the term Web 2.0 has been coined, and it is not a technical specification but rather an umbrella term for sites that emphasize user-generated content, such as blogs, wikis and social media sites (Baxter et al., 2011; Murugesan, 2007). Amount of people using Internet daily has also risen rapidly, and for example Facebook alone has reportedly 2 million active daily users just in Finland alone (Kärkkäinen, 2015).

Malware spread through advertisements has lately been such popular method, that a term "Malvertising" has been coined to describe the behavior. The method works in the way that e.g., a legitimate and respected site, that normally displays non-malicious advertisements it gets from advertisement

company's servers, gets malicious advertisement and displays it to user (Sakib & Huang, 2015). Depending on how it was designed, users might not even have to click the advertisement to get infected, for the malvertisement might utilize vulnerabilities in e.g., Flash or Java to infect users' computer.

Besides not using computers, no security mechanism can provide full protection against malicious websites. Users can lower the risk by using browser add-ons like µBlock Origin and Disconnect with specific filter lists to automatically block access to blacklisted known malicious sites, but since they work on blacklist mode, it may take time for them to get up to date. Blacklists are also generally ineffective against targeted attacks, since someone or something needs to tag the address as malicious and add it to the list, which may not happen if the address is used only for dedicated attacks against one or handful of targets. Even so, if attacker uses common malware, it's signature or its behavior might rise a flag in the anti-virus program. If the attacker combines fresh address with custom made or edited malware that doesn't attract attention from anti-virus applications, and uses exploit to deliver it to user, noticing the attack is next to impossible before it is already too late.

Users can also lower the risk of being exposed to malicious sites by not visiting suspicious sites (e.g., sites selling cheap drugs or fake versions of expensive brand products) and by not clicking links in emails that they did not expect. Users can also use browser extension tools to help them navigate on the Internet, e.g., Web of Trust (WOT). WOT works in a way that users rate sites trustworthiness and child safety, and the extension displays circle next to link describing the site with color: green for good site, yellow for suspicious and red for site with bad reputation, or question mark if the site doesn't have enough votes. Problem lies with sites that don't have enough votes, and possible vote manipulation. For example, some controversial sites have gained bad reputation, even though the site itself is safe, but the opinions in the site are opposite of voters' opinions. Even though WOT has methods to stop vote manipulation towards one way or another, advanced persistent threats (APT) may still have means to manipulate their site to appear as a good site if they deem it beneficial.

Another danger is sending sensitive data through insecure connections. Users may e.g., send their social security number and personal information via unsecured connection to web server, which may be intercepted, for example if combined with earlier example of unprotected wireless network. Modern browsers display e.g., padlock near the address bar if connection to site is secured. While there is not much that users can do for this, as this is more of a site owners matter, users should be aware of potential eavesdropping when submitting sensitive information site without secure connection. VPN connection can help to protect against e.g., Wi-Fi eavesdropping, but even then, the connection is unsecure between VPN server and the target site.

Third threat is partly similar to aforementioned threats but is more related to an authenticity rather than confidentiality, that is, an issue of entering sensitive information to site that is deceptive. These may either appear as legitimate site or as something that promises reward in a return for sensitive information,

e.g., pop-up window with dancing banana asking for credit card information in exchange for a chance to win million dollars. Example of deceptive site that poses as legitimate site might be fake online banking site made by criminals to steal banking credentials. Users may protect themselves against these threats by being vigilant and using common sense. If the offer appears to be too good, it most likely is a scam. Aforementioned blacklist browser extensions may be of help, as well as not clicking links in suspicious emails and websites.

Besides basic websites, users should also be aware of potential dangers of posting in social media. For example, burglars are reported to monitor social media for people going on vacations or otherwise being absent from their homes (Axon, 2010; Johanson, 2013; Pleasance, 2015; Tomlinson, 2011). Criminals have been known to have checked airport parking lots for potential targets (Yle, 2016), so they might as well verify the emptiness of the targeted home by checking car owners social media accounts for possible vacation updates and pictures. While it is not easily possible to completely remove owners name from cars information, it might be beneficial for users to remove public access to their address information. Users should also postpone publishing vacation pictures and updates to when they are already back in home.

Attacking users on social media can be done on multiple ways. One could be to make fake account that mimics one of user's friends, ask users other friends as friends and then finally ask user as a friend. After befriending user with fake account, attacker could send either malicious link or file with message saying it is something interesting or embarrassing, like telling that they found photo of the target nude in the Internet with attachment of photo.jpg.exe, or something that attracts their interest. Another way would be to just spam all their friends with link to something like free personality test, that needs access to user's friend list and wants to send messages on behalf of the user. While user might be suspicious about link coming from stranger, if they see their friends posting links to test, they might click it out of curiosity. Even though from attacker's perspective, unless it is necessary for the victim to be that particular target, they might as well just send time and context aware phishing mail with fairly high success rate. A study by Zinaida Benenson and her team found that up to 56% of e-mail recipients and about 40% of Facebook users clicked on the link received from unknown sender, even though 78% of all respondents stated that they were aware of risks (Benenson, Gassmann, & Landwirth, 2016). 34% of those who clicked the link stated curiosity as the reason for clicking. Interestingly, 27% listed "fits my New Year party" as reason for clicking the link. If attacker combines this knowledge with even basic data gathering, e.g., checking users twitter and Instagram feeds for where they were this weekend, and sending similar message as Benenson et al. did with spoofed email address and less suspicious URL, click rate might rise much higher.

Against common spam, fake and malicious tests, and mass targeted phishing, using anti-virus application, browser add-on to blacklist known bad URLs, and being suspicious of everything even though it appears to be or even if it is from known sender, are cheapest and most effective defenses. Benenson at her

Blackhat USA 2016 talk lists under the title "Lesson 2: Requirements on Users" following advice: "Be suspicious of everything!" (Benenson, 2016).

3.7 Updates and alerts

Developers publish security fixes, new features and stability improvements through software updates. It has been shown that there is clear correlation between the updates and infection rates, where infected machines were not being updated (M. Khan, Bi, & Copeland, 2012). Many experts and papers refer regular system and application updates as necessary, vital, or important (Bechtsoudis & Sklavos, 2012; Brodie, 2009; Reeder & Consolvo, 2015, p. 330). Running outdated software may compromise the system, even though the outdated software itself might not be that important and it might not even play vital role in the system, but from attackers' point of view it may still appear as a gateway to the network. For example, running outdated browser exposes user to many possible targeted and coincidental attacks, e.g., user might fall victim of Malvertising, as explained in 2.6, or they might click link in e.g., spam or phishing mail, and be taken to site with malicious code that exploits outdated browsers known vulnerability. Running outdated software might not even require users to actively do anything to get infected. For example, Windows XP had vulnerability on Server service at port 445, which allowed remote code execution by sending specifically crafted RPC request (Microsoft, 2008). This is banal example, as it is commonly referenced and used on Metasploit penetration testing software tutorials. Remote code execution in short means that attacker can run malicious code of their choice on targeted machine, eventually resulting in the targeted system to be compromised.

Another aspect to the update issue is malvertising and malicious tools posing as anti-virus tools or security updates. It might be difficult for users to distinguish between legitimate alert and malicious advertisement or pop-up designed to trick users. Users may have been advised to not click anything they do not understand, and to just close any windows that they do not expect, resulting in users closing both real and fake warnings. Study made in 2016 concluded that users commonly dismiss system-generated alerts (Jenkins, Anderson, Vance, Kirwan, & Eargle, 2016). This is because disruptions cause dual-task interference, which means that human brain can't perform multiple tasks at once without significant loss in performance. Users still prefer to be interrupted immediately to be asked for permission rather than be informed later that permission was granted, if the issue concerns their privacy (Patil, Hoyle, Schlegel, Kapadia, & Lee, 2015). Akhawe & Felt found in their study that 70.2% of users ignored Google Chromes SSL warnings, whereas for Mozilla Firefox the number was 31.6% (Akhawe & Felt, 2013). They also found variation between demographic groups. Interestingly, more technically savvy users appeared to ignore SSL warnings more than less technically savvy users, which Akhawe & Felt presumed might be because they either feel more confident

about the security of their system, they are more curious about blocked websites, or that they may feel patronized by the warnings. Updates to software that is deeply integrated with the operating system, such as anti-virus software or GPU drivers, may also require restart of the system which may interrupt users' workflow, resulting in user clicking "Skip update" button. Some developers have made their application to give user an option to install now or to install later, where installing later results in updates being installed at night while device is idle or at next time device is shut down or started, delaying update a little instead of ignoring updates completely.

3.8 Phone security

According Ericsson Mobility Report, there were total of about 7.4 billion mobile subscriptions of which 55% were smartphone subscriptions. Of the 7.4 billion mobile subscriptions, about 5.1 billion are unique. (Ericsson, 2016) According to United States Census Bureau there were about 7,3 billion humans at the moment of writing this. (U.S. Department of Commerce, 2016) This results in nearly 70% of world population having a phone.

As smartphones are getting more and more common and popular, they have become interesting target for criminals. According many authors, smartphone malware has become serious threat (Amamra, Talhi, & Robert, 2012; Brown, Anwar, & Dozier, 2016; Peng, Yu, & Yang, 2014; Shrestha, Ma, Zhu, Li, & Saxena, 2015; Xin, Li, Qin, & Zhang, 2012). Modern phones can store lots of information about its owner, including but not limited to photos, personal information, geolocation, medical information, financial information and credit card data. In addition, many users have 2-factor authentication (2FA) applications such as Authy or Google Authenticator, or have set their mobile phone to receive 2FA code messages through SMS. 2FA codes are one-time used short key codes, that are usually entered after successful username and password entry. One of the most famous 2FA identity access management devices is RSA's SecurID hardware token, which is small physical device, small enough to hang from keyring (RSA, 2016). 2FA can moreover block attacks when users reuse their passwords, leading their other accounts compromise too. While this may prevent damage, it is still not advisable to reuse passwords, as attackers are known to have found ways to bypass 2FA due implementation failures (Duo Labs, 2014), or by posing as service provider like Google (Ragan, 2016).

Brown, Anwar & Dozier list on their 2016 study common vulnerabilities that have been and are being exploited by malware developers, of which overgranting permissions can be, while easy to avoid, one of the most harmful ones. Granting permissions basically means that when user is installing application, the app asks user for permissions to do something, e.g., using camera and send SMS's. In earlier versions of Android operating system, users could not grant specific permissions but had to either accept all asked permissions or they couldn't install the application. In newer versions, this has been changed so that

applications only ask permissions when they use the feature, but applications can still ask permissions for something that they really shouldn't do. Researchers from security company named Check Point found malware from Google Play store, which they named DressCode. Applications containing DressCode were downloaded between 500 000 and 2 000 00 times. DressCode was used to create botnet, which in turn was used as socks proxies and to generate revenue to attackers. (Menczer & Lysunets, 2016)

For attackers targeting specific users, attacking the smartphone of the user is good idea, since many services employ 2FA, which makes knowing just the username and password not very useful. However, if attacker has access to victim's smartphone, they can read the applications or messages for 2FA codes. If they don't have access and try to log in, it might alert the user that they receive 2FA code even though they haven't tried to login recently. Cyber crooks that are more interested in earning money quick, it might be more beneficial to set up chargeable number and use the malware to send SMS's or to make calls to that number. This will however alert users at the latest when their next phone bill arrives.

Because of rise of malware for smartphones, more anti-malware software and better detection mechanisms are being developed for smartphones every year and are recommended to be used to increase security (see e.g., Amamra et al., 2012; Eshmawi & Nair, 2013; McDaniel, Thuraisingham, & Khan, 2014; Peng et al., 2014; Shrestha et al., 2015; Wu Bin, Lu Tianliang, Zheng Kangfeng, Zhang Dongmei, & Lin Xing, 2014; Xin et al., 2012)

3.9 Malware

We will go next through malware in general and what it has become. We will also differentiate between different types of malware. Last, we go through common ways for malware to spread, and ways to protect against malware.

3.9.1 General about malware

NIST defines malware, which is short for malicious software, in their glossary of key information security terms as "A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.". (NIST, 2013) Malware is also commonly used as an umbrella term for viruses, worms, Trojan horses, adware, spyware, and other code-based malicious entities. While all the previously mentioned malware is unwanted, differencing between viruses, worms, and Trojans is advisable to help communication. Virus is a program, that hooks itself into another program becoming part of it, and spreads from one computer to another. Viruses almost always are executable files, and require user interaction to be

executed. Worms are similar to viruses, as they too want to spread and infect other devices, but they are more autonomous and try to infect others by exploiting vulnerabilities in target system, for example outdated services or outdated browser plugins. Trojan horses are usually made to look like something else to trick the user to execute the malicious code. Trojan is also used as a concept meaning malicious code that gives attacker a backdoor access to the system. Trojans are usually more targeted and do not spread by themselves, but any of these malicious programs may have characteristics from other groups, making labeling malicious programs hard, hence umbrella term malware.

While it is typical for malware to be spread in executable format, it can be spread in other ways. PDF-format is a common way to send documents, and they may contain JavaScript and elements used to exploit vulnerabilities in PDF-readers like Adobe Reader to install download and install malware in the targets computer. Images might contain malicious code hidden in them using steganography (Mosuela, 2016), or they might contain runnable script code that is decoded and executed for instance by a web browser (Shah, 2015).

As an example, from 2011, ZeroAccess is an extremely persistent and dangerous malware. It could be categorized as a Trojan horse, as it spreads by pretending to be something that user wants, by malvertising, and by third party installing it to targeted computer. ZeroAccess adds the infected computer as part of the ZeroAccess botnet, but its main purpose is to mine bitcoins and perform click frauds to make money to the attackers. ZeroAccess is extremely persistent. It uses advanced rootkit abilities to hide itself to the computer and making removal very hard. Microsoft led an attack to take down ZeroAccess command & control (C&C) servers, but the attack fell short, and some C&C servers persisted, and in addition, ZeroAccess has P2P component, meaning infected devices could still be updated to contact new C&C servers. (Symantec, 2013)

Back in 3.5 we wrote about Stuxnet, which was sophisticated and large malicious program, which is believed to be joint operation by American and Israel. It was first modern state sponsored malware that was brought into public discussion (The Economist, 2010), and after that there has been more reveals, for example Flame and Duqu. Stuxnet however posed no actual danger to regular users, as it was targeted against very specific target and required multiple things, such as Siemens S7 PLC to be connected to device for the malware to do anything. Stuxnet used extremely advanced detection avoidance techniques, such as stolen signed legitimate certificates, advanced rootkits, and 4 different 0-day vulnerabilities, making it next to impossible to defend against.

Malware has followed normal software trends, and become Software-as-a-Service (SaaS). Interested parties can purchase attacks, attacking tools, or infected computers for a price. There exist commercial exploit toolkits that are being utilized with malvertisement campaigns by attackers, e.g., Blackhole, MPack and Angler. Prices for example to Blackhole Exploit Kit went for $1500 USD annually or $50 USD for a day in 2012 (Grier et al., 2012).

3.9.2 Protecting against malware

Typical ways for malware to spread are spam, malvertising, and downloading that appears to be legitimate but turns out to be malware. Some e-mail service providers have high quality spam filters configured out of box, while some require users to setup and use their own. Changing to e-mail provider that offers good protection against spam might be the easiest way to lower the amount of spam getting through to the inbox folder. Other way is to use e-mail client like Microsoft Outlook or Mozilla Thunderbird, or use third-party program like Apache SpamAssassin to filter out spam. Even when using spam filter, there is chance that some spam will pass through, so in the end it is user responsibility to distinguish between legitimate mail and spam. Not all spam contains malware, but spam may contain malware as an attachment, or as a link to site that tries to infect the visitor. Not clicking unexpected links and attachments is very cheap and efficient way to protect against malware spreading by e-mail. However, differentiating between spam and legitimate unexpected mail may be difficult, especially if users act in rush. Even more so, if the mail is not an ordinary spam, but phishing, or even spear phishing. Wang et al. found that knowledge about phishing plays major role in phishing detection (Wang et al., 2012), so educating users and making users aware that such dangers exists is a step forward. Another way for malware to spread is through vulnerabilities in services, plugins, operating system, or other running software. Users should disable unused services in systems to minimize possible targets for attackers. For example, running ftp-server can result in system being compromised if attacker finds or knows about vulnerability in the ftp-server. Vulnerabilities in browsers were gone through more in-depth back in 3.7.

Anti-malware programs typically scan computer against known fingerprints of malware, which are gained by analyzing identified samples of said malware. This provides very low number of false alerts and can identify known malware very efficiently. However, as described in 3.1, since even slightest change in file is enough to provide completely different hash, it is easy to generate malware with different fingerprint and avoid detection. To battle this, anti-malware applications use heuristic methods to detect activity or file patterns like that of malware. This however may result in false alarms, as some applications may have some characteristics that of malware, for example they may inject themselves into another program, but be completely legitimate. It is in users' judgement to set heuristic detection to lighter or stricter mode. Besides anti-malware applications, some browser plugins provide additional security against malware, for example, µBlock Origin has filter lists to block browser accessing known malicious domains before it can load anything from there, helping in battle against malvertising, which was gone through in chapter 3.6.

Taking regular backups should also be practiced, as it will come handy if the system is being taken as a hostage by malware, that encrypts important files and asks ransom in return of the files, also known as ransomware. Backups should be kept in external device that is only attached to the system when the

backups are being made. If the drive used for backups is constantly attached or accessible, the ransomware can encrypt the backup files among other important files, rendering whole backup process worthless.

Despite using best practices and educating users, no system is ever completely secure. As Gene Spafford, professor at Purdue University and analyzer of one of the earliest computer worms, once stated, "The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards – and even then I have my doubts."(Dewdney, 1989). Also, quoting Bruce Schneier, "History has taught us: never underestimate the amount of money, time, and effort someone will expend to thwart a security system."(Schneier, 1997). However, even if it's safe to assume that resourceful attacker can and will gain access to the system if they really want, it is also worth noting that attacker will make their own profitability analysis, meaning it is unlikely that they would spend years trying to attack users' devices just to read their e-mails or to delete their photos. Being aware of possible dangers, keeping software updated, disabling unused services, being mindful when downloading files, and using anti-malware applications, browser plugins, and firewall provide users with good basic security against most attackers.

3.10 Social engineering

This chapter explains what is social engineering, common aspects of it, example case of social engineering in practice, and some ways to defend against it. NIST defines social engineering as an attempt to trick someone into revealing information that can be used to attack systems or networks, or as a process of attempting to trick someone into revealing information (NIST, 2013). Christopher Hadnagy, lead developer of social engineering framework, defines social engineering as "act of manipulating a person to take actions that may or may not be in the target's best interest" (Hadnagy, 2010, p. 10). Social engineering attacks can vary from basic attacks like spoofing e-mail address and then asking for valuable information from the target, to the more elaborate schemes where attacker collects information for weeks, builds rapport to multiple persons, impersonates someone, and gains information without anyone noticing anything unusual.

Social engineering attacks are usually seen as socio-technical acts, because the attacks usually are combination of psychological approaches and technical parts, for example, in the study by Ticher et al. (2016) mentioned in chapter 3.5, they spread USB flash drives around campus with different labels to attract interest and curiosity of the people to stick unknown flash drive to their computer. Another example of the socio-technical attack is spear phishing, where the attacker carefully forms phishing e-mail designated just for the target. The initial contact might not even be dangerous per se, but used to raise interest in the target and lower suspicions. Hadnagy writes in his book about a case, where penetration tester was tasked to gain access to company's systems, but it proved to

be hard. He then found that the high-ranking corporate official was interested in stamps from 1950s, so he registered stamp related domain, called the official, told him that he saw in the forum-site that the target was interested in 1950s stamps, that his grandfather had recently passed and that he was left with collection of them, and that he could send him link with more information if his interested. The target was interested, and the penetration tester then sent a message with a link to the site that would ran bunch of exploits against common browsers and plugins, and the target now expecting the message clicked the link as soon as the message arrived, resulting in the company network being compromised. (Hadnagy, 2010, pp. 23–24)

Attackers usually tend to use one or more of the six basic tendencies of human nature, as theorized by Robert Cialdini. First of the six items is reciprocity, meaning people tend to return a favor, because we feel inclined to. Second is consistency, meaning that people have tendency to comply if they have made oral or written commitment to idea or goal, because we don't want to appear untrustworthy. Third is social validation or social proof, meaning people will do things if they see or hear that other people are doing it too. Fourth is authority, as in people will comply if the request comes from someone with authority, or they believe that the person authority to do such a request. Fifth is liking, meaning that users have tendency to comply if they like the person making the request, or the person has similar interests and beliefs as victim. Sixth is scarcity, which means that object in question is limited in amount and is highly sought on. (Mitnick & Simon, 2002)

Besides being used to attack more or less directly, social engineering can also be used to sow distrust between people and the main target, and even get ordinary people to attack the target. For example, if attacker wants to take down online bank, they might make fake articles and fake pictures that work as a proof that the bank is owned by horrible person, and then provoke people on online forums and social media by posting links to those articles and pictures under multiple different names, and by providing tools to attack the bank, like link to software used to perform denial of service attacks, (e.g., Low Orbit Ion Cannon) and basic tutorial on how to use it. This has already happened on some extent on Estonia in 2007, when a large scale cyber-attack was orchestrated against a nation (Caso, 2014). However, this goes beyond the scope of this topic, as it is more in the field of information- or cyber-warfare.

Hadnagy's suggestions to prevent and mitigate social engineering attacks are learning to identify social engineering attacks, creating personal security awareness culture to organization, keeping software updated, and being aware of the value of the information you are being asked for. These suggestions are in line with results from Greitzer et al., who suggest minimizing stress to avoid making mistakes in haste, encouraging healthy security culture, and developing training and awareness programs (Greitzer et al., 2014). Lorenz and Kikkas also propose awareness as main solution to prevent the success of social engineering attacks (Lorenz & Kikkas, 2012). Mitnick & Simon write that key to prevent and mitigate social engineering attacks is through technology, awareness and train-

ing, and procedures (Mitnick & Simon, 2002). Not one of those alone is enough, as no technology can prevent humans from leaking vital information, and no human can defend everything without technical solutions. Social engineering is in a way a sum of all previous topics. Attacker may utilize e-mail to phis passwords, tailgate employee to company premises, login physically on company computer or find unlocked computer, exploit vulnerability on outdated software to gain escalated access on system, install Trojan on computer from USB flash drive, and then leave as quietly as they came. Here, not falling for phishing, not allowing personnel without ID-tag to enter company premises, not leaving computers unlocked, keeping software updated, and having working anti-malware application could have prevented the attack.

4 DEVELOPED QUESTIONS

In this chapter, we develop questions based on previous research, explicate their importance, and reason why they should be used to measure users' information security awareness. The questions are formed to be answered in Likert 5 scale (1 = Strongly Disagree, 2 = Slightly Disagree, 3 = Neither Agree Nor Disagree, 4 = Slightly Agree, 5 = Strongly Agree).

First question (Q1) is "My friends or family are more likely to crack my password than someone I do not know.". The purpose of this question is to see if users know whether password are cracked programmatically after security breach on some site they have used, or do they think they are being cracked guessing by someone they know. While it is possible that for example their spouse might try and guess their social media accounts password to read their private messages, it is more likely that random attacker gains access to database files from some site and cracks their password.

Second question (Q2) is "It doesn't matter if I use same password on many services if the password is very strong.". Ives et al. argue that users who reuse passwords usually fail to realize that their other accounts are not any more secure than their other accounts where they reuse that password (Ives et al., 2004). Even if user login data is properly secured with e.g., PBKDF2 with high amount of iterations, 241000 hashes per second is entirely possible cracking speed (Gosney, 2015), and is almost certainly even higher depending on implementation and iteration count. Taylor Hornby has combined "Human Passwords"–list that contains 64 million different passwords from various leaks (Hornby, 2016), which is a good starting point, considering that most used passwords in 2016 still include "123456", "password" and "qwerty" (Cooper, 2016). Testing leaked hash against said list with previously given speed would about 4 minutes 25 seconds. If attacker would target just one specific user, they could try 20,8 billion passwords in previously mentioned conservative speed. To compare, English language has about 470000 words (Merriam-Webster, 2015), meaning that testing against all those would take bit under 2 seconds.

Question three (Q3) is "Email attachments may contain malicious content even when they appear to come from known source.". As mentioned in 3.2, e-

mail addresses can be spoofed, the password of the sender could have been leaked, the could have worm that sends itself to other people in the mail book, or the user could just be mischievous. It is also possibility, that the sender doesn't know that the attachment is infected, because they do not have anti-malware applications, or the malware at hand is new and quiet enough to pass undetected.

Fourth question (Q4) is "Opening e-mail is always safe if you do not open attachments.". There are few possible damages caused by opening e-mail, even when not opening the attachments. First, the application used to read the e-mail could have vulnerability, that is triggered by the e-mail. Secondly, unless set otherwise, opening the e-mail may load external images, which may be used to verify that the e-mail was opened, meaning the e-mail address is a valid, and may be now targeted more carefully, or just spammed more.

Question number 5 (Q5) is "Attacker can read your e-mails if you use unsecured wireless network even if you use secured connections to (https) websites.". While we would never recommend anyone to use unsecured wireless network, as it presents many attack points and any unsecured connections may be intercepted by attackers, using for example Google Gmail via TLS-secured https protocol should be safe even in unsecured network. While the attacker can most certainly capture the traffic, they can't read the contents. This is because the traffic is encrypted end-to-end, meaning attacker would first have to break the TLS encryption before they could read the contents. While there are some known attacks against TLS, it is still considered to be secure.

Sixth question (Q6) is "Securing your workstation from the malware is above all a technical issue.". While technical systems play important role on keeping unauthorized personnel out, detecting malware, and keeping data secure, security is first and foremost a human issue. No security system can keep humans from leaking the information, or acting in a way which renders those said security systems useless. For example, door may have best locks in the world, but humans may still use wedge to keep the door from closing, allowing anyone to enter. Users need to be aware of the issues, and be motivated to act accordingly.

As for the question number seven (Q7) "People I do not recognize walking around the office pose no danger to information security, because they don't know passwords to the computers." Having unnecessary people on the premises is a security risk, because there is no knowing what is their agenda. They might steal items, they might plug key loggers to the computers, they might destroy devices, or they might be performing social engineering attack. They might even know a username and password pair from prior social engineering attack, and now come to pick up the data they could not retrieve from outside network.

Eighth question (Q8) is "Inserting USB stick to a computer can be dangerous even if you don't open anything.". As we wrote in 3.5, there are devices that look like USB flash drives, but when inserted to the computer, they appear as a keyboard, and are free to enter and type commands with same privileges as the

user. Dedicated computer that is not connected to the network or the Internet should be set up to verify contents of unknown USB devices. Also, even if it were USB flash drive, it might have been set to autorun malware components. Some anti-malware applications allow blocking autorun features of CD's and USB flash drives, and those should be enabled unless they are absolutely needed.

Question number 9 (Q9) is "Visiting a website is safe if you don't click or download anything.". Just by visiting website, browser executes many different scripts used to make site responsive, visually more pleasant, and add features. They may also be used to track user's actions, like clicked links, where their cursor moved, and how long they stayed per page, as well as displaying ads. There is possibility that the site has been hacked, and it tries to exploit every visitor's browser and its plugins to infect them with some malware. Even if the site itself is clean, the ads the site displays might be used to spread malware.

Tenth question (Q10) is "Using latest version of the software should be preferred, as it usually contains latest vulnerability fixes.". As discussed in chapter 3.7, updated software and operating systems are vital for keeping the system secure, and outdated vulnerable applications are one of the main ways for attacker to infect the user. Unless it is necessary to use old version, for example for the sake of removed functionality in newer versions or for the sake of compatibility, newer version should be used. If the older version is used, other safety measures such as blocking the applications access to network or using it on the device that is not connected to the Internet should be applied.

Question eleven (Q11) is "Smartphone operating systems are different from computer operating systems so they can't get infected.". Smartphone operating systems are not anymore that much different than typical computer operating systems. Ubuntu can be used on smartphones, and laptops using Android OS have been around for years. Smartphones are also very common, they contain lots of information, and they can be used to make payments, so it is only natural that malware industry pays attention to smartphones too.

For the twelfth question (Q12) "PDF-files and images are safe because they don't execute anything." We discussed PDF-files in 3.9.1, and as explained, they may be used to attack PDF-readers to spread the actual malware, and images may contain malicious elements. It is not reasonable to expect for every user to become expert in steganography and malware forensics, but users should be cautious, be mindful what they open and from where, and to use anti-malware application to detect what is possible to detect. This is might be considered as a trick question, and should probably be dismissed if the targeted audiences technical level is very low.

- My friends or family are more likely to crack my password than someone I do not know.
- It doesn't matter if I use same password on many services if the password is very strong.

- Email attachments may contain malicious content even they appear to come from known source
- Opening e-mail is always safe if you do not open attachments
- Attacker can read your e-mails if you use unsecured wireless network even if you use secured connections (https) to websites
- Securing your workstation from the malware is above all a technical issue
- People I do not recognize walking around the office pose no danger to information security, because they don't know passwords to the computers.
- Inserting USB stick to a computer can be dangerous even if you don't open anything
- Visiting a website is safe if you don't click or download anything.
- Using latest version of the software should be preferred, as it usually contains latest vulnerability fixes.
- Smartphone operating systems are different from computer operating systems so they can't get infected.
- PDF-files and images are safe because they don't execute anything.
- Removed files are extremely difficult to recover.
- Hiding the wireless network and using whitelist MAC-address filtering is efficient but hard way to protect network.
- Well-known and popular websites are safe or they wouldn't be popular.
- If it is very urgent, updates to software and operating system are often sent by e-mail.
- Apple's Mac computers are inherently safe from viruses and other malicious programs.
- Re-installing operating system removes all malicious programs from the device.
- If you use 2-factor authentication, you don't need to worry about using strong passwords.
- Police can lock computers remotely if they notice illegal activities, and request payment for opening them.

Measuring abstract concept such as knowledge of a thing is much harder than measuring something concrete such as length or weight, and the fact that the measured concept consists of multiple topics that are even by themselves very broad and difficult makes measuring reliably even harder. By utilizing the concept analysis and identifying core features, we could find some topics that could work as a frame to build upon the rest of the questionnaire. These developed questions are from most addressed topics, meaning they should be quite universal topics. However, we would like to second the issue addressed by many researchers, that one size does not fit all, meaning that while these are important issues, some issues are more critical in some environments than in others. For example, if the organizations computers are all Apple’s Mac com-

puters, it may be redundant to make questions about Windows devices, and vice versa. Questions should be selected or formed the targeted audience in mind. It should be noted that even within company there might be reason to emphasize different topics between different user groups, for example between software developers and upper management. To obtain most interested from users, awareness programs should be used to raise knowledge about issues relevant to the users, which means the questions testing the awareness should be relevant too.

5 CONCLUSIONS

The aim of this thesis was to develop questions to measure information security awareness. The questions were to be well-argued and relevant for the users. We used concept analysis to identify features of information security awareness, and studied the existing research of the identified features to see what aspects of those features are crucial, and to which users can affect by knowing more about and by altering their behavior. This was to result in body of knowledge, of which we then could develop sample questions.

Research method in this thesis was concept analysis as described by Puusa (2008), which is based on book by Walker and Avant (1988), which bases on work of Wilson (1969). Concept analysis was chosen because it allows researcher to utilize their existing knowledge and interest of the subject to fullest, and was deemed to generate interesting results. As a result of the concept analysis, we formed a list of identified features and how they were addressed in the literature. To formed body of knowledge of studying those topics was then used to develop and argue for 12 sample questions with 8 additional suggestions.

Limitations exist in the research. First, the developed questions are examples and merely a frame of the questionnaire used to test for information security awareness. We argue that developing one standard test that would work for every user group would be impossible, as different user groups have different needs and different base knowledge. However, some topics are more critical, common, and relevant than some in most organizations, and identifying those is what we hope to have achieved here. Secondly, testing the validity of the questions is left out of the thesis, and may be performed as a future research.

Our research provides base of knowledge that is usable for other researchers aiming to do research related to information security awareness and its training programs. Our research and developed questions should also give good starting point for practitioners to begin forming information security awareness testing questionnaires and training program topics. The results of feature identification yielded similar topics to what most used papers had. Many papers however didn't use all the features, which is understandable, considering that it is recommended for ISA questionnaires and training programs

to be targeted, and not all topics are relevant for all audiences. However, we would argue that the ten topics gone through in chapter three should constitute the frame of most ISA programs, as failing any one of those is dangerous enough to result in loss of information security.

Obvious problem in the results is that we went through research about information security awareness to provide better questions to measure information security awareness, which is in a sense recursive method. We could have chosen different main concept, such as information security or information system to identify aspects that should be covered. However, our research might also be seen as a sort of cumulative approach, since we have combined results and best practices of previous researches to provide best guidelines and most critical topics.

Testing and comparing the developed questions to other information security awareness raising and training programs would provide topic for another study. One study might be about interviewing users and testing whether they understand the formed questions in the way they are supposed to understand them. Especially with non-technical users, it might provide interesting insights to users' way of thinking and reasoning. Testing whether users know their biggest gaps in knowledge might also provide interesting results in this sector. Asking users what they think their current level is, on what areas they think they have most knowledge about, and then comparing it to the set of questions like we have provided might provide some insight on how well users can identify their need for training, and whether they estimate their level of knowledge above or below the results.

REFERENCES

44 U.S. Code § 3542. Retrieved from https://www.gpo.gov/fdsys/pkg/PLAW-113publ283/html/PLAW-113publ283.htm

Adams, A., & Sasse, M. (1999). Users Are Not The Enemy. *Communications of the ACM*, *42*(12), 41–46.

Akhawe, D., & Felt, A. P. (2013). Alice in warningland: a large-scale field study of browser security warning effectiveness. *Proceedings of the 22nd USENIX Security Symposium*, 257–272.

Al-Hamdani, W. a. (2006). Assessment of need and method of delivery for information security awareness program. *Proceedings of the 3rd Annual Conference on Information Security Curriculum Development - InfoSecCD '06*, 102. https://doi.org/10.1145/1231047.1231069

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers and Security*, *29*(4), 432–445. https://doi.org/10.1016/j.cose.2009.12.005

Aloul, F. (2010). The Need for Effective Information Security Awareness. *International Journal of Intelligent Computing Research (IJICR)*, *1*(3), 130–137.

Amamra, A., Talhi, C., & Robert, J. M. (2012). Smartphone malware detection: From a survey towards taxonomy. *Proceedings of the 2012 7th International Conference on Malicious and Unwanted Software, Malware 2012*, 79–86. https://doi.org/10.1109/MALWARE.2012.6461012

Amankwa, E., Loock, M., & Kritzinger, E. (2016). Enhancing information security education and awareness: Proposed characteristics for a model. *2015 2nd International Conference on Information Security and Cyber Forensics, InfoSec 2015*, 72–77. https://doi.org/10.1109/InfoSec.2015.7435509

Awawdeh, S. Al, & Tubaishat, A. (2014). An Information Security Awareness Program to Address Common Security Concerns in IT Unit. In *2014 11th International Conference on Information Technology: New Generations* (pp. 273–278). IEEE. https://doi.org/10.1109/ITNG.2014.67

Axon, S. (2010). Don't Get Robbed: Burglars Use Facebook to Pick Targets. *Mashable*. Retrieved from http://mashable.com/2010/09/11/facebook-places-burglars/#swrbOeVkciqJ

Ayodele, T., & Adeegbe, D. (2013). Cloud based emails boundaries and vulnerabilities. *Proceedings of 2013 Science and Information Conference, SAI 2013*, 912–914. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84892543507&partnerID=40&md5=58ba52ad49a33735ddfa984d239dc271

Balogh, Š., & Mydlo, M. (2013). New possibilities for memory acquisition by enabling DMA using network card. *Proceedings of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems, IDAACS 2013*, *2*(September), 635–639.

https://doi.org/10.1109/IDAACS.2013.6663002

Barton, B. F., & Barton, M. S. (1984). User-friendly password methods for computer-mediated information systems. *Computers & Security*, *3*(3), 186–195. https://doi.org/10.1016/0167-4048(84)90040-3

Bashorun, A., Worwui, A., & Parker, D. (2013). Information security: To determine its level of awareness in an organization. *AICT 2013 - 7th International Conference on Application of Information and Communication Technologies, Conference Proceedings*. https://doi.org/10.1109/ICAICT.2013.6722704

Baxter, G. J., Connolly, T. M., Stansfield, M. H., Gould, C., Tsvetkova, N., Kusheva, R., … Dimitrova, N. (2011). Understanding the pedagogy Web 2.0 supports: The presentation of a Web 2.0 pedagogical model. In *2011 7th International Conference on Next Generation Web Services Practices* (pp. 505–510). IEEE. https://doi.org/10.1109/NWeSP.2011.6088231

Bazrafshan, Z., Hashemi, H., Fard, S. M. H., & Hamzeh, A. (2013). A survey on heuristic malware detection techniques. In *The 5th Conference on Information and Knowledge Technology* (pp. 113–120). IEEE. https://doi.org/10.1109/IKT.2013.6620049

Bechtsoudis, A., & Sklavos, N. (2012). Aiming at higher network security through extensive penetration tests. *IEEE Latin America Transactions*, *10*(3), 1752–1756. https://doi.org/10.1109/TLA.2012.6222581

Benenson, Z. (2016). Exploiting Curiosity and Context. Retrieved September 4, 2016, from https://www.blackhat.com/docs/us-16/materials/us-16-Benenson-Exploiting-Curiosity-And-Context-How-To-Make-People-Click-On-A-Dangerous-Link-Despite-Their-Security-Awareness.pdf

Benenson, Z., Gassmann, F., & Landwirth, R. (2016). *One in two users click on links from unknown senders*. Erlangen. Retrieved from https://www.fau.eu/2016/08/25/news/research/one-in-two-users-click-on-links-from-unknown-senders/

Black, J., Cochran, M., & Highland, T. (2006). A Study of the MD5 Attacks: Insights and Improvements. In *Fast Software Encryption* (pp. 262–277). https://doi.org/10.1007/11799313_17

Black Hat USA. (2014). BRIEFINGS - AUGUST 6 & 7. Retrieved August 12, 2016, from https://www.blackhat.com/us-14/briefings.html

Bookman, C. (2003). *Linux Clustering: Building and Maintaining Linux Clusters*. Sams Publishing. Retrieved from https://books.google.com/books?id=CxPZ4DLvo_QC&pgis=1

Brodie, C. (2009). The Importance of Security Awareness Training. *Sans Institute*, 27.

Brown, J., Anwar, M., & Dozier, G. (2016). Detection of Mobile Malware : An Artificial Immunity Approach, 74–80. https://doi.org/10.1109/SPW.2016.32

Campbell, J., Kleeman, D., & Ma, W. (2011). Impact of restrictive composition policy on user password choices. *Behaviour & Information Technology*, *30*(3), 379–388. https://doi.org/10.1080/0144929X.2010.492876

Caso, J. S. (2014). The rules of engagement for cyber-warfare and the Tallinn

Manual: A case study. In *The 4th Annual IEEE International Conference on Cyber Technology in Automation, Control and Intelligent* (pp. 252–257). IEEE. https://doi.org/10.1109/CYBER.2014.6917470

Cherdantseva, Y., & Hilton, J. (2013a). A Reference Model of Information Assurance & Security. *2013 International Conference on Availability, Reliability and Security*, 546–555. https://doi.org/10.1109/ARES.2013.72

Cherdantseva, Y., & Hilton, J. (2013b). Information Security and Information Assurance. In *Organizational, Legal, and Technological Dimensions of Information System Administration* (pp. 167–198). IGI Global. https://doi.org/10.4018/978-1-4666-4526-4.ch010

Chiasson, S., Oorschot, P. van, & Biddle, R. (2007). Graphical password authentication using cued click points. *Computer Security–ESORICS …*, *4734*(September), 359–374. https://doi.org/10.1007/978-3-540-74835-9_24

Chu, C., & Florio, E. (2014). Security Advisory 2953095: recommendation to stay protected and for detections. Retrieved December 28, 2016, from https://blogs.technet.microsoft.com/srd/2014/03/24/security-advisory-2953095-recommendation-to-stay-protected-and-for-detections/

Cisco. (2009). Best Practices for Business Class E-mail: Encryption, Authentication, and Control. Retrieved February 21, 2016, from http://www.cisco.com/c/en/us/about/security-center/best-practices-business-class-e-mail.html

Common Sense. (2015). The Common Sense Cencus: Media use by tweens and teens. Retrieved from https://www.commonsensemedia.org/research/the-common-sense-census-media-use-by-tweens-and-teens

Cooper, D. (2016). Too many people still use terrible passwords. Retrieved October 3, 2016, from https://www.engadget.com/2016/01/19/worst-passwords-2015/

Cotroneo, D., Pecchia, A., & Russo, S. (2013). Towards secure monitoring and control systems: Diversify! *Proceedings of the International Conference on Dependable Systems and Networks*, 4–5. https://doi.org/10.1109/DSN.2013.6575341

Criscione, C., Bosatelli, F., Zanero, S., & Maggi, F. (2014). ZARATHUSTRA: Extracting Webinject signatures from banking trojans. In *2014 Twelfth Annual International Conference on Privacy, Security and Trust* (pp. 139–148). IEEE. https://doi.org/10.1109/PST.2014.6890933

Cubrilovic, N. (2009, December 14). RockYou Hack: From Bad To Worse. *TechCrunch*. Retrieved from http://techcrunch.com/2009/12/14/rockyou-hack-security-myspace-facebook-passwords/

Dewdney, A. (1989). Computer Recreations: Of Worms, Viruses and Core War. *Scientific American*.

Dhinakaran, C., Lee, J. K., & Nagamalai, D. (2009). "Reminder: please update your details": Phishing Trends. In *2009 First International Conference on Networks & Communications* (pp. 295–300). IEEE. https://doi.org/10.1109/NetCoM.2009.86

Donnelly, C., & Scaff, R. (2016). Who are the Millennial shoppers? And what do they really want? Retrieved March 24, 2016, from https://www.accenture.com/us-en/insight-outlook-who-are-millennial-shoppers-what-do-they-really-want-retail.aspx

Dougherty, C. (2008). MD5 vulnerable to collision attacks. Retrieved February 4, 2016, from http://www.kb.cert.org/vuls/id/836068

Duo Labs. (2014). Duo Security Researchers Uncover Bypass of PayPal's Two-Factor Authentication. Retrieved October 3, 2016, from https://duo.com/blog/duo-security-researchers-uncover-bypass-of-paypal-s-two-factor-authentication

Enisa. (2010). The new users' guide: How to raise information security awareness. *Information Security*. https://doi.org/10.2824/19110

ENISA. (2009). *ENISA ' s ten security awareness good practices*. https://doi.org/10.2824/12769

Ericsson. (2016). MOBILITY REPORT, (September). Retrieved from https://www.ericsson.com/res/docs/2016/mobility-report/emr-interim-september-2016.pdf

Eshmawi, A., & Nair, S. (2013). Smartphone applications security: Survey of new vectors and solutions. In *2013 ACS International Conference on Computer Systems and Applications (AICCSA)* (pp. 1–4). IEEE. https://doi.org/10.1109/AICCSA.2013.6616461

Farooq, A., Isoaho, J., Virtanen, S., & Isoaho, J. (2015). Information Security Awareness in Educational Institution: An Analysis of Students' Individual Factors. In *2015 IEEE Trustcom/BigDataSE/ISPA* (pp. 352–359). IEEE. https://doi.org/10.1109/Trustcom.2015.394

Farooq, A., & Kakakhel, S. R. U. (2013). Information Security Awareness: Comparing perceptions and training preferences. In *2013 2nd National Conference on Information Assurance (NCIA)* (pp. 53–57). IEEE. https://doi.org/10.1109/NCIA.2013.6725324

Florencio, D., & Herley, C. (2007). A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web - WWW '07* (p. 657). New York, New York, USA: ACM Press. https://doi.org/10.1145/1242572.1242661

Florêncio, D., Herley, C., & Coskun, B. (2007). Do strong web passwords accomplish anything? *Security*, 10. Retrieved from http://portal.acm.org/citation.cfm?id=1361419.1361429

Fuchs, L., Pernul, G., & Sandhu, R. (2011). Roles in information security – A survey and classification of the research area. *Computers & Security*, *30*(8), 748–769. https://doi.org/10.1016/j.cose.2011.08.002

Gaw, S., & Felten, E. W. (2006). Password management strategies for online accounts. In *Proceedings of the second symposium on Usable privacy and security - SOUPS '06* (p. 44). New York, New York, USA: ACM Press. https://doi.org/10.1145/1143120.1143127

Gehringer, E. F. (2002). Choosing passwords: security and human factors. In *IEEE 2002 International Symposium on Technology and Society (ISTAS'02). Social Implications of Information and Communication Technology. Proceedings*

(Cat. No.02CH37293) (pp. 369–373). IEEE. https://doi.org/10.1109/ISTAS.2002.1013839

Goodin, D. (2015, November). Hacking tool swipes encrypted credentials from password manager. *Ars Technica*. Retrieved from http://arstechnica.com/security/2015/11/hacking-tool-swipes-encrypted-credentials-from-password-manager/

Gosney, J. M. (2015). 8x GTX Titan X cudaHashcat Benchmark. Retrieved February 4, 2016, from https://gist.github.com/epixoip/63c2ad11baf7bbd57544

Grawemeyer, B., & Johnson, H. (2011). Using and managing multiple passwords: A week to a view. *Interacting with Computers*, *23*(3), 256–267. https://doi.org/10.1016/j.intcom.2011.03.007

Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D., & Cowley, J. (2014). Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits. *2014 IEEE Security and Privacy Workshops*, 236–250. https://doi.org/10.1109/SPW.2014.39

Grier, C., Pitsillidis, A., Provos, N., Rafique, M. Z., Rajab, M. A., Rossow, C., … Nappa, A. (2012). Manufacturing compromise: The Emergence of Exploit-as-a-Service. In *Proceedings of the 2012 ACM conference on Computer and communications security - CCS '12* (p. 821). New York, New York, USA: ACM Press. https://doi.org/10.1145/2382196.2382283

Hadnagy, C. (2010). *Social engineering : the art of human hacking*. Wiley.

Hak5. (2014). USB Rubber Ducky Project Wiki. Retrieved August 12, 2016, from https://github.com/hak5darren/USB-Rubber-Ducky/wiki

Halderman, J. A., Schoen, S. D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J. a., … Felten, E. W. (2008). Lest We Remember: Cold Boot Attacks on Encryption Keys. *USENIX Security Symposium*, 1–16. https://doi.org/10.1145/1506409.1506429

hashcat. (2015a). hashcat - advanced password recovery. Retrieved February 3, 2016, from http://hashcat.net/hashcat/

hashcat. (2015b). oclHashcat - advanced password recovery. Retrieved January 3, 2016, from http://hashcat.net/oclhashcat/

Heikkinen, S. (2006). Social engineering in the world of emerging communication technologies. *Proceedings of Wireless World Research Forum*, 1–10. Retrieved from http://www.cs.tut.fi/~sheikki/docs/WWRF-Heikkinen-SocEng.pdf

Hornby, T. (2016). CrackStation's Password Cracking Dictionary. Retrieved October 3, 2016, from https://crackstation.net/buy-crackstation-wordlist-password-cracking-dictionary.htm

Ilyin, Y. (2014). A confirmed eBay leak: another password alert. Retrieved February 4, 2016, from https://business.kaspersky.com/a-confirmed-ebay-leak-another-password-alert/1876/

InternetLiveStats.com. (2016). Total number of Websites. Retrieved August 15, 2016, from http://www.internetlivestats.com/total-number-of-websites/

Ives, B. B., Walsh, K. R., & Schneider, H. (2004). Password Reuse.

Communications of the ACM, *47*(4), 75–78.

Jama, A. Y., Siraj, M., & Kadir, R. (2014). Towards Metamodel - based Approach for Information Security Awareness Management. *2014 International Symposium on Biometrics and Security Technologies (ISBAST)*, 316–321.

Jenkins, J. L., Anderson, B. B., Vance, A., Kirwan, C. B., & Eargle, D. (2016). More Harm Than Good? How Messages That Interrupt Can Make Us Vulnerable. *Information Systems Research*, (August). https://doi.org/10.1287/isre.2016.0644

Johanson, M. (2013). How Burglars Use Facebook To Target Vacationing Homeowners. *International Business Times*. Retrieved from http://www.ibtimes.com/how-burglars-use-facebook-target-vacationing-homeowners-1341325

Khan, M., Bi, Z., & Copeland, J. A. (2012). Software updates as a security metric: Passive identification of update trends and effect on machine infection. In *MILCOM 2012 - 2012 IEEE Military Communications Conference* (pp. 1–6). IEEE. https://doi.org/10.1109/MILCOM.2012.6415869

Khan, W. Z., Khan, M. K., Bin Muhaya, F. T., Aalsalem, M. Y., & Chao, H.-C. (2015). A Comprehensive Study of Email Spam Botnet Detection. *IEEE Communications Surveys & Tutorials*, *17*(4), 2271–2295. https://doi.org/10.1109/COMST.2015.2459015

Kim, E. B. (2012). Recommendations for information security awareness training for college students. *Computer Security Computer Security Computer Security Information Technology & People Iss*, *22*(5), 115–126. https://doi.org/10.1108/IMCS-01-2013-0005

Klein, D. V. (1990). Foiling the cracker: A survey of, and improvements to, password security. *Proceedings of the 2nd USENIX Security Workshop*, 5–14. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.149.9721&rep=rep1&type=pdf

Klima, V. (2006). Tunnels in Hash Functions: MD5 Collisions Within a Minute, 17. Retrieved from http://eprint.iacr.org/2006/105.pdf

Krebs, B. (2013). Adobe Breach Impacted At Least 38 Million Users. Retrieved February 4, 2016, from http://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/

Kärkkäinen, H. (2015). Facebook paljasti Suomi-lukuja. *IT-Viikko*. Retrieved from http://www.itviikko.fi/uutiset/2015/04/15/facebook-paljasti-suomi-lukuja/20154707/7

L0pht Holdings LLC. (2012). L0phtCrack Password Auditor - Learn about L0phtCrack. Retrieved February 3, 2016, from http://www.l0phtcrack.com/learn.html

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security and Privacy*, *9*(3), 49–51. https://doi.org/10.1109/MSP.2011.67

Lenhart, A., Madden, M., Smith, A., Purcell, K., Zickuhr, K., Rainie, L., & Project, A. L. (2011). Teens , Kindness and Cruelty on Social Network Sites. *PewResearchCenter*, 1–86. https://doi.org/378

Lindenlauf, S., Hofken, H., & Schuba, M. (2015). Cold Boot Attacks on DDR2 and DDR3 SDRAM, 287–292. https://doi.org/10.1109/ARES.2015.28

Lorenz, B., & Kikkas, K. (2012). Socially Engineered Commoners as Cyber Warriors – Estonian Future or Present ? *Cyber Conflict (CYCON), 2012 4th International Conference on*, 1–12.

Lunden, I. (2012, July 12). Yahoo Confirms, Apologizes For The Email Hack, Says Still Fixing. Plus, Check If You Were Impacted (Non-Yahoo Accounts Apply). *TechCrunch*. Retrieved from http://techcrunch.com/2012/07/12/yahoo-confirms-apologizes-for-the-email-hack-says-still-fixing-plus-check-if-you-were-impacted-non-yahoo-accounts-apply/

Mackenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct Measurement and Validation P Rocedures in Mis and B Ehavioral Research : Integrating New and Existing Techniques. *MIS Quarterly*, *35*(2), 293–334.

Mahadevan, Y., Cangussu, J., & Dantu, R. (2009). Penetration Testing for Spam Filters. *2009 33rd Annual IEEE International Computer Software and Applications Conference*, 410–415. https://doi.org/10.1109/COMPSAC.2009.168

Mahto, D. (2015). Enhancing Security of One-Time Password Using Elliptic Curve Cryptography with Finger-Print Biometric, 301–306.

McCoy, C., & Fowler, R. (2004). "You are the key to security": establishing a successful security awareness program. *Proceedings of the 32nd Annual ACM SIGUCCS Fall Conference SE - SIGUCCS '04*, 346–349. https://doi.org/doi: 10.1145/1027802.1027882

McDaniel, N., Thuraisingham, B., & Khan, L. (2014). Deploying malware detection software for smart phones. In *Proceedings of the 2014 IEEE 15th International Conference on Information Reuse and Integration (IEEE IRI 2014)* (pp. 24–27). IEEE. https://doi.org/10.1109/IRI.2014.7051867

Menczer, A., & Lysunets, A. (2016). DressCode Android Malware Discovered on Google Play. Retrieved September 20, 2016, from http://blog.checkpoint.com/2016/08/31/dresscode-android-malware-discovered-on-google-play/

Merriam-Webster. (2015). How many words are there in English? Retrieved October 4, 2016, from http://www.merriam-webster.com/help/faq-how-many-english-words

Microsoft. (2008). Microsoft Security Bulletin MS08-067 - Critical. Retrieved September 4, 2016, from https://technet.microsoft.com/library/security/ms08-067

Microsoft. (2016). Minimum password length. Retrieved February 4, 2016, from https://technet.microsoft.com/en-us/library/hh994560.aspx

Mitnick, K., & Simon, W. (2002). *The Art of Deception*. (C. Long, Ed.) (First). Indianapolis: Wiley Publishing.

Monk, T., Van Niekerk, J., & Von Solms, R. (2010). Sweetening the Medicine : Educating Users about Information Security by means of Game Play. *Proceedings of the 2010 Annual Research Conference of the South African*, 193–

200. https://doi.org/10.1145/1899503.1899525

Montoro, M. (2014). oxid.it - Cain & Abel. Retrieved February 3, 2016, from http://www.oxid.it/cain.html

Mosuela, L. (2016). How It Works: Steganography Hides Malware in Image Files. Retrieved December 30, 2016, from https://www.virusbulletin.com/virusbulletin/2016/04/how-it-works-steganography-hides-malware-image-files/

Murugesan, S. (2007). Understanding Web 2.0. *IT Professional*, *9*(4), 34–41. https://doi.org/10.1109/MITP.2007.78

Nagarajan, V., Arasan, V., & Huang, D. (2010). Using power hopping to counter MAC spoof attacks in WLAN. *2010 7th IEEE Consumer Communications and Networking Conference, CCNC 2010*, 1–5. https://doi.org/10.1109/CCNC.2010.5421588

Nakhila, O., Attiah, A., Jinz, Y., & Zoux, C. (2015). Parallel active dictionary attack on WPA2-PSK Wi-Fi networks. In *MILCOM 2015 - 2015 IEEE Military Communications Conference* (pp. 665–670). IEEE. https://doi.org/10.1109/MILCOM.2015.7357520

NIST. (2003). *Building an Information Technology Security Awareness and Training Program*. *NIST Special Publication 800-50*. Gaithersburg, MD. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

NIST. (2013). *Glossary of key information security terms*. *NIST IR* (Vol. 7298). Gaithersburg, MD. https://doi.org/10.6028/NIST.IR.7298r2

Openwall. (2010). John the Ripper - wordlist rules syntax. Retrieved February 5, 2016, from http://www.openwall.com/john/doc/RULES.shtml

Openwall. (2015). John the Ripper password cracker. Retrieved February 3, 2016, from http://www.openwall.com/john/doc

Patil, S., Hoyle, R., Schlegel, R., Kapadia, A., & Lee, A. J. (2015). Interrupt Now or Inform Later?: Comparing Immediate and Delayed Privacy Feedback. *Proceedings of the ACM CHI'15 Conference on Human Factors in Computing Systems*, *1*, 1415–1418. https://doi.org/10.1145/2702123.2702165

Peng, S., Yu, S., & Yang, A. (2014). Smartphone malware and its propagation modeling: A survey. *IEEE Communications Surveys and Tutorials*, *16*(2), 925–941. https://doi.org/10.1109/SURV.2013.070813.00214

Pew Research Center. (2015). *The Smartphone Difference*. Retrieved from http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/

Pleasance, C. (2015). Holidaymakers who post information about trips on Facebook face having insurance claims rejected if their home is targeted by burglars while they are away. *Dailymail*. Retrieved from http://www.dailymail.co.uk/news/article-3051671/Holidaymakers-post-information-trips-Facebook-face-having-insurance-claims-rejected-home-targeted-burglars-away.html

Puhakainen, P. (2006). *A design theory for information security awareness*. *Processing*. Retrieved from http://en.scientificcommons.org/13922630

Puusa, A. (2008). Käsiteanalyysi tutkimusmenetelmänä. *Premissi*, 36–43.

Ragan, S. (2016). Need to bypass Google's two-factor authentication? Send a text message. Retrieved from

http://www.csoonline.com/article/3079512/techology-business/need-to-bypass-googles-two-factor-authentication-send-a-text-message.html

RainbowCrack Project. (2015). RainbowCrack - Crack Hashes with Rainbow Tables. Retrieved February 3, 2016, from http://project-rainbowcrack.com/index.htm

Reeder, R., & Consolvo, S. (2015). "... no one can hack my mind": Comparing Expert and Non-Expert Security Practices. *Symposium on Usable Privacy and Security*, 327–346. https://doi.org/10.1080/0888431022000070458

Reid, R., & Van Niekerk, J. (2014). From information security to cyber security cultures. In *2014 Information Security for South Africa* (pp. 1–7). IEEE. https://doi.org/10.1109/ISSA.2014.6950492

RSA. (2016). RSA SECURID ACCESS. Retrieved September 21, 2016, from https://www.rsa.com/en-us/products-services/identity-access-management/securid

Sakib, M. N., & Huang, C.-T. (2015). Automated Collection and Analysis of Malware Disseminated via Online Advertising. *IEEE Trustcom/BigDataSE/ISPA*, 1411–1416. https://doi.org/10.1109/Trustcom.2015.539

Scarfone, K., & Souppaya, M. (2009). Guide to enterprise password management (draft). *NIST Special Publication*, *800*, 118. Retrieved from http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf

Schatzmann, D., Burkhart, M., & Spyropoulos, T. (2009). Inferring Spammers in the Network Core. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 5448, pp. 229–238). https://doi.org/10.1007/978-3-642-00975-4_23

Schneier, B. (1997). Why Cryptography is Harder Than It Looks. Retrieved December 21, 2016, from https://www.schneier.com/essays/archives/1997/01/why_cryptography_is.html

Security Standards Council. (2014). Information Supplement : Best Practices for Implementing a Security Awareness Program. *Security Standards Council*, (October).

Shah, S. (2015). *Stegosploit*. Amsterdam. Retrieved from https://conference.hitb.org/hitbsecconf2015ams/wp-content/uploads/2015/02/D1T1-Saumil-Shah-Stegosploit-Hacking-with-Pictures.pdf

Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., … Cranor, L. F. (2010). Encountering Stronger Password Requirements : User Attitudes and Behaviors Categories and Subject Descriptors. *Proceedings of the Sixth Symposium on Usable Privacy and Security - SOUPS '10*, 1. https://doi.org/10.1145/1837110.1837113

Shikha, Kaushik, V., & Gautam, S. (2013). Wireless LAN (WLAN) spoofing detection methods - Analysis and the victim Silent case. In *2013 INTERNATIONAL CONFERENCE ON SIGNAL PROCESSING AND COMMUNICATION (ICSC)* (pp. 155–160). IEEE. https://doi.org/10.1109/ICSPCom.2013.6719774

Shrestha, B., Ma, D., Zhu, Y., Li, H., & Saxena, N. (2015). Tap-Wave-Rub: Lightweight Human Interaction Approach to Curb Emerging Smartphone Malware. *IEEE Transactions on Information Forensics and Security*, *10*(11), 2270–2283. https://doi.org/10.1109/TIFS.2015.2436364

Siponen, M. (2000). A conceptual foundation for organizational information security awareness, *8*(1), 31–41. Retrieved from http://northumbria.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwY2BQME0zMEoElogWaYlGiSlmhhZpoFPrgCkjzSAx1Qy8SRgxVYBUmrsJMTCl5okyKLm5hjh76MKKxvjEJFCvP7mkOB40SWAJrHAMxRh4E0ErwPNKwDvFUgBerh50

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

Siponen, M., & Vance, A. (2014). Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations. *European Journal of Information Systems*, *23*(3), 289–305. https://doi.org/10.1057/ejis.2012.59

Skracic, K., Petrovic, J., Pale, P., & Tralic, D. (2014). Virtual wireless penetration testing laboratory model. In *Proceedings ELMAR-2014* (pp. 1–4). IEEE. https://doi.org/10.1109/ELMAR.2014.6923370

Steube, J. (2014). PRINCE - modern password guessing algorithm. Retrieved from https://hashcat.net/events/p14-trondheim/prince-attack.pdf

Stevens, M., Karpman, P., & Peyrin, T. (2015). Freestart collision on full SHA-1. In *Cryptology ePrint Archive, Report 2015/967* (pp. 1–21). Retrieved from https://eprint.iacr.org/2015/967

Stewin, P., & Bystrov, I. (2012). Understanding DMA Malware. In *Proceedings of the 9th Conference on Detection of Intrusions and Malware & Vulnerability Assessment*. Crete.

Straub, D. W., & Welke, R. J. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly*, *22*(4), 441. https://doi.org/10.2307/249551

Stubblefield, A., Ioannidis, J., & Rubin, A. (2004). A key recovery attack on the 802.11 b wired equivalent privacy protocol (WEP). *ACM Transactions on Information …*, *V*(2), 1–15. https://doi.org/10.1145/996943.996948

Symantec. (2013). Trojan.Zeroaccess. Retrieved December 21, 2016, from https://www.symantec.com/security_response/writeup.jsp?docid=2011-071314-0410-99

Talib, S., Clarke, N. L., & Furnell, S. M. (2010). An Analysis of Information Security Awareness within Home and Work Environments. In *2010 International Conference on Availability, Reliability and Security* (pp. 196–203). IEEE. https://doi.org/10.1109/ARES.2010.27

Tamir, D. (2014). Cybercriminals Use Citadel to Compromise Password Management and Authentication Solutions. Retrieved February 5, 2016, from http://securityintelligence.com/cybercriminals-use-citadel-compromise-password-management-authentication-solutions/#.VG48s0srf1p

Telegraph Reporters. (2016, March 10). Billion dollar bank heist foiled by hacker's typo. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/technology/2016/03/10/billion-dollar-bank-heist-foiled-by-hackers-typo/

The Economist. (2010). The meaning of Stuxnet. Retrieved from http://www.economist.com/node/17147862

Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E., & Bailey, M. (2016). Users Really Do Plug in USB Drives They Find. In *In Proceedings of IEEE S&P 2016* (pp. 1–14). Illinois: IEEE. https://doi.org/10.1109/SP.2016.26

Tomlinson, S. (2011). How's your social security? Burglars monitor Facebook and Twitter to see when you're away from home. *Dailymail*. Retrieved from http://www.dailymail.co.uk/sciencetech/article-2056079/Hows-social-security-Burglars-monitor-Facebook-Twitter-youre-away-home.html

Tracy, M., Jansen, W., Scarfone, K., & Butterfield, J. (2007). Guidelines on Electronic Mail Security Recommendations of the National Institute of Standards and Technology.

Treanor, J. (2014, October 26). Digital revolution presents banks with more change in 10 years than last 200. *The Guardian*. Retrieved from http://www.theguardian.com/business/2014/oct/26/banks-digital-revolution-change-regulation-job-losses

Trost, R. (2009). *Practical Intrusion Analysis: Prevention and Detection for the Twenty-First Century*. Pearson Education. Retrieved from https://books.google.com/books?id=3y2fhCaJJA0C&pgis=1

Tsai, C. S., Lee, C. C., & Hwang, M. S. (2006). Password authentication schemes: Current status and key issues. *International Journal of Network Security*, *3*(2), 101–115. https://doi.org/10.1109/ICM2CS.2009.5397977

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2010). Aligning Security Awareness with Information Systems Security Management. *Journal of Information System Security*, *6*(1), 36–54.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2012). Analyzing trajectories of information security awareness. *Information Technology & People*, *25*(3), 327–352. https://doi.org/10.1108/09593841211254358

Tsohou, A., Kokolakis, S., Lambrinoudakis, C., & Gritzalis, S. (2010). A security standards' framework to facilitate best practices' awareness and conformity. *Information Management & Computer Security*, *18*(5), 350–365. https://doi.org/10.1108/09685221011095263

U.S. Department of Commerce. (2016). U.S. and World Population Clock. Retrieved from http://www.census.gov/popclock/

Velki, T., Solic, K., & Ocevcic, H. (2014). Development of Users' Information Security Awareness Questionnaire (UISAQ) - Ongoing work. In *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (Vol. 58, pp. 1417–1421). IEEE. https://doi.org/10.1109/MIPRO.2014.6859789

Viehböck, S. (2011). Brute forcing Wi-Fi protected setup. *Wi-Fi Protected Setup*, 9. Retrieved from

https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf

Vu, K.-P. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B.-L. (Belin), Cook, J., & Eugene Schultz, E. (2007). Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies*, *65*(8), 744–757. https://doi.org/10.1016/j.ijhcs.2007.03.007

Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE Transactions on Professional Communication*, *55*(4), 345–362. https://doi.org/10.1109/TPC.2012.2208392

Whitman, M. E., & Mattord, H. J. (2012). *Principles of Information Security, 4th Edition* (4th ed.). Course Technology.

Whitty, B. (2012). Bypass Windows Logons with the Utilman.exe Trick. Retrieved April 20, 2016, from https://www.technibble.com/bypass-windows-logons-utilman/

Wi-Fi Alliance. (2016). Who We Are. Retrieved February 24, 2016, from http://www.wi-fi.org/who-we-are

Witherden, F. (2010). Memory Forensics over the IEEE 1394 Interface, 1–28. Retrieved from https://freddie.witherden.org/pages/ieee-1394-forensics.pdf

Wood, C. (1995). Information Security Awareness Raising Methods. *Computer Fraud and Security Bulletin*, *June*(June), 13–15. https://doi.org/10.1016/0142-0496(95)80197-9

Wu Bin, Lu Tianliang, Zheng Kangfeng, Zhang Dongmei, & Lin Xing. (2014). Smartphone malware detection model based on artificial immune system. *China Communications*, *11*(13), 86–92. https://doi.org/10.1109/CC.2014.7022530

Xin, K., Li, G., Qin, Z., & Zhang, Q. (2012). Malware Detection in Smartphone Using Hidden Markov Model. *International Conference on Multimedia Information Networking and Security*, 857–860. https://doi.org/10.1109/MINES.2012.134

Yan, J., Blackwell, A., Anderson, R., & Grant, A. (2004). Password memorability and security: empirical results. *IEEE Security & Privacy Magazine*, *2*(5), 25–31. https://doi.org/10.1109/MSP.2004.81

Yle. (2016). Parking at the airport could tip off burglars—here's how to stop them. *Yle Uutiset*. Retrieved from http://yle.fi/uutiset/parking_at_the_airport_could_tip_off_burglarsheres_how_to_stop_them/9056642

Yu, F., & Huang, Y. (2015). An Overview of Study of Passowrd Cracking. *Computer Science and Mechanical Automation (CSMA), 2015 International Conference on*, 25–29. https://doi.org/10.1109/CSMA.2015.12

Zhang, L., & McDowell, W. C. (2009). Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords. *Journal of Internet Commerce*, *8*(3–4), 180–197. https://doi.org/10.1080/15332860903467508

Zisiadis, D., Kopsidas, S., Varalis, A., & Tassiulas, L. (2012). Enhancing WPS security. *IFIP Wireless Days*, 1–3.

https://doi.org/10.1109/WD.2012.6402836