jamk.fi

Social engineering against security policy

How to infiltrate company's premises using social engineering?

Miika Sillanpää

Master's thesis
September 2019
Technology, communication and transport
Master's Degree Programme in Information Technology
Cyber Security

jamk.fi

Description

Author(s)	Type of publication	Date
Sillanpää, Miika	Master's thesis	September 2019
		Language of publication: English
	Number of pages 92	Permission for web publication: x

Title of publication

Social engineering against security policy

How to infiltrate company's premises using social engineering?

Degree programme

Master's Degree Programme in Information Technology, Cyber Security

Supervisor(s)

Jari Hautamäki; Jouni Huotari

Assigned by

Abstract

Social engineering is as old as human beings and has been used for a thousand years in some way such as non-verbally and orally. Today it is still a very potential attack vector, and everybody could be its target. The assigner company was a target of social engineering attacks and all techniques and skills used were meant to measure their personnel's resilience to spot and even stop these attacks from occurring. In addition, the results show how dangerous such attacks can be.

The task was to investigate how employees respond and how they work with regard to social attacks. Information about the company was collected passively in order to find out what all potential attackers see on the Internet. Maltego software was used here. In addition, the trend of phishing emails and the connection factors between the most clicked phishing emails were investigated.

The background information was collected through a survey the results of which were analyzed bearing in mind the security policy. The goal was to measure employees' security awareness and culture. Gathering information about the company was the first step. Based on that information, physical penetration cases were created, which measured and compared the information of the survey and the cases. The data of phishing emails was used to identify the trend and connection factors between the most clicked phishing emails.

On paper, the security culture was good; yet, not perfect. The reality differed much from the paper. Publicly available information did not reveal critical information but did provide attack vectors. Social media was the most successful way of phishing email. Social engineering is a real threat to business. The only way to defend against this is to improve the security culture for the first line of defense which in this case is the people themselves.

Keywords/tags (subjects)

Social engineering, security policy, physical penetration, phishing email, reconnaissance

Miscellaneous (Confidential information)

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Sillanpää, Miika	Opinnäytetyö, ylempi AMK	syyskuu 2019
	Sivumäärä 92	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi

Social engineering vastaan tietoturvapolitiikka

Miten päästä yritykseen sisälle käyttäen social engineeringiä?

Tutkinto-ohjelma

Ylempi AMK, kyberturvallisuus

Työn ohjaaja(t)

Jari Hautamäki; Jouni Huotari

Toimeksiantaja(t)

Tiivistelmä

Social engineering on yhtä vanha kuin ihmiset ja sitä on käytetty tuhansia vuosia eri tavoin kuten ei-verbaalisti ja puhumalla. Tänä päivänäkin se on todellinen hyökkäysvektori, ja kuka tahansa voi olla kohde. Yhteistyöyritys oli kohde sosiaalisille hyökkäyksille, ja kaikki käytetyt tekniikat mittasivat yrityksen työntekijöiden kykyä havaita, jopa lopettaa hyökkäys. Lisäksi tulokset näyttävät, miten vaarallisia tällaiset hyökkäykset voivat olla.

Tehtävänä oli tutkia, miten työntekijät reagoivat sosiaalisiin hyökkäyksiin ja miten he toimivat näissä tilanteissa. Yrityksestä kerättiin tietoa passiivisesti, jotta saataisiin tietoon, mitä kaikkea mahdolliset hyökkääjät näkevät Internetistä sekä Maltego -ohjelmistoa käyttämällä. Lisäksi selvitettiin kalastusviestien trendiä sekä yhdistäviä tekijöitä eniten avattujen kalastusviestien välillä.

Lähtökohta kerättiin mielipidekyselyllä, jonka tuloksia analysoitiin tietoturvapolitiikka mielessä. Tämän tarkoitus oli mitata työntekijöiden tietoturvatietoisuutta sekä kulttuuria. Tiedon kerääminen yrityksestä oli ensimmäinen vaihe. Tämän tiedon perusteella tehtiin fyysisiä penetraatiotapauksia, jotka mittasivat ja vertailivat kyselyn ja tapauksien informaatiota keskenään. Kalastusviestien dataa käytettiin hyväksi trendin sekä yhdistävien tekijöiden selvittämiseksi eniten avattujen kalastusviestien välillä.

Paperilla tietoturvakulttuuri oli hyvä mutta ei täydellinen. Todellisuus erosi paljon verrattuna tähän. Julkisesti saatavilla oleva tieto ei juurikaan paljastanut mitään kriittistä mutta antoi hyökkäysvektoreita. Sosiaalinen media oli menestynein tapa kalastushyökkäyksiin. Social engineering on todellinen uhka yrityksille. Ainoa tapa puolustautua tätä vastaan on parantaa tietoturvakulttuuria ensimmäiselle puolustuslinjalle, joka on tässä tapauksessa ihmiset itse.

Avainsanat (asiasanat)

Social engineering, tietoturvapolitiikka, fyysinen penetraatio, kalastus sähköposti, tiedon kerääminen

Muut tiedot

Contents

Figures

Tables

1 Introduction

1.1 Purpose of research

Social engineering has been and will be one of the easiest ways to launch attacks. It is also often the most devastating way. The target could be an individual person, a company or even a government. Because targets of social engineering are other human beings, they are the guardians of the information and possible breach. This means that they need to be aware and know attack patterns and techniques used by the social engineers.

This research evaluates the target company's ability to stop and mitigate possible social engineering attacks by using survey questions to personnel and other social engineering techniques from reconnaissance to physical penetration. Survey questions give the baseline of the personnel security awareness, and social engineering techniques measure how personnel behave when a social engineer launches attacks based on the questions. All attacks and reconnaissance are conducted as black box testing: no internal information is used and only information that a malicious social engineer could get and attacks that malicious social engineer could do are used. This way the real security awareness of the personnel and the security company's premises will be revealed.

All cases and the whole research are carried out with help from one company, so this research evaluates only this company's security and not that of a whole country or other companies. Nevertheless, this can give visibility to other companies as well regarding how devastating a social engineer's attacks could be and how to prevent them.

1.2 Fictional or real case?

An employee gets a phone call from service desk. The service desk has found a malware from the employee's laptop and it is possibly ransomware. According to the service desk, it has not activated yet; however, it will activate later if not removed. The service desk must connect the laptop using remote access to be able

to remove it. The main remote access tool of the service desk has a malfunction and it does not work on the service desk specialist's computer, which is why the employee needs to download another tool for the remote access. It can be downloaded from the internet. If the employee does not download and run it, all the laptop's data can be encrypted and then it is gone. Fear of losing all data and helpful service desk make this request easy to follow and the employee downloads that software and runs it. The remote tool is a new; it has never been tested before and it does not do anything. The service desk apologizes because that software did not work and informs the employee that another service desk specialist with a working remote tool calls the employee immediately and removes that ransomware via remote access. The service desk closes the phone when employee is satisfied that his problem is solved soon.

This is a fictional story made by the author in his own mind; however, this still might have occurred many times before, and it can be assured that this kind of social engineering attack will occur many times in the future. The attack uses social engineering skills such as fear, manipulation, pretext and the most importantly, the trust to lure an employee to do something what he or she should not do. Who would not trust their own service desk or ICT personnel who help fixing all problems in the employees' computers, applications and mobile devices?

Cyber world is a strange place because it is anonymous. One can be who one likes to be or pretend to be somebody else. When one thinks about hackers or black hats who work in the cyber world and attack from there to companies using found vulnerabilities, what does one think about who they are. This could be a big question and maybe one never finds out their identity. The same argument applies to social engineering. The attackers launch their attacks such as phishing mails from the cyber world and one probably never meets them face to face or if one does, one does not know it.

But why are other people attached? Why do hackers or black hats attack them and not companies' devices and systems? Companies' security controls could be so sticky and hardened that it is impossible. One could be hitting one's head in firewalls and does not get through. However, why try to pass an unbreakable device if there is another way to do the same and it is easier? Of course, one attacks to weakest link of

all. Probably the weakest link of all is a human and his/her mind (Diogenes & Ozkaya 2018, 7).

Although social engineering is a very old technique, it is still very well used today in malicious intent. According to Verizon (2018, 8), social engineering techniques, such as phishing and pretexting belong to the top 20 of all incidents and breaches this year so far. The number of confirmed data disclosures out of all 1,450 incidents was 381 (Verizon 2018, 11). Last year the disclosure of information was much higher: 828 of 1616 (Verizon 2017, 32). Neely's survey (2018, 8) indicates that over 50% of all exploits of endpoints (laptops, desktops etc.) used phishing. Even in Finland, phishing is a popular way of trying to gain sensitive information (CERT-FI 2018, 13). Phishing is one of the main tools of social engineering arsenal; however, one should not underestimate all other tools such as pretexting and manipulation.

Who can be a victim of social engineering? The answer is anybody. An employee, CIO, unemployed or even another hacker. Kevin Mitnick's two different accounts have been hacked by script kiddies using social engineering: AOL (Mitnick & Vamosi 2017, 74) and AT&T (Mitnick & Vamosi 2017, 170). Not to mention all "fake" police officers who entered old people's houses to steal or called them to ask for their bank account numbers and PIN-codes in Finland (Karppinen 2018).

The victim may be anybody so who can be a malicious or good social engineer then? Again, the answer is anybody. A reporter of YLE just walked into 10 of 11 companies pretending to be a worker wearing a yellow vest, ladder and speaking on the phone. No questions were asked, people opened the door for him and let him pass. (Jokinen 2017)

Most people may think that social engineering is only for malicious purposes; however, it is not true. Every day and every people use someway social engineering skills in some ways, e.g. asking to do something just to help. One can think about children. They are professionals in social engineering and masters in social engineering skills. What can they do when they just want one candy or something else? They could scream, beg, cry or just be stubborn. If one likes to learn about social engineering, one could just watch and listen to children. The author knows this based on his own experience.

When a social engineer starts to attack a company with a malicious intent or just carries out penetration testing, the company's security devices will not help. Firewalls, Intrusion Detection Systems (IDS) and all other devices will not notice anything. The security devices only see if something bad has occurred; however, in most cases that is often too late. The only security measure against social engineering is users' security awareness, a good security policy and training. (Mitnick & Simon 2002, 245)

If one thinks about the fictional story above and thinks about it with open eyes and memorizes all that was said before, a question should be asked: is that fictional or not? Maybe it is fictional because it is the production of the author's own mind; however, again that could have happened in some way and as said before, that will happen. Maybe not exactly as was written; however, almost similarly.

1.3 Previous studies

There are multiple studies and researches over the years from various institutions and individuals about social engineering and used methods and techniques on it. There is a great amount of literature and books from researchers who have studied persuasion and building rapport many years such as Dr. Robert Cialdini and Robin Dreeke. Dr. Robert Cialdini has studied persuasion his entire career over 30 years: what it means, how it is used and principles of influence (Robert Cialdini n.d.; Cialdini 2016). Robin Dreeke has studied, how to build rapport over his career (Macmillan speakers n.d.; Dreeke 2011). A professional social engineer use these to achieve the goal. Persuasion to another person is must and building rapport is important to gain information and trust.

Phishing is one of the most successful social engineering attack types. It has been studied a great deal and there are many research articles such as Gupta, Singhal & Kapoor (2016) about how to detect phishing and how to defend against of them using education and different solutions. There are studies such as Patil & Dhage (2019) where phishing detection was carried out using software-based with blacklist and machine learning, heuristic tests and many more included features and they were then compared.

Users' education and awareness about phishing are studied as well. One study result was that users with a good knowledge about phishing were the most resistant for that; however, knowledge about negative consequences did not help with phishing. The conclusion of that study was that educating users about phishing attacks is better than warning them about what might happen. (Khonji, Iraqi & Jones 2013, 2097)

There are multiple studies about social engineering attack models stating how attacks occur and how to detect them. Social Engineering Attack Detection Model (SEADM) is one of them. It can be used as a framework to defend against attacks and mitigate or stop them from occurring (Mouton, Nottingham, Leenen & Venter 2018, 146).

How social engineering attacks work, and all its steps are studied as well. This is called a framework. There are multiple different frameworks done to social engineering attacks. Maybe the most common framework is from Kevin Mitnick with four phases and based on that, researchers have created more frameworks.

Social engineering is very wide area to which plenty of information belongs. This attack type most often includes technology as well such as a malicious weblink which needs to be done. Most often, a social engineer cannot just use social skills to get information. They need to get inside to the company or a person's device, which requires technological skills. The results based on this research point out that social engineering is not enough but very important for security.

1.4 Research objective

The objective of this thesis is to study how to bypass company security controls using social engineering skills. Studying physical security, phishing and one of the social engineering's main phases, information gathering, and personnel security awareness all belong to the research objectives of this study. Security policy perspective is also added to these.

This research is conducted with the help from one Finnish company. For security reasons, the name is not revealed, and it is just referred to as “company”. Survey questions are created for its personnel, and a physical penetration test is carried out to the company. The same physical penetration tests are carried out that were used on the survey questions in order to be able to verify its results. There is a one problem in this physical breach. Many employees know the author but not all; hence, a physical breach could give false information. For that reason, the personnel must be chosen carefully and target the employees who do not know the author very well or at all to get better results.

Reconnaissance is very important for any social engineering which is why information was gathered in passive ways from the target company and also one of the Finnish operators. After this, the information was cross-analyzed to figure out the findings; if there are any differences in them and whether the gained information is helpful for launching possible attacks.

1.5 Research methods and questions

1.5.1 Research questions

Because social engineering affects people and not directly technology, it is hard to measure the potential vulnerabilities caused by employees. How can one check employees’ security awareness of social engineering attacks? It is impossible to verify all individuals’ awareness one by one.

If an employee gives access to the premises to a social engineer, it is like opening a door or if there is plenty of information on public to gather, what harm may the social engineer do and what can the employees do to prevent that? Social engineers might use so many skills to get what they want, which is why it is hard to research all possible situations and ways. There are no limits to social engineering attacks; only ability to think and find new ways to persuade people.

The research problem was solved by carrying out a few different tests that a social engineer could try to do and then analyzing the collected data and survey questions. The tests and data will answer the research questions which are:

1. Is there publicly available information that gives away too much information to launch attacks?
2. Are there any differences between survey answers and real act?
3. Is there any pattern how employees handle possible physical security breach when a social engineer walks among them?
4. Are there trends/common elements between the most clicked simulated phishing emails?

1.5.2 Research methods

How to evaluate personnel security awareness when there are hundreds of employees? The best research strategy is a survey with two categories: questionnaire and interview (Trochim 2006). The questionnaire was chosen as a method. This way all employees could give their own answers to the asked questions. In addition, because the amount of the employees is huge on the company, the survey questions are the only solution to get to know the personnel security awareness.

Survey is a baseline to other tests. It tells how personnel would act on different situations. However, it is only a survey where the personnel can think and make a judgement; they also have time to do this. In real-life, answers and real act would be different, which is why some of the survey questions will be tested on a real act and some cases are created based on those questions. Case study tests different theories, inputs or whatsoever on the real life (Shuttleworth 2008), which is is why this research is also a case study where cases verify or reduce the personnel's answers on the survey.

Collecting and analyzing plenty of data determined the research approach to this thesis. The selected research approach is inductive. In inductive approach, the collected data needs to be analyzed and make conclusions are made based on that (Saunders, Lewis & Thornhill 2009, 126).

Another reason why the inductive approach was chosen was the lack of existing data. Of course, there are many surveys from different companies and plenty of very good books from social engineer consultants and penetration testers; however, this research mainly focuses on only one company and data collected from its personnel. There is no data on other sources. Maybe on the company in case it had collected data; however, in this research, such data is not used even if there was some.

Although the inductive approach was chosen, there are deductive aspects as well. The survey questions were targeted to the whole personnel of the company and not just a few; and physical penetration cases try to verify the survey questions made based on social engineering techniques. Reconnaissance may provide more cases to the physical penetration phase and data from phishing mails may verify some of the survey questions and will answer one of the research questions. Figure 1 links all these previously mentioned methods together.

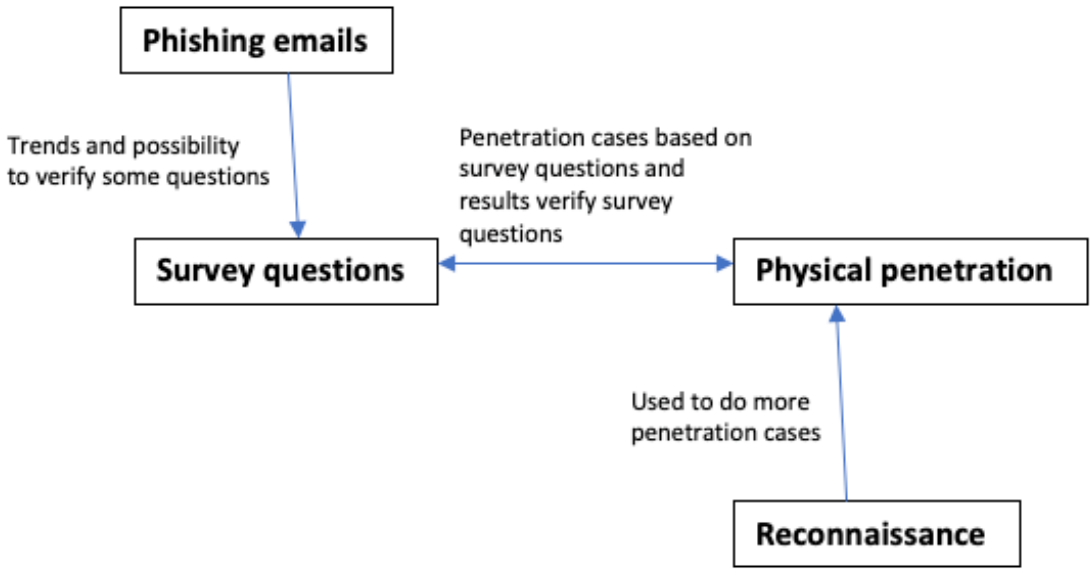

Figure 1. Research methods and how all is linked together

Qualitative data analysis method is used in this research. The qualitative method can contain many different sources such as questions, interviews and numeric format, and it is not limited to only numeric data like on quantitative method (Saunders, Lewis & Thornhill 2009, 151). This research includes a numeric data collection and observations such as physical penetration testing. Information gathering could contain any information.

1.5.3 Research benefits

The main objective is to research the awareness of the personnel concerning social engineering attacks. This research should produce points of advantages and

disadvantages; hence, the assigner company's security team is aware and can take countermeasures against the attacks that need them and raise security awareness. The research can provide information and help to create an education program on security awareness for the personnel or improve the current one. Of course, education and social engineering attacks evolve over time, which means this program needs to be frequently upgraded. Overall, the result will answer the question about the current state of the personnel's awareness.

Although the company has carried out audits and its own red team has conducted physical penetration testing, the results of this research give another point of view on how secure the premises are and how to make them more secure. Publicly available information is the most interesting part of all. This information can be used to launch precise attacks to the personnel. It is crucial to know, what is visible on the Internet for everybody in the whole world.

After all these tests it can be stated how to penetrate the company or at least the assigner company; yet, tests could also give more information how easy it is to penetrate to the premises. Although there are many different researches about social engineering, this research is an attempt to create another point of view on this area. This research includes many social engineering techniques all gathered in the same report.

1.6 Research structure

This thesis includes many of the social engineering skills, and there was an attempt to create a structure easy to follow. Thus, it will also be easier to answer every research question.

Chapter 2 informs the reader about social engineering. Without it, it is hard to do anything relating to it. It informs about its techniques and how to use them. Social engineering follows a framework that includes all steps on the process with building rapport with anyone.

The rest of this report is about the actual research. Chapter 3 discusses the research results and what was done about them as well as analyzing all tests one by one, which is why all research objects are divided into separate sub-chapters. In this

chapter security policy steps are discussed; however, the reader must remember that all that was said about security policies is the writer's opinions.

Chapter 4 then summarizes the results and contains more a precise analysis based on the actual research questions: What was found and what the findings mean. This chapter discusses everything about this research and analyzed data so if the reader would just like to read about analyses and nothing about theory or results, then this is the chapter to read.

Chapters 5 and 6 are conclusions and discussions. The conclusions summarize the data analyzed in chapter 4 and answer the research questions. In the final chapter (Chapter 6), all about this research is explained: how it went and if there were any problems. This chapter also includes any future research objectives or work that the writer did not yet complete and areas in need of further research.

2 What is social engineering?

2.1 Theory of social engineering

When about social engineering is discussed, what is meant by it? Every person might have a different opinion what it means. KnowBe4's website states that it is an art that uses manipulation and influence to deceive the people to gain access to their systems (What is social engineering? n.d.). For their perspective, social engineering is malicious, and its purpose is to get inside of the companies' or persons' systems and do something harmful. According to Karakasiliotis, Furnell and Papadaki (2006), social engineering is an art but also a science which is used at people to make them do what one wants them to do. When the definition is discussed, behind it is a malicious intent but not as much as in the previous definition. Humans' behaviour and nonverbal communication have been studied by many researchers over time and these studies are used by social engineering and with science, a social engineering is an art. The best definition is Hadnagy's (2011, 10):

> "*Social engineering is the act of manipulating a person to take an action that may or may not be in the target's best interest*".

Social engineering is not just malicious. It can also be a good thing for a person or a company. One can think about psychiatrists when they help people and try to figure out a person's real problems. When the person talks about him or her problem, the psychiatrists may use their social engineering skills to change behavior, e.g. asking a question which makes question about or doubts a person's mind and the person starts to think in some other way than before, which is a way to help him/her. Penetration testers can help companies to secure their premises from malicious social engineering attacks. (Social Engineering isn't just for the bad guys n.d.)

Humans are social beings. We are helpful, trustworthy, polite, kind, a team player and so on (Mitnick & Simon 2006, 221; Alexander 2016, 2). Our senses can trigger emotions and those emotions can be used against us, so we do not think clearly or logically (Hadnagy & Ekman 2014, 168). These are the keys for social engineers so we can be influenced and manipulated. Influence means changing a person actions, attitudes or beliefs (Singh, Mani & Pentland 2014, 1903). Manipulate means the same but effect to the target differently. Manipulation has more malicious intent than influence. Manipulator do that for oneself to get what one wants, and it does not matter how to accomplish or how target feels after (Hadnagy & Fincher 2015, 53; Hadnagy & Ekman 2014, 33).

There are six principles why influence is a powerful psychological method. Those are reciprocation, social proof, liking, authority, consistency and scarcity (Cialdini 2016, 153).

When somebody gives or do something for someone else, giver will very likely get something back from the receiver. Gift do not need to be any object or material. It can be a smile, giving help or opening a door and so on. You can think that receiver is on dept and one like to pay that dept someway. This is **reciprocation**. (Cialdini 2016, 153-157; Jones 2003, 4)

Social proof means that people behave, believe or do things that other people do. Social proof can spread like a wildfire among people. Somebody does something; others follow and do the same. The victim is convinced that others have done that so why would he or she not do it as well. (Cialdini 2016, 160-164; Manjak 2006, 8)

When one likes somebody, it is easier to talk with one or just be with one. Similarities and compliments can build up **liking** principle. There is no need to be familiar or known person. One may instantly like somebody if one just sees one and through that one may also trust one. If one really likes the other, the other one might see that and like one also. Humans like naturally other people who are like them. (Cialdini 2016, 158-160; Jones 2003, 4)

One follows the superiors' orders in the army such as a team leader or a captain. This kind of behaviour belongs to the army. Superiors have **authority** over the lower ranks. At work, one has one's own superior who can give orders. One may follow authority even another is not superior or even if the authority may have a lower rank than one has. One can behave like an authority in ways such as talking, dressing and behaving and one does what the other one says. Authority can also be used when saying that a CEO or another high-level superior has asked to do that and that must be done now. (Cialdini 2016, 164-167; Dolan 2004, 5)

When a person has done something or believes something, one very probably does or believes the same way in another situation. One is consistent with one's previous commitments. People like to behave consistently. This is the **consistency** principle. (Cialdini 2016, 168-170)

People want that what they do not have or more of that one has less; this is **Scarcity**. One can take for example an advertisement where a company sells a new revolutionary vitamin; however, it is only available one day. Since it is a very rare vitamin, people buy it based on its rarity. (Cialdini 2016, 167-168)

2.2 Social engineering framework

Social engineering attacks follow a pattern, a framework. There are many different frameworks out there. Figure 2 shows one of them made by Kevin Mitnick.

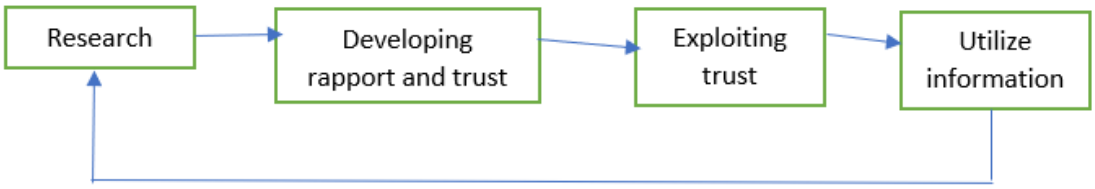

Figure 2. The social engineering cycle (Mitnick & Simon 2002, 331).

The research is all about reconnaissance and gathering information about the target. There is no meaningless information and every information can help when planning an attack (Mitnick & Simon 2002, 15; Hagnagy 2011, 23). Research phase is the most important phase on the cycle to success. Information can be gathered from many sources such as Google, websites, observation and using software such as Maltego and Shodan (Hadnagy & Ekman 2014, 28-29).

After a social engineer has enough knowledge about the target, the next phase is to start to gain trust and developing rapport. Building a rapport is a key to gain trust and the trust is a key getting information easily. According to Mitnick & Simon (2002, 331), developing rapport can use insider information, pretending to be somebody else, citing people known by the victim, need for help or just using authority.

There are ten techniques to developing rapport as follows:

- Artificial time constraints: the other person needs to know and understand that there is end near when talk is initiated. This feeling can be accomplished by saying it does not take long and there are leaving activities such as standing up and heading to the door. (Dreeke 2011, 13-18)
- Accommodating nonverbals behavior: One should look like non-threatening to another person. Smiling is one way to develop rapport. (Dreeke 2011, 19-20)
- Rate of speech: Talking slowly will give another person a positive feeling and one should not sounding nervous. (Dreeke 2011, 23-32)
- Sympathy themes: One should be helpful and when asking any request, do not ask anything that could be threatening or could cost something to

another person. The request should be simple and light, so another person has a good feeling to answering. (Dreeke 2011, 33-40)

- Suspend one's ego: Simple, let others be "right" even they are not. Suspending an ego will help in many situations and it is effective for building rapport. Suspending an ego could be hard and it is not always easy, which is why it needs to be trained. (Dreeke 2011, 41-48)
- Validation: Everybody likes to be accepted and liked. There are three types of validation development: just listening, giving something to another person and validating the other person's thoughts and opinions. (Dreeke 2011, 49-56)
- Ask why, when and how questions: Asking open-ended questions where there are not accepted no and yes answers. Another person needs to think and talk to answer those. Suspending someone's ego and letting another person talk when one keeps listening and asking more questions shows that one cares. (Dreeke 2011, 57-65)
- Quid pro quo: If one does not share something about oneself, there is a big change that another person is not sharing either. One should give a little information so that the other person feels comfortable and can share his/her information. (Dreeke 2011, 66-71)
- Giving a gift: A gift could develop rapport quickly. It does not need to be any object. It can also be something that is said to the other person. (Dreeke 2011, 72-76)
- Manage expectations: Everything does not go as expected, which might give a feeling of disappointment. Managing expectations will help you and reduce the feeling of it. The methods need to be targeted at another person and not oneself. (Dreeke 2011, 77-82)

Using gained trust to get information from the victim or getting the victim to do an action such as opening that malicious attachment is a next phase. This step can also use reverse social engineering technique where the victim asks the attacker for help. The final step is to use that gained information to reach the goal or if that

information was only one part before the main goal, the attack is continued. (Mitnick & Simon 2002, 331)

Kevin Mitnick's social engineering attack cycle has been the foundation to another framework containing detailed information about it and clarifies it. Figure 3 shows this detailed framework. (Mouton, Malan, Leenen & Venter 2014, 3)

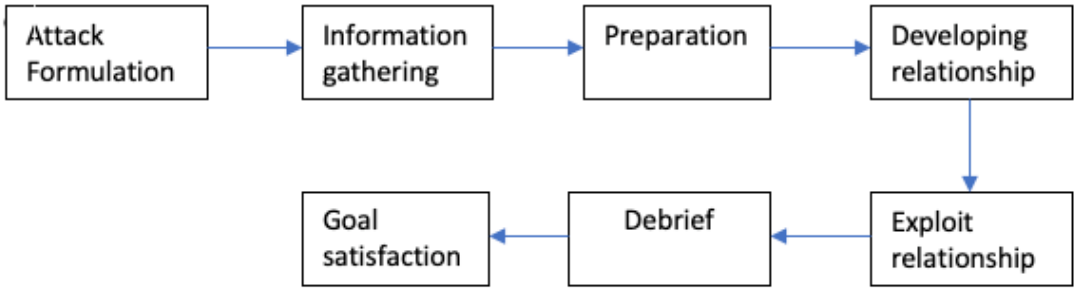

Figure 3. Detailed social engineering framework (Mouton, Malan, Leenen & Venter 2014, 3)

Attack formulation contains steps about the goal and the target. What is the goal and based on that, who is a potential target to reach that goal? When the goal and the target are clear, reconnaissance begins. The preparation phase uses the gathered information to get a bigger picture and developing an attack vector used at the target. After these preparations are done and an attacker is ready, a real attack occurs by building a relationship and rapport using the medium identified on the preparation phase and any social engineering techniques. Exploiting that gained trust using influence and/or manipulation will get the attacker the information that he/she was after. Debriefing after exploiting a relationship is important. In that phase, the attacker tries to return the target's mind to desired state. After that, the target does not feel that an attack happened. The final state is a goal or if the attacker is not satisfied about the gained information and needs more, the cycle starts over again. (Mouton, Malan, Leenen & Venter 2014, 4-6)

2.3 Social engineering techniques

Social engineers use various methods and techniques to get what they need or want. Figure 4 shows these methods and after the figure, the methods are being explained. All methods and techniques are pointless and will not succeed without social engineers' influence and manipulation skills; hence, they must be good.

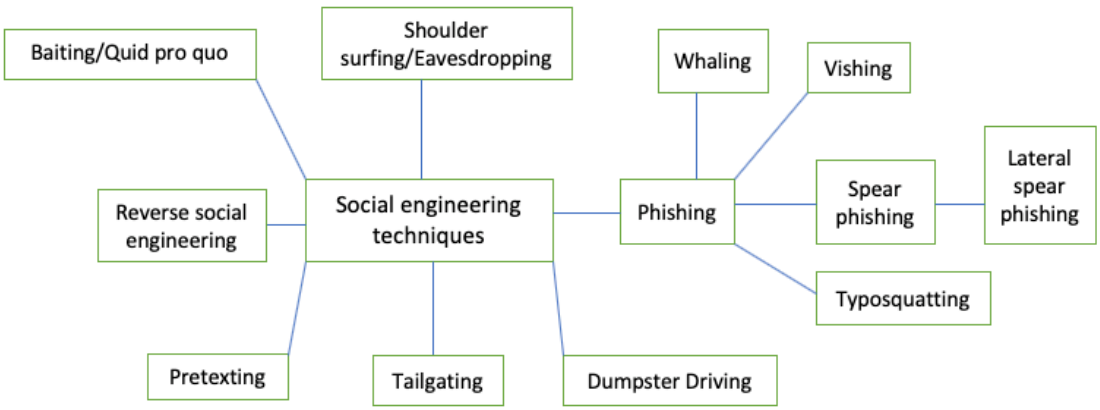

Figure 4. Social engineering techniques made by the author

Phishing is an information gathering technique where commonly emails are used to lure a receiver to give information, open a harmful attachment or click the link which goes to the malicious website. This way the attacker could gain a receiver's credentials or compromise receiver's workstation. (Alazri 2015, 199; Dou, Khalil, Khreishah & Guizani 2017, 2798-2799) According to Khonji, Iraqi & Jones (2013, 2092), there are three motives about phishing: financial, identity hiding and fame and/or notoriety. These are not only for phishing but also for all notorious activities from hackers and adversaries.

Phishing can be divided into multiple different techniques; however, all of these have the same principles; get information or deceive receiver to open malicious link or attachment. **Vishing** is a phishing technique by phone and can be used in various ways to deceive a receiver to trust that the caller is who he/she says or after malicious email to manipulate a receiver to open that harmful attachment (Alazri 2015, 199). **Spear phishing** is a more targeted and precise attack to individuals or

companies and more reconnaissance has been done to accomplish the attack (Bhadane & Mane 2019, 133). **Lateral spear phishing** is almost the same as spear phishing but on that, the adversary has gained foothold on the company and has access to a real compromised email account of the employee which is used to launch spear phishing to other employees under the company (Bhadane & Mane 2019, 133). On **Typosquatting**, the hacker makes a new website and domain almost the same as the original (one or two letters changed) that the victim uses and the hacker tries to lure the victim to use that instead of the original (Peterson 2016). **Whaling** is a phishing type where the targets are in high-level on the company's hierarchy such as CEO or other high-level persons (Hoxhunt n.d.)

Becoming somebody else is **Pretexting.** However, to successfully use pretexting is more than just pretending to be another person. Pretexting needs detailed information about the person who is used on pretext. One needs to act, dress, talk and behave like the other person. Information gathering is important if one likes to succeed in pretexting. Without a good information about a place where pretext is used will result in a failure. (Alazri 2015, 199)

Some other people's trashes are somebody's treasure. People can throw away valuable information such as credit card numbers or personal information without even trying to dispose of them safely. **Dumpster Driving** uses this behavior. Social engineers try to find confidential information from trashcans, e.g. papers, USB sticks or CDs. This is a reason why individuals and companies should dispose of all sensitive information using the safest way that is possible. (Alazri 2015, 199; Kee 2008, 6)

Trying to see and get somebody's credentials, bank numbers and other valuable information over one's shoulder from a close range or afar is called **shoulder surfing** (Alazri 2015, 200; Kee 2008, 7). A person who uses this technique could be anybody from a total stranger in the shop line to the co-worker who needs another person's credential to do something with them. The only mitigation techniques for this are watching behind one's shoulders when shopping, using screen filters on workstations and being aware of one's surroundings. **Eavesdropping** is just listening to what employees or persons talk to get information (Manjak 2006, 10).

Baiting is a technique where a victim is deceived by giving or promise of a reward or something else. This can be divided into two scenarios: something malicious which is named to be something else (e.g. Trojan virus) and use of malicious USB sticks left behind to an open place from which the victim collects and opens them for curiosity. (Norvanto 2018, 197) **Quid pro quo** is similar to baiting but on this non-baiting techniques are used. Instead, the attacker promises some reward or compensation if the target does something for the attacker (What is "Social Engineering"? n.d.).

Reverse social engineering is opposite to the normal social engineering attack. This uses the trust gained from the victim. The victim calls for the attacker to get help. In this attack type, the victim is very helpless because he/she calls and not otherwise. The victim can also use this technique when he/she notices that an attack is happening and uses influencing to get information from the attacker. (Kee 2008, 7; Dolan 2004, 3-4)

Tailgating is used to get inside the company or other places just by waiting and following another person when one gets access to premises. People are helpful and very easily allow another person to walk with them inside or in some cases people do not even check behind their shoulders who are coming after them. (Jones 2003, 9-10)

3 Research results

This chapter includes answers of the questionnaire with the analyses perspective of the security policy. What the answers tell the author and what the security policy could contain to mitigate social engineering attacks. All gathered information from the various sources are discussed as well. Physical penetration attempts were carried out based of the survey's questions and gathered information. What and how did all happen in these physical penetration cases are discussed.

3.1 Survey questions on employees' security awareness

Attackers using social engineering to gain access to the company focus all their efforts on personnel. The personnel need to be aware of social engineering techniques and tools and of course, they need to have the current threat intelligence

about social engineering attacks. This survey tries to measure the awareness of the assigner company's personnel about social engineering attacks. The questions contain many social engineering attack types that could answer the research questions.

The survey was carried out using the company's own Webropol question tool. A total of 70 employees responded to this survey. The author hoped to gain more answers; however, after looking at the answers he noticed that there were many different answers; wrong and right ones which could be analyzed. One must remember that the attacker only needs that one employee or a hole to get inside, and the company's assets and information might be compromised because of the attack.

Next, the survey's questions are listed in bold with diagrams and some information about an analysis of the answers. The questions and answers can also be found in Appendix 1.

1. Do you use a strong password for work related systems, such as your workstation, to log in?

A strong password means a password that contains special characters, capital and lowercase characters, and is at least 8 characters long, preferably longer. It should also be difficult to guess or find out, e.g. aK6ZZk89F5!!. A weak password is not cryptic and is easy to guess or find out e.g. November2018.

61 % of the respondents use a strong password (Figure 5), which is good. However, the rest who use a weak password could possibly be the weak link to bypass all security controls. Security policy needs to contain password policy that this assigner company has.

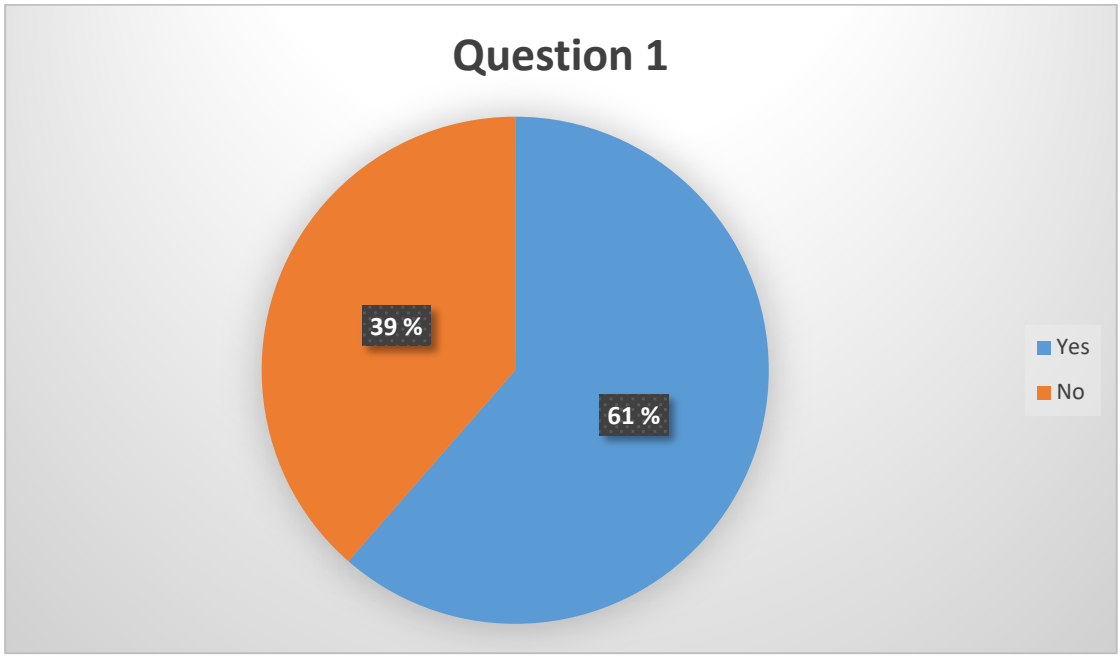

Figure 5. Personnel answers for question 1

Today, passwords which are 8-character long are not very secure even though they are strong and cryptic. The calculation speed of devices is very good, and they do not need much time to calculate an 8-character long password. It is not recommended to any company to use at least 8-character long password. All passwords should be at least 12 or more characters long. That the employees do not like long passwords is the author's own experiences and even when there is a need to change an 8-character long password to a new one, it will take some time. Passwords should contain uppercase and lowercase letters, numbers and special characters and be long.

2. Do you use the same password for a variety of services such as Facebook or Instagram?

Using the same password on multiple services or sites is a security risk for that person. It does not affect the company's assets directly but indirectly it might, assuming that a person uses the same password for multiple sites and a malicious hacker gets this person's password. First, the hacker tries that password for every possible site and checks where it can be used. Using the person's email and password, the attacker has access to email, Facebook and multiple other services. He

gathers more information about co-workers and sends emails to them from the hacked email account. The email includes a malicious file or a link to a malicious website. Now the whole company is compromised.

In the social media such as Facebook, the hacker could post misinformation about the company or post something malicious about the company, which then could affect the company's image. Customers might leave and the company loses money as its business is compromised.

37 % of the respondents use the same password for multiple sites or services (Figure 6), which is a high percentage. Then again, in this digital media time, one could have e.g. so many different accounts and mails that using different a password to all and possibly a different username also might be a problem. The solution might be to use one of the many password software such as KeePass which allows to save all one's passwords to it and then use a very strong password on it to keep all one's passwords safe. One problem, though, is the single point of failure. If one forgets this software's password, recovering all password inside it might be very hard or even impossible. If one uses this kind of software, one should make sure that a different accounts or software is used for the personal passwords and work-related passwords. If one of them is compromised, then another is safe.

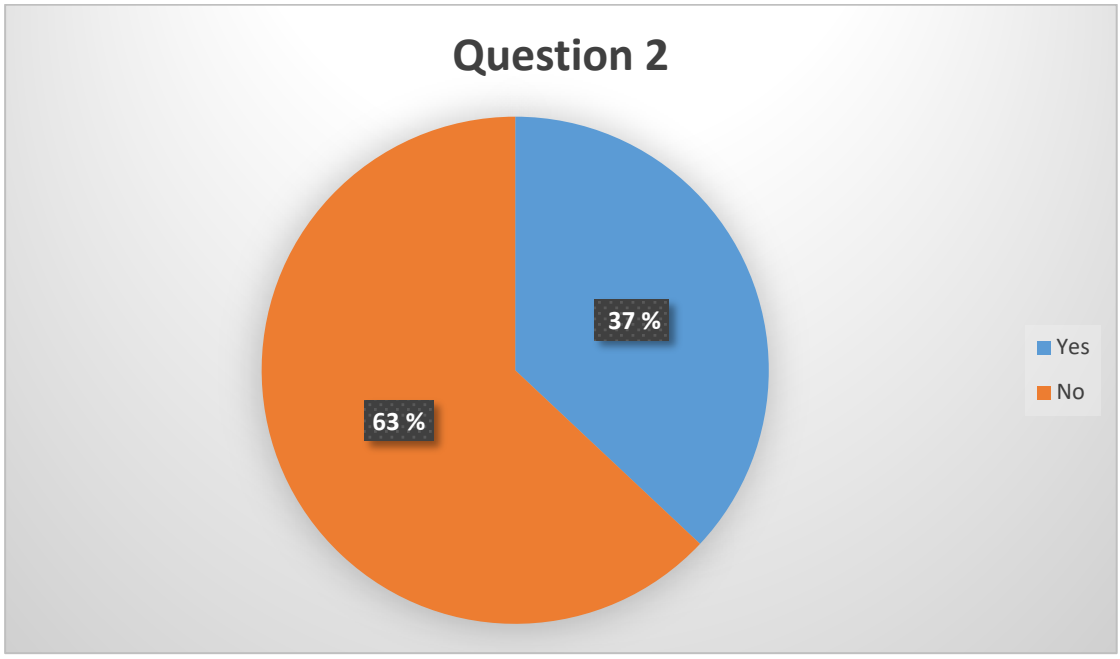

Figure 6. Personnel answers for question 2

Because the employer cannot say or order the personnel to use different passwords to all services or accounts, the personnel should be aware what could happen if somebody gets that password. The employer could for example inform the employees about security awareness training time that could take place, so the personnel know this and maybe change their habits.

3. Do you use the same password to log in work related systems, such as workstation, and some personal services e.g. Facebook?

If one thinks that the using same password on the multiple personal accounts or services is very bad, the worst is to use the same password to work related systems such as workstations. If a malicious hacker gets that password and just tries it anywhere, including work related systems and then gets access, the company is in trouble. Solving that kind of penetration is likely to be very time and resources consuming. Of course, if a hacker thinks and sees that password work with work related systems, one might wonder where else that same password goes. Work and personal accounts are in danger.

It is very good to know that many members of the personnel do not use the same password to personal and work accounts. Only 10 % of the respondents use the same

password (Figure 7). The Percentage 0 would be the best; however, it is understandable that there are people who use the same password. Security policy must contain rules what passwords must be used and more importantly, one should never use the same password on work systems that is used in one's personal life.

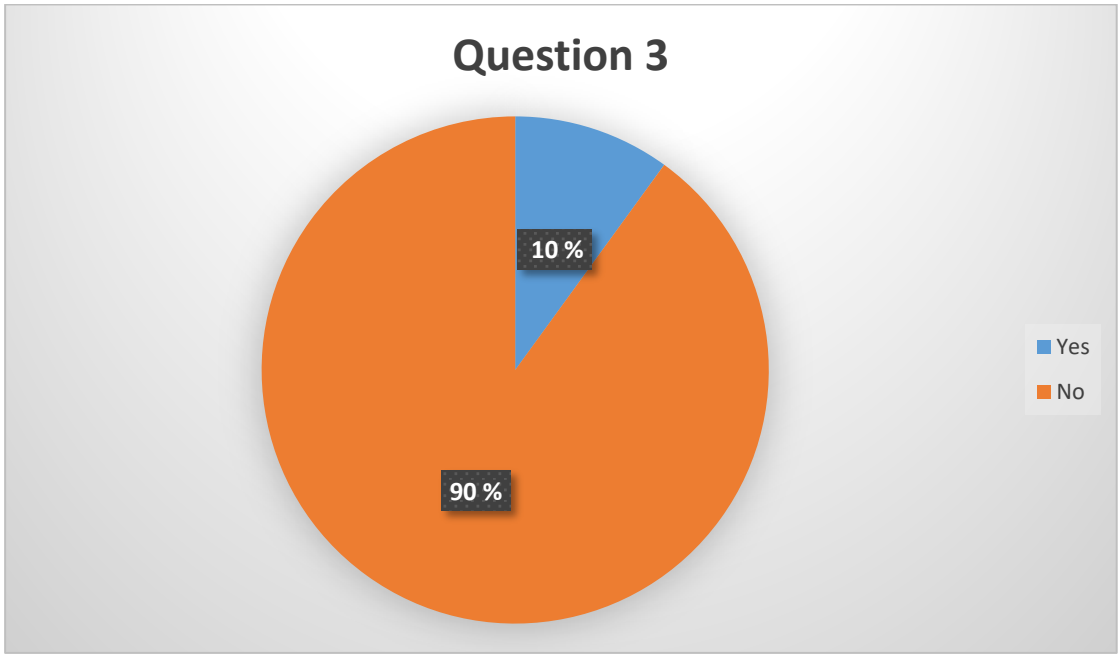

Figure 7. Personnel answers for question 3

4. You are working on your workstation and the fire alarm goes off. What do you do in that situation?

There are no excuses when a fire alarm goes off. Everyone should leave. It does not matter if it is a test run or a real situation. Some of the personnel members ignore this. About 1 % of the respondents just continue what they were doing when the alarm went off. The rest of the personnel leaves; however, about 3 % of the respondents just leave and do not bother to lock their workstations. 96 % of the respondents lock their workstations and then leave. (Figure 8)

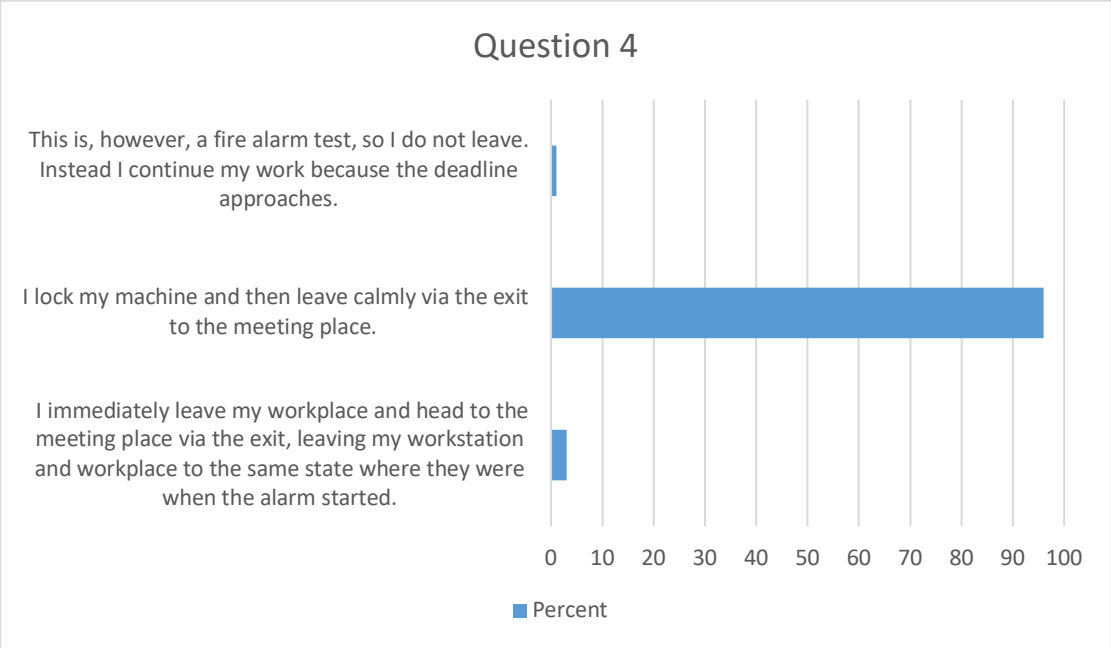

Figure 8. Personnel answers for question 4

Finnish law includes a subsection about a rescue plan. It must be implemented if there is a danger to people when something e.g. a fire occurs. This rescue plan is a part of the security policy. Therefore, it could be said that the 1 % of the respondents who ignore a fire alarm also ignore the Finnish law and their company's security.

Good practise is to lock the computer before leaving. No matter if one needs to leave because of the alarm or just to go to the printer. Malicious user or outsiders who are already inside do not need much time to do something to an open workstation. An outsider could be responsible for the alarm and hence, when everybody leaves, he /she just goes to an open workstation and starts to infect the workstation. He/she can create remote access from the outside to it and do much more harm. Then he/she leaves with access to that computer.

The employer should make clear to all that when leaving the workstation, one should lock it. This kind of action could also be a part of the security training. Then the personnel might learn and lock their computer. 96 % could be 100 %, which is not even hard to accomplish.

5. Do you have or does your computer have any valuable information that might interest a hacker?

Any piece of information is valuable to a social engineer. The source could be e.g. listening, file or Internet. It can help him to plan the next phase of attack. 68 % of the respondents think that they and their computers have valuable information (Figure 9). It must be now remembered that most of the data or information is somewhere else than on the computer. The data is most often in servers or in the cloud where they are backed up. If a computer is compromised, then all data on the other server or in the cloud might also be in danger when a user has access. It can be said that everybody has information that is important, and workstations as well have information or data.

9 % of the respondents believe that they do not have valuable information and neither do their workstations (Figure 9). The author does not know any job in this assigner company where there is no valuable information or where that information is not handled. Service desk has information about their customers, which is very valuable; Human Resources (HR) control all company's employee information; a system specialist or ICT knows all about technology and most often, a receptionist has some way access to an access management. The receptionist can modify the personnel's access to the company's premises. They know much about the company.

13 % of the respondents say that they have information; however, it is not in their device (Figure 9). Persons must have a very good memory if they remember all information and that information is only in their own heads. That is a minor problem if that information is not anywhere else. If that valuable information that the company needs is memorized by one person or persons, and they leave or something happens to them, the information is lost. Workstations must have valuable information or this information could be somewhere else in a safe place or it should be. Security policy should include that all work data must be somewhere where it is backed up, and very valuable information must be somewhere written down.

10 % of the respondents say their computer has information only (Figure 9). The 10 % whose computers have information only must be wrong. If they have created that information or data file, they know about it. One possibility is that they have access to valuable information; however, they have not read everything, so they do not know it. In that case, asking or manipulating a person to reveal sensitive information

is useless unless they tell where that information is located and then try to access it there.

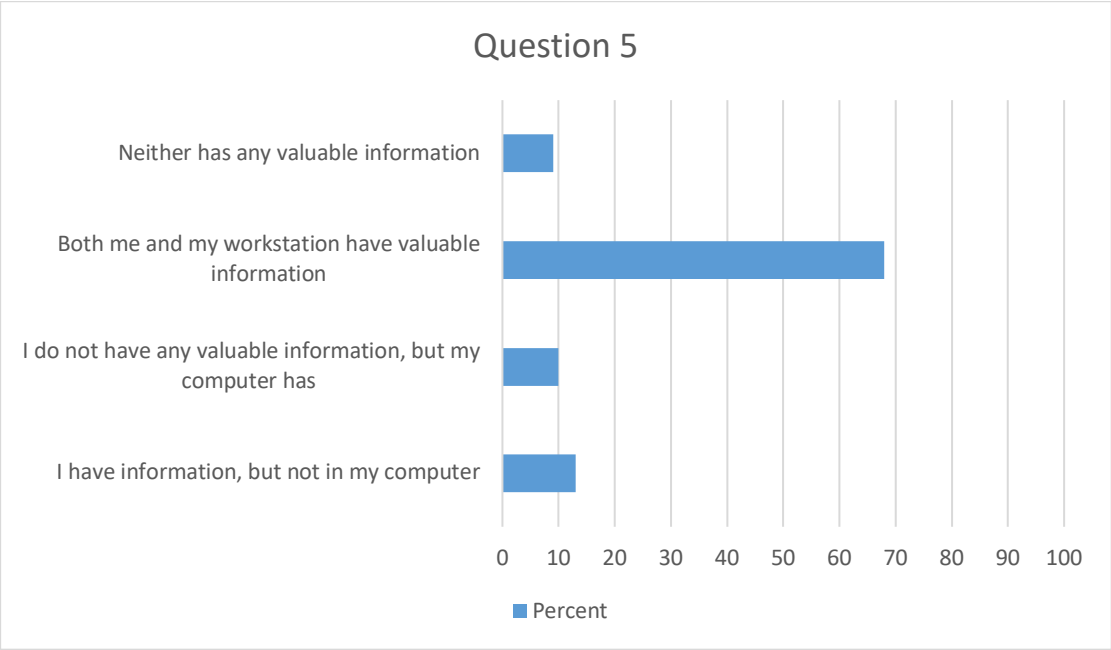

Figure 9. Personnel answers for question 5

6. Your manager calls you from an unknown number. He is ill at home and his voice is about to go away and you do not know exactly what he says. He immediately needs the team's three most recent meeting reports and those should be packaged in one file, encrypted and sent to his private email (firstname.lastname@hotmail.com). The number your supervisor is calling from belongs to a member of the family. He has forgotten the computer and the phone on the previous day at work, cannot pick it up and these reports must go through asap. You can send the password for the compressed file as a text message to that number. What do you do?

Who would not do what the supervisor tells? He/she has authority over what an employee does, and social engineers and other hackers know that. That is a skill that they use because it is hard to resist or sometimes impossible without consequences, e.g. in the military.

When a supervisor calls the personnel like in this question and asks an employee to take this kind of action, the employee must think carefully and doubt this. No work files or anything related to work should ever be sent to private emails no matter who is requesting that, a supervisor or even the chief Executive Officer (CEO). They are always sent to work email. Good security policy should include this rule.

77 % of the respondents start to identify the caller (Figure 10). Nobody can be sure if the caller is real or fake. It is so easy to buy a prepaid phone and use that. Little gathered information may help to launch this kind of attack at a right time if the information is available somewhere on the Internet e.g. social media. This may be another security policy rule: never create anything in social media that could inform a possible attacker to launch an attack. That is never or often very hard to control. Security awareness training should inform about this to the personnel. If somebody gets a phone call like this one and notices it must be fake; an attacker tries to get access to information, the employee can use social engineering skills to the attacker to get information from him, which is called reverse social engineering. This requires much more skills from an employee and its success rate is low if the attacker is a very skilled with social engineering techniques.

Only 2 % of the respondents do what is asked (Figure 10). This figure is very low and that is good. Every time one should think before action. 21 % of the respondents just finish the call, which is a very good action if this attack type is noticed. However, if the caller was one's supervisor and the next time, he or she yells from at the staff member, one can just state that security policy denies that kind of action.

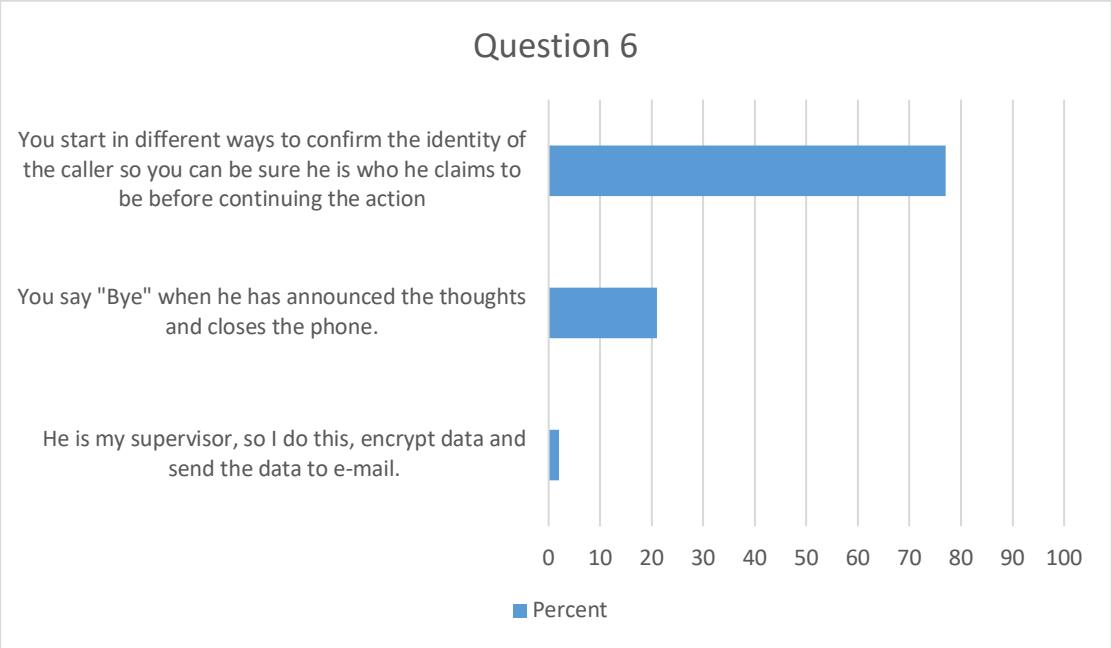

Figure 10. Personnel answers for question 6

7. You have plenty of data on the computer that you should save. Network does not work, so you cannot save the data on the network. You need some external media to store your data. You do not have enough large enough media for information. However, you notice a USB stick on the unused table next to you and you will notice that it so big that all the data will fit to it and there will be still space left. What do you do?

USB sticks may contain anything. They may have real files or information but also malicious files or the whole USB stick is malicious. Opening a harmful file or just plugging stick to a workstation means that an attacker may have and probably has access to that computer.

3 % of the respondents use that stick and make a possible breach (Figure 11). 70 % of the respondents do not use it because they do not know what it is and its origin. Nobody gives it to another colleague for testing. Giving a malicious stick to another is same as using it on your own computer. A skilled hacker could just infect that person's computer when one is inside and gathering information and see where one has access. Then one just makes lateral movement and tries to get more foothold inside infecting other devices.

Somebody just takes that stick to security personnel where they can test it. 27 % of the respondents would do that (Figure 11). That is one solution but that will burden security personnel and when a company has hundreds of sticks, the company needs a new employee or more, and a job for that purpose only, which is not very handy.

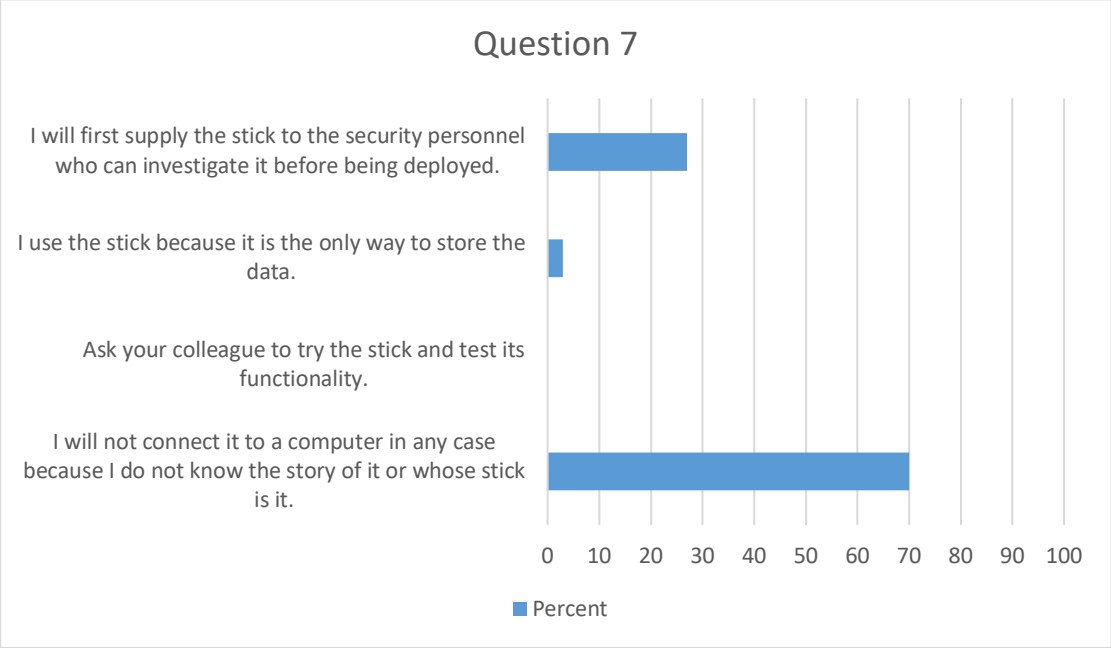

Figure 11. Personnel answers for question 7

When one sees a random stick somewhere, one should not plug it in at any case. It is better just to dispose of it safely and just go to pick up a new stick. If there are not any, then one should go and buy a new one. They are very cheap today. One should not ask a security specialist to test sticks because they do not. They have more important things to do than just investigate random USB sticks.

8. You are coming to work, and you will discover an unknown man in a suit with a computer briefcase in hand coming after you to inside smiling and thanking you. What do you do?

One should not let anybody enter company's premises in any circumstances if one is not certain about that person. If one does not see a personnel's ID card, one should ask. If one is a new employee, one cannot know everybody. Then one should verify all when going inside and somebody coming after you might be a vice president or

CEO oneself. Following these simple rules will make the company much more secure. The company's security policy should contain these. 83 % of the respondents will do that (Figure 12).

14 % of the respondents just let everybody inside without asking (Figure 12). This is somewhat high. It is so simple to just ask person a single question: "Do you have a personnel ID card?". That is hard to us and most of the people do not ask. Maybe it is too frightening or people think asking somebody for their ID card could do something harmful.

Letting somebody unfamiliar inside and then informing all personnel about that is the same if one lets somebody real hacker in. A few minutes could lead serious trouble. A professional black hat hacker does not need much time to install a backdoor or something else to some computer and then he/she has access. 3 % of the respondents inform the security personnel and all others about this breach; however, when somebody reacts or even finds this person, could take time and, in that time, the black hat is gone (Figure 12).

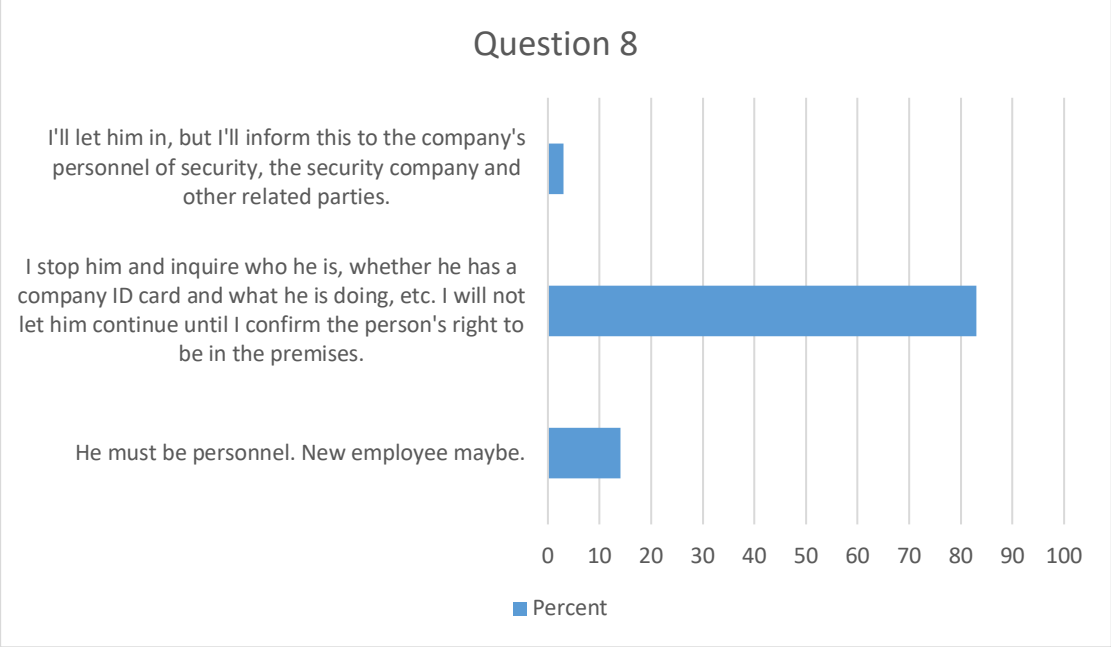

Figure 12. Personnel answers for question 8

Security policy and security awareness training should teach the personnel to ask and watch when coming inside who is coming after them. The personnel should also know that there is nothing bad or nothing bad will happen when they ask for a card or someone's right to enter premises.

9. You get a call. The caller is from a research institute where a research has been purchased by the company related to the personnel; identify strengths and areas of development and utilize information when designing development activities. The study is carried out on the telephone. A prize is awarded to the recipients. Do you answer the following questions about the research?

This question is interesting. What information would the personnel give to 3rd party? Mostly they do not give any information. Job is about 50/50 (Figure 13). That is not so secret, and that information is probably available on the Internet or social media sites such as LinkedIn or Facebook.

All these questions could give nice information but if one watches those questions, one can see two very dangerous questions between almost normal survey questions: personnel ID number and how one walks in the company's premises. Why are these dangerous? A social engineer gets inside information about premises that there are, what one needs and how to walk there. Without that information if one likes to enter the premises, one must do that blindly. Now one has information and that makes the physical breach easier.

ID number is a unique to all employees. It separates all employees from each other. If there are many persons with the same name, the ID number tells who is who. Depending on the company where this number is used; however, some services might need that information. If a company use 3rd party for their ICT problems such as service desk or similar, how do they identify the personnel when they call them. The service desk cannot just do everything without identifying a person on phone. There is no simple software or some other way which could help. One solution is to use the personnel ID number which is only known by the person and HR; maybe others as well but not by everyone. An outsider should never know this number. It is powerful number.

This kind of approach is a common way to get information from people by some small talk and jokes so that a person has a good feeling and is not on the alerted or by asking simple questions and between them asking that devastating question which is the purpose of the talk.

97 % of the respondents do not answer that ID number question and 99 % do not answer that premises question (Figure 13). From this survey's perspective, these are good results. In a real life thought one could say that the results could be much worse when a very social and skilled social engineer lures and manipulates persons.

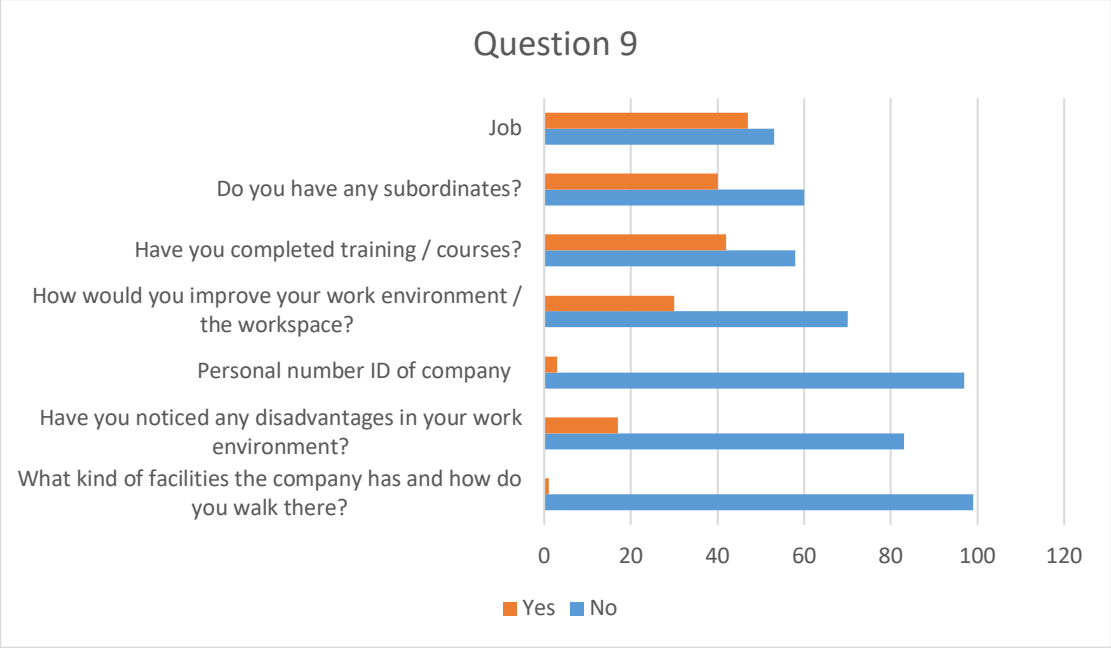

Figure 13. Personnel answers for question 9

How can one avoid this? There is a simple rule: not answer anybody unfamiliar anything about one's work or the company. All surveys must go through the company's own tools, so all information stays inside the company and not in the 3rd party. The personnel must stay alert though all the time when speaking with somebody they do not know and even that may not help every time. One rule might be that only communication team can answer questions which involve personnel and the company.

10. Your friend comes to you. He has problems with the network, and he should be able to retrieve some documents for a review. He has the rights to such documents. He has a USB stick that can be used to store the documents so he can access them. The stick is found on the top of the cabinet. How do you handle it?

This question is similar than question 7 but the perspective is different. If somebody gives an unfamiliar USB stick and asks to plug it in, what does one do. It is nice to know that everybody helps a colleague in some way and not just ignores them. It is nicer is to know that 93 % of the respondents do not plug that stick to the workstation (Figure 14).

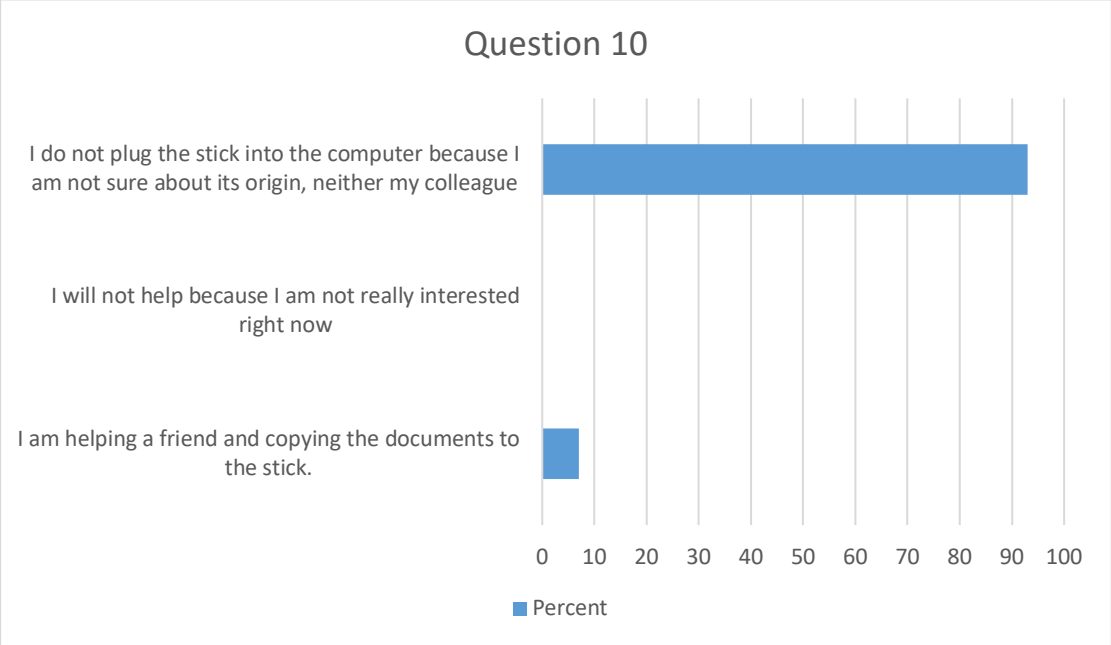

Figure 14. Personnel answers for question 10

11. You are coming to work in the morning. You will find that an unknown person is trying to get inside using his own card; however, the card will not work, and the doors will not open. What do you do?

This kind of penetration is very simple to do unless the personnel do not check key card carefully. An unknown person must raise some warnings to the personnel's mind. An attacker gathers information and tries to find a picture from the Internet

where there is a visible key card and makes a fake one and uses that. Or another possibility is trying to get a picture of it from the personnel. This is little more complicated and riskier because an attacker needs a direct contact to the personnel or needs to be close and there is a risk to be exposed.

When thinking about any company, there are or should be more locked doors than just doors where everyone can come into the building. Inside of the building there must be locked doors where the personnel need to use the key card if they want an access. If the key card does not work and the person cannot get inside although an employee, how can one can move or get any other floors or rooms where a card is needed. The card's permissions need to be checked in that case. 89 % of the respondents check the key properly and make sure it is not fake and they advise person to check a card and its rights (Figure 15).

1 % of the respondents checks a card properly and when all is good and the unknown person is verified to be employee, they let the person to enter (Figure 15). Although a person belongs to the personnel, what a person could do if one cannot access nowhere inside. Card verification is very important; however, card permissions are also important. If a card is not working properly, permissions need to be checked.

Without a good card and person verification, there is a risk that an unauthorized person may enter the building. This is a huge security risk. 10 % of the respondents do not check a card thoroughly (Figure 15).

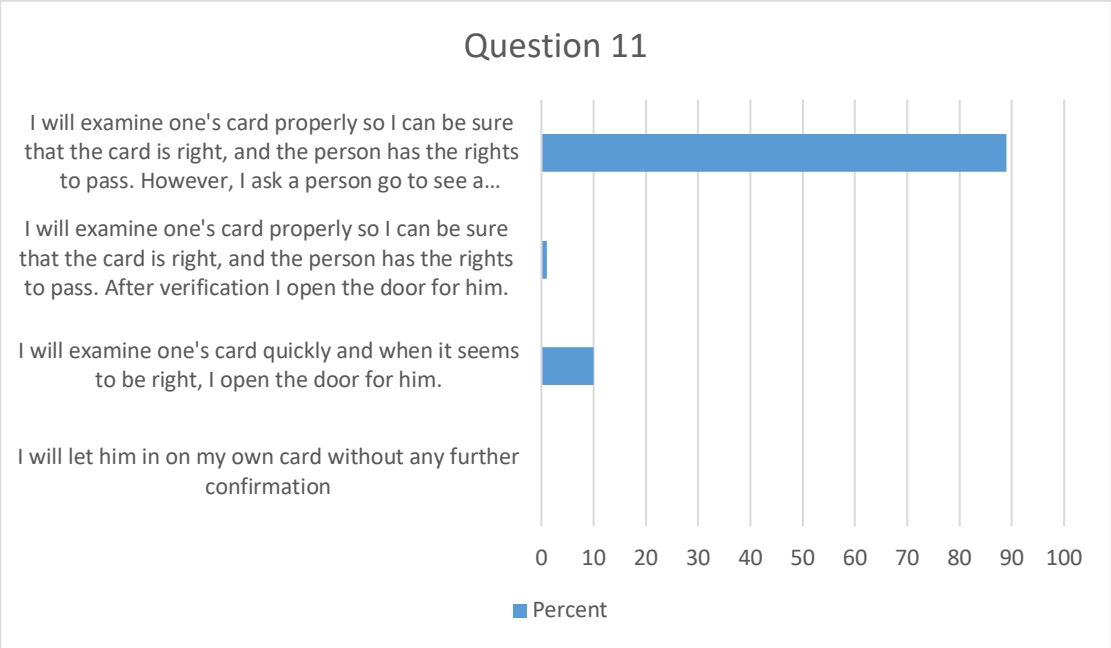

Figure 15. Personnel answers for question 11

How to prevent or mitigate an attacker from using a fake card so that the personnel do not let one inside? It should be made sure that fabricating a fake card is very hard or impossible. Information on the Internet should be minimal but that is very hard to achieve. All images may reveal something that helps to make a fake card. Taking pictures from personnel's cards is hard if the card is not visible. Personnel should not wear a card when going outside or at least they should hide it so that there is no way to take pictures of it.

The best solution is the personnel itself. Using a fake card is futile if the personnel check cards inside out. Companies should include this kind of behaviour to the security training and security personnel should remind of that from time to time. Then the risk is very low that an unauthorized person enters using a fake card.

12. You get a call. The service desk is calling. Virus software has detected a malicious program on your computer, which may be a ransomware, which, when activated, would encrypt all the data on the computer and therefore no access to them anymore. Malware can be removed but it must be done manually by remote access. There is a problem with the Service Desk workstation and there is no normal remote connection, so you should install

another remote access software from the Internet, and this does not require any rights. He asks to download this to get remote control with the machine and remove this malicious program. What do you do?

Fear, hurry and company's own service desk could be very potential social engineering attacks types and together they may also be a serious risk. Employees may not know if that service desk person on the phone really is the one who one claims to be. And a possible fear of losing all data will also help this kind of attacks to succeed. Of course, service desk asking to download something from the Internet and installing should make some warning signs to an employee; however, some will do what the caller is asking them to do.

94 % of the respondents will not do what a caller asks and do not download that file and install it (Figure 16). Instead, they go to their local support who they really know and let them handle this malware. This kind of action is the only way to be safe. 2 % of the respondents ignore the caller and hang up the phone and 4 % of the respondents do what has been asked.

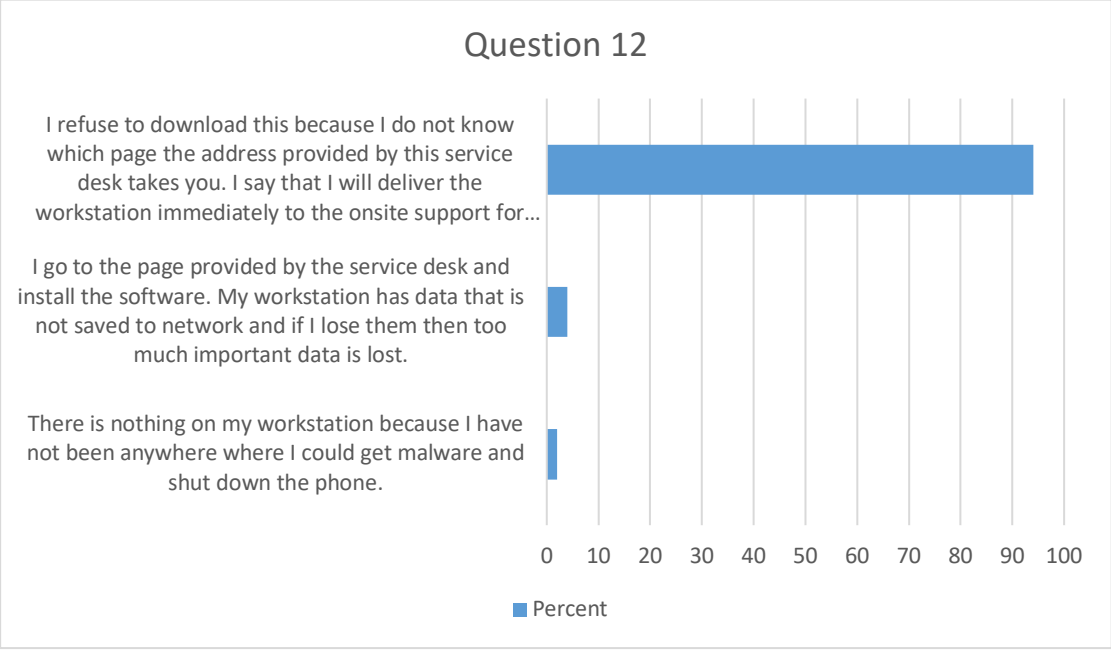

Figure 16. Personnel answers for question 12

Downloading and installing unfamiliar software is not safe at all. An attacker might get inside if doing this. Ignoring a caller will make a possible attack hard but again if that caller is a real person who one claims to be and there is a real ransomware on the employee's workstation, the situation is bad. Losing all data or installing potential malware is both very harmful. Data might be recoverable but sometimes they are not. Installing a malware, any malware, and letting an attacker to get inside to the workstation will be a serious risk unless somebody fast removes that malware and an attacker was not fast enough to install backdoors or something else to the workstation. Anyway, the company must have strict rules on what must be done when any malware is found or there is even a possibility of malware.

Companies should think and choose their remote access tools which are only legitimate software and all other tools are prohibited. All personnel should be aware of that software so there is no way that this kind of attack could ever happen. In addition, of course, this software must be installed to all workstations, so that the personnel do not need to install anything.

There could be a rule on the security policy where it is mentioned that remote access tools and no other tools are allowed. If malware is found or there is a possibility of any malware, the workstation must be scanned and researched thoroughly via legit remote tool or locally. There might be a rule that when someone finds a malware, a workstation must be installed again. The main rules are to only use legitimate software, all possible virus and malwares incidents must be checked and no website should be download, installed or visited which somebody on the phone asks if a person on the phone is not verified totally.

13. You receive an email from your co-worker. The headline is "Look at this! Make your day much better!" The email has a Youtube link and additional text that says, "the best laugh this day". What do you do?

Trusting to co-worker is important in any job. But when an employee gets that kind of an email, the employee should look at that message thoroughly and verify its origin and is that really from the co-worker. 51 % of the respondents verify an email and 3 % of the respondents trust a co-worker and open it (Figure 17). 26 % of the respondents ignore that email. If that email was really from a co-worker and funny

and one wanted to show it, a co-worker very often asks if you watched it and then you know it is real. 20 % of the respondents report it as a phishing email.

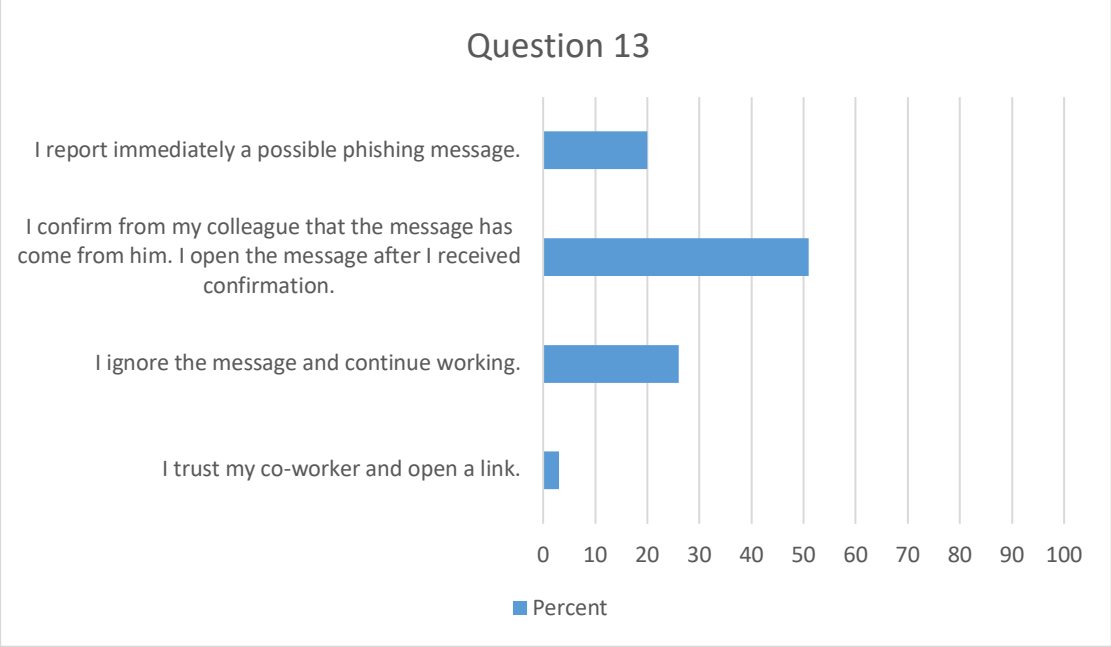

Figure 17. Personnel answers for question 13

Making a fake email is simple. An attacker might have information which may help one to do a very good and real phishing email and target that email at one target who might open it. The personnel are aware of phishing emails; however, some are so good that even a security specialist could be fooled to open those and that has happened. Because phishing emails are easy to do and the risks to get caught are minimal, they are very often used to compromise companies.

The personnel should be trained to look at all emails with open eyes. The company might carry out phishing email campaigns on their own and teach the personnel that way or use 3rd party which does phishing emails for business. The personnel should follow the rules on how to handle all suspicious emails. All should be verified and if an email is not from a person who was the ender on the email, it should always be reported as a phishing email, so the company's security personnel are aware and can take some countermeasures e.g. inform the whole company about phishing email. One should never ignore a potential phishing email because an attacker just targets

that email at another person who may open it. Security training program might teach all personnel about this kind of behaviour.

14. You are going to a cafe in the canteen and you notice a person walking toward you and you cannot see an ID card. What do you do?

The personnel should wear an ID card all the time. It is also important that an ID card is visible and not under shirt or jacket or somewhere else. The personnel should also ask for an ID card if that is not visible. According to Figure 18, 49 % of the respondents ask that very important question: where is your ID card and 47 % do not ask and continue doing what they were doing. 4 % of the respondents stay and talk to a person.

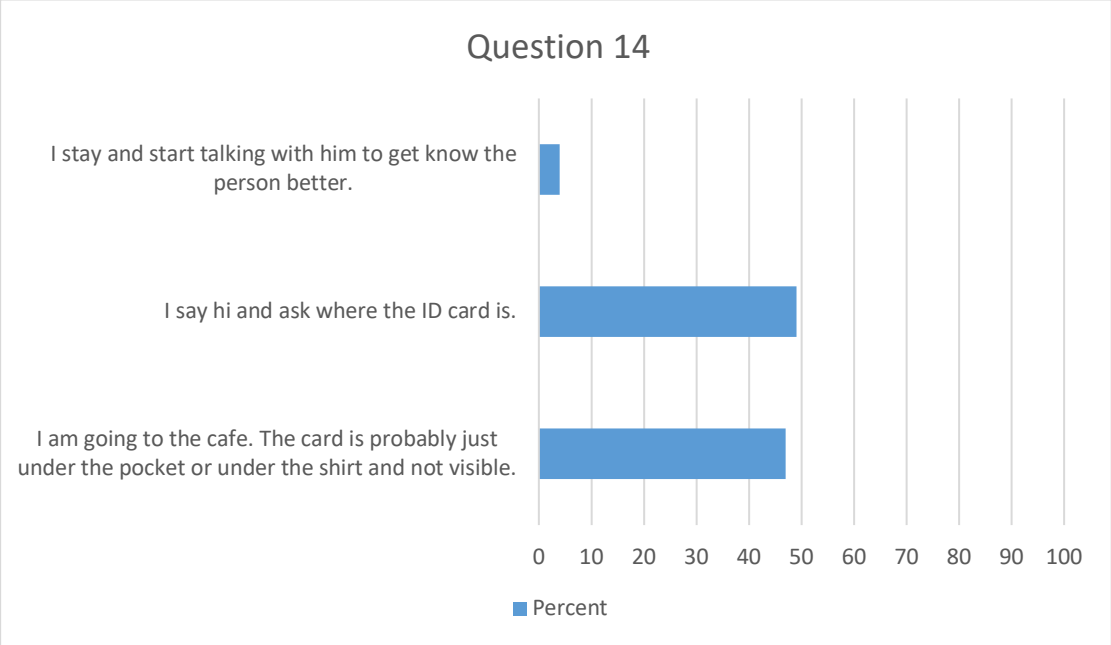

Figure 18. Personnel answers for question 14

Because almost half of the personnel do not ask anything about an ID card, the company may have some security risks if an attacker comes and gets inside. All should have security behaviour that includes asking about missing or not visible ID card; they should also wearing the ID card. Although security policy includes that not wearing an ID card is against the policy, some personnel may wear that place what is not logical, or they do not ask about it. Company should teach personnel that asking

is everyone's responsibility and that way attackers are easier to identify and stop. In addition, if everyone wears an ID card logical place like hanging on the neck, everybody eventually notices if someone does not have an ID card and starts to ask about it.

3.2 Information gained from publicly available medias

In this chapter information is gathered from the assigner company, and only passive gathering is used, e.g. Google, a website and Maltego. Information is also gathered from the operator and is cross-analyzed. The author needs to know what differences are available. Because no names are revealed from now on, the assigner company is referred to as company and the operator as operator.

3.2.1 Website

The easiest way to start gathering information is a company's website. Most often, it reveals a great deal of interesting information. After checking that, one can expand the research to other areas. Table 1 shows what information was gathered from these two, the company and the operator, from their website.

Table 1. Information from website

Company	**Operator**
Personnel names and job titles.	Some names of personnel, their job titles, images and phone numbers.
Organization structure and images.	Organization structure and images.
The main business plan and another job inside of the company; what they do for business.	Core business and expanded business from subsidiaries and their names.
Charity area and couple of charity customers.	Some startup companies that the operator has helped.

One team's structure and one member on it.	
Company address	Company address.
Emails addresses (e.g. helpdesk) and phone numbers.	Helpdesk and other numbers. Also, many different email addresses.
Social media links	Social media sites
Structure of email address	Structure of email address
Annual and other reports.	Many annual reports that may give more information.

There is a great deal of information available on the website; however, not much of it is relevant, which could help further. The table above summaries both corporations' gathered information that was found the most interesting. The same information is on the same row to help to see the differences better. They are almost identical. What does that information say?

One can think about that information with business in mind. Both are limited liability companies: hence, they must follow many laws such as the one stating that the revenue must be visible. Both companies have that on their website. Of course, that gives information about the company's size and how healthy is it; however, it does not reveal any other valuable information. The annual reports inform how the previous year went and possibly discusses new strategies and gives other information for next year. Information like that might give a possible social engineer valuable information which could be used with other information to launch attacks. One must remember that any information is relevant. One piece of meaningless information given by the company or any staff member may be a valuable piece of information for a social engineer.

There is no business without a business plan. It is difficult to create a company without any vison of its operations. This information helps social engineer much; however, that information should be on a website. It does not matter. One can also get that information from other sites on the Internet. It is better from business perspective that the website includes that information for the customers. However,

inside knowledge is bad; e.g. possible job titles or teams' structures. A social engineer can draw almost a whole company's structure, how all parts are linked together from the CEO and board of directors to low-level employees. Yet, there is still need for more information from other sites or media. In this digital age and with social media, one can draw almost the whole company's structure; hence, it is the same if there is this kind of information publicly available. If there is none, the social engineer must work more to link all personnel together from the other sites, e.g. social media.

Because of all social media, it does not matter if a website contains personnel photos unless they reveal some valuable information such as an ID card or something else. These two corporations' websites revealed nothing. Social media provides the employees' photos if needed.

If a company likes to keep business running smoothly, it must have contact information somewhere where customers can find it. Without it, the customers must find the information in some other place, which might be hard and probably give customers a feeling that the company does not bother to keep customers satisfied or they do not like to give out their contacts. This kind of information gives contact points where to call or send emails when starting to launch attacks or just for getting more information. Company address is a piece of information where a social engineer might start to observe e.g. employees, entrances, or possible video surveillance. Observation is a very effective way to get information. These is information that must be somewhere to find.

Email syntax is something that should not be kept visible; however, the syntax is a standard in Finland used by many. Firstname.lastname is a start for almost every email, so one does not need to be an expert to figure out if that is the right or wrong syntax. There is no point to give that information in public unless the syntax is different. Then a company needs to think about that again and evaluate it bearing the information risk management in mind. If a social engineer does not know the syntax and it is not a standard, one must make a huge effort trying to figure it out. Still, it is possible to get it but it requires more work.

Charity gives a company a better name and better image. Who would not like corporations who gives money to charity or startups? It is a good idea to make it visible. In this case, the company's website gave out some charity customers and their names, and the operator's website revealed the startups. How could that information help the social engineer? They could pretend to be one of the charity customers and lure the personnel then to do something malicious. It is not as simple as it sounds. A social engineer must get more information, how the whole charity works and how and who to contact for gathering more information.

Social media such as Facebook, LinkedIn and Twitter are today almost "must have" services for any corporations no matter what size they are. They are very good for marketing purposes. One does not need to use only paper or television for marketing. Social media also reveal so much information. The author studied the assigner company's LinkedIn site and some personnel profiles and he found hundreds of the company's employees and their job titles and job descriptions. If an attack were launched at the company, this information would be very valuable. Are all social media links on the company's website relevant or irrelevant? One can say that it is better from customers' perspective that a website contains the links to their social media websites. It is more crucial for the company what personnel write for their own social media or the company's profiles. Security policy must contain something about this, e.g. personnel are prohibited to write any information connected to the company on their own sites or anywhere where it is publicly available. The personnel must also think about what they write even on the company's own social media sites.

3.2.2 Google

Google and its image search and Google's advanced features are very good for reconnaissance. Much information can be obtained by just only using Google. The images may show very valuable information and an advanced search may find possible documents, Excel files or even some configuration files on the websites.

Table 2 shows what information was revealed by just using Google. It was categorized based on what was searched and what was discovered.

Table 2. Information from Google

	Company	Operator
Images	- Google images where there was a text about a new tablet and its model - Personnel ID card almost readable	- Images with personnel ID card visible
Normal search	- Information about a new service provider - Operator who operates all company's network of places of sales.	- Customer name and what services are included - Partners who help to develop a new mobile network
Domain Name System (DNS)	- Internet Protocol (IP) address space range - Public DNS names and IP addresses. - Public mail servers and IP addresses. - Persons' names - Many subdomains	- The same information
Advanced Google search (files etc.)	- Many PDF files but nothing useful information found	- Many PDF files and other files but nothing crucial information.

Searching images related to the company revealed personnel ID card. When watching closely for those images, one can see what an ID card contains and that information can be used to make own fake ID card. No company, no matter what the purpose is, can control all images that are uploaded to the Internet. Companies can only try to mitigate possible threats from images and give instructions to the personnel that images they upload to the Internet should not show all possible that can be used against to the companies. Like on this case, valuable information for malicious social engineer is this ID card that allows one to try to get access to the premises using a fake ID card.

Searching images revealed also a tablet used in the company and its model. This kind of information gives more solutions to launch attacks. A malicious social engineer could pretend to be from a manufacturer and make a call or send phishing email to the employee in the image.

The assigner company changes its service provider according to the news on the Internet. However, no time scale was found when this new provider starts so it is hard to launch attacks pretending to be for example a person from the service desk. If there was available, a malicious attacker could launch an attack when a new provider has just started. In that case, the personnel do not have any clue if that person is real or fake. In addition, if the social engineer is good, it is very probably a breach if the personnel is not aware what one says and do not know the new service provider's policies of the help desk.

DNS information gives public IP addresses and the names and addresses of public servers. These need to be public if the company likes to keep business and all its services running for public use. However, the information contained also names of persons who have something to do with the domain. They are very probably personnel who work on ICT services and control domain services. Moreover, if that is the case, it would mean they could have more privileges than a normal user or even domain admin rights. If a malicious social engineer targets them and gets somebody of them to do something they should not do, then a whole company's infrastructure might be compromised. Getting one foothold with domain admin account or admin account with more than normal privileges to the workstation or the worst scenario to the server can escalate to more compromised accounts and devices.

3.2.3 Maltego + Shodan

Maltego is an open source information gathering, Open Source Intelligent (OSINT), tool that allow multiple add-ons to be installed. Shodan add-on was installed to Maltego in this reconnaissance phase.

Table 3 shows the result from Maltego and Shodan. The left column informs what syntax or palette/tool was used on Maltego to get information and on the right are its results.

Table 3. Information gained from Maltego and Shodan

Domain **(Search syntax: company.fi)**	- DNS names - Subdomains (syntax: text.company.fi) - Email addresses - Personnel names - IP addresses - MX and NS records - Phone numbers - Web sites and other subdomains
DNS names	- IP address of DNS servers - Information, how all different DNS servers link to each other. - Services that belong to that DNS server such as web sites. - Subdomains found (syntax: text.company.fi) - More DNS names found
Subdomains	- Subdomains linked together - NS records - Email addresses - Phone numbers - More DNS names
MX and NS records	- Domain names - DNS records - IP address blocks
Websites	- Websites' titles - Technology and relationship
Public IP addresses	- Domain names - Services/port numbers - Email addresses - IP address ranges - Personnel names - Phone numbers - Other company's information before merging together - IP address blocks (not company's own) - Hash values

Information gathering phase in Maltego started using domain name. The results were almost the same as in a manual gathering phase but there were differences such as more DNS names, different personnel names and phone numbers. Maltego found results better than searching manually and it was faster. Shodan found other

domain names that were almost the same as the company's but still were a different domain. All domains were checked and removed if not related to the company. After removing all that did not belong to the company, the domain search was run again, which gave more information such as email addresses, phone numbers and DNS names.

The author continued information gathering from found results on domain name search phase. DNS names were the first. During this phase, Maltego linked IP addresses to all DNS servers and linked similar servers together. This information gives an attacker a good understanding about the relations of the servers to each other and web sites that belong to that DNS server in some way. DNS information revealed more accurate domain names the syntax of which was text.company.fi. More DNS names were also found, and they needed to be searched again. After the search, more NS records were found that not not directly connected to the company but belonged to Amazon. There are probably some Amazon services running.

After searching information from one of the subdomains found on the DNS gathering phase, many subdomains found on Domain name search phase, were linked to together. More NX records and email addresses were found as well. There are many subdomains but after gathering information about them all, it was noticed that there were not many related directly to the company itself. Most of them were different domains and related to different companies. Some of them were related to the company such as websites which redirected to the real website of the company. Searching all subdomains and finding which ones are relevant and related to the company is time consuming.

Information from the IP addresses contained more domain names and services that were turned on. More personnel names were also found, which gives more attack points. IP addresses gave other company's information. After the Internet search, these two companies merged together. IP addresses and plenty more information; necessarily not relevant, because information could be obsolete already. Two of the addresses belong to the Finnish operators. One of them is the operator whose responsibilities are company's network of places of sales and the other probably is an operator controlling the company's WAN.

Websites search found very interesting information. Maltego found technologies used on the websites such as X-XSS-Protection, X-Frame-Options, jQuery and DAV. This kind of information does not help social engineering attacks but helps much when trying to find vulnerabilities that could be used to penetration. Maltego found also a relationship with 3rd party such as Google Analytics on the websites.

Every search might bring out more information such as domain names, IP addresses, subdomains so to get accurate information, the search must be done multiple times, and it is better to mark all of those that were searched before. This helps to see which are the new ones and need to be searched. It also helps removing all non-necessary findings. Otherwise, all non-necessary information is found as well, and there could be soon so much data that it is futile to get any information from it.

3.3 Physical penetration testing

Physical penetration to any company is very simple if the personnel is not aware, do not check and watch who comes after them or walks inside without an ID card. No matter if that person is familiar or not. This chapter focuses on physical penetration testing, which is done using cases based on the survey questions. Table 3 shows these cases and all their objectives and purposes. The objective column informs what the meaning of this case was, and the purpose indicates which survey question this particular case will answer and verify.

Table 4. Physical penetration cases

Case	Objective	Purpose of the case
1	- Get inside to the building following employee - Tailgating	- Test and verify survey question 8 and partly question 14
2	- Get inside the building using a fake ID card.	- Test and verify survey question 11
3	- Walking inside without ID card - Tailgating	- Test and verify survey question 14 and partly question 8

3.3.1 Case 1

This case includes two different scenarios. The first scenario was carried out five times on a single day in about three hours' time slot and the other scenario was done four times; however, on different days and a different time of day. Table 5 summarizes all these scenarios. The time column indicates the time when attempts were launched, the breaching point shows where this penetration happened, and success rate explains how many attempts this particular scenario took and how many of those were successful. The information informs briefly about the scenario and what happened in it.

Table 5. Case 1 scenarios and results

Scenario	**Time**	**Breaching point**	**Success rate (attempts/successful)**	**Information about breach**
1	Morning when employees come to work. (7.30 am – 10 am)	Personnel main entrance	3/3 Success	No questions asked and not watching behind. Not trying to get any floors.
		Side door	2/2 Success	Getting inside via stairs and elevator to the floors with "helpful" employees.

2	Morning (8 am)	Car garage	1/1 Success	Through car garage to the building and the floor via elevator with employee
	Midday (10 am)	Personnel main entrance	1/1 (tailgating) Success 0/1 (moving without ID badge) Failure	Tailgating inside and to other floors. Got caught from unfamiliar employee on the floor
	Morning (7.30 am)	Personnel main entrance	1/1 Success	Tailgating to the building and then with another employee to the floor via elevator.
	Morning (about 7.30 am)	Side door	1/1 Success	Un-familiar employee opened the door from inside and let me pass.

				Used elevator with other employees and got to the floor. No questions or any verification asked.

The case was simple on both scenarios. The author stays outside and not wear an ID card at all. It was about just waiting for a potential victim who would let the author in. When the employee came, then it was just about following this one in. More information about these different scenarios can be below.

3.3.1.1 Scenario 1

The first scenario was performed five times and all of them were successful. Three tests were successful from employee's main entrance. Nobody looked back if somebody else was coming after them; not even when the author ran inside, which was twice from the side entrance. Those times the author watched a phone, so it looked like a busy moment and nobody did disrupt him.

Those side door penetrations were the most interesting part of all. During those times, accessing to floors was a success as well. For the first time, the author was waiting for an employee when coming to work and walking behind the person inside the building. The employee used stairs and the author was following him to the other floor. The employee even held the door open.

The second time was the same; however, this time the employee came from inside out for a smoke. After a while a co-worker came and they talked about 10 minutes. During that time, the author used a phone and waited close to them to get in. That time is was a risk because when going in behind them after waiting, what they would

say in that case. They said nothing and the author got access to another floor using the elevator with them. Why stop there and why not get another floor using stairs when one had got inside? After waiting in the stairs for about 30 minutes, an employee came from the lower floor and very surprisingly went to the floor where the author was waiting. Nobody watched after the author and yet another floor was open to him.

3.3.1.2 Scenario 2

The first attempt of scenario 2 was successful via carpark in the morning. The author was waiting outside when the personnel come to work by a car. When the carpark's door was open, the author walked inside. The author waited some time near a door on cover and tailgated inside the lobby. From there the author continued to the floor via elevator with an employee. He had his phone all the time in his hands and no questions were asked. After a while, he tailgated again to a lower floor. Some personnel watched when the author was coming after them; however, not everyone and nobody doubted the author's rights to be inside or asked anything.

The second attempt was successful from the personnel's main entrance. First there was tailgating inside and then to the other floors wearing an open jacket and sunglasses hanging around the neck. The purpose was somehow to get the personnel watch who is walking inside. For that reason, the sunglasses were hanging to get the personnel's focus more on a possible ID card. After accessing some floors, the unfamiliar employee was sharp to make that first question about the ID card. He rechecked ID card for the second time after seeing it.

The author followed the employee through the main entrance during the third attempt. Then he waited inside when another employee would come and try to enter the floors. There was no need to wait a long and the author managed to get into an elevator and to the floor. There were not so many employees at work at that time so malicious social engineer could do many things. Nobody made any questions what is going on. The author was wearing shirt, shorts and backpack.

Attempt 4 was interesting. When an employee opened a door, the author tried to get inside; however, the door closed and could not get in. However, an employee who just came in, opened the door for the author and let him pass. The author used an

elevator where there were more employees; yet, nobody checked the ID card or not even watched more closely who this guy was and the access to the floor was successful.

3.3.2 Case 2

Images were found on information gathering phase where was a personnel ID card almost visible. The images showed the background color, logos and their positions. The only thing that was messy in these images was some text below in the employee's image. However, it can be assumed that it contains at least the employee's name. With these pictures at hand, a personnel ID card can be done. If that text needs more verification, more information is needed and, in that case, the best solution is to get a picture of a personnel's ID card.

This case was done six times and at a different time and on the different day to get more statistics. Table 6 summaries these attempts, times when they were executed, if that attempt was successful or a failure and there is information and summary about that attempt. The table below describes these attempts more in detail.

Table 6. Case 2 results

Attempt	**Time**	**Successful (S) or failure (F)**	**Information and summary**
1	11.30 am	S	Receptionists deceived by the fake card.
2	7.30 am	S	Employee opened the door and helped to get to the first floor via elevator. Card was not checked.

3	9 am	S	Used side door and through that got access to the floor via elevator with employee. Employee watched more closely at the card but did not ask to see it better.
4	8 am	S	Floor access via elevator. Employee did not watch at any way the ID card.
5	8 am	S	ID card was not watched when got access inside. Floor access with another employee.
6	9.30 am	F	Very good security behavior from one of the consultants. Very sharp eyes, good

			questions to verify and information to the security team.

After creating a fake ID card, it was first tested by going to receptionists. They see many ID cards and if that fake card deceives them, then it can be said that the first attempt is successfully tested. The plan was simple: the card is not working anymore. They took it and looked at it. Then they started to troubleshoot the problem and finally took that card out of its ID card holder. The back of the fake card was empty and that made them notice that the card is not real. But only that; so, if personnel, who watch it, do have not very sharps eyes, this fake card could fool them, and the door would be is open.

The pretext was simple at every attempt. The author pretended to be an internal employee whose card is not working anymore. For that reason, the door would not open. The author had hurry to work to solve network problem and he will solve this card problem when he has computer access. The objective is to get an employee to open the door and from there to get to any floor.

Attempt 2 went as planned. An employee opened the personnel entrance's door after the author said that the card is not working anymore for some reason. He did not check the card closely but only saw it. He said that the card should be checked and showed where to go; however, because of the hurry and after saying that the author would solve the card problem when he gets to the workstation, he got access to the floor. The author asked an employee which floor he goes and saying that going to the other floor helped the author to get that floor. The employee used his own card on the elevator.

The author waited for a while on attempt 3 an unfamiliar employee who would help him to access to the floor. After using the pretext, the author got inside and then to the elevator. Because the author card was not working, the employee used her own card on the elevator so the author could continue. She recommended that the card

should be checked right now but because of the author's pretext and hurry, the employee gave access to the floor. She looked more closely at the card when it was hanging on the neck but did not see it was a fake.

Attempts 4 and 5 were successful just like the previous attempts; no questions were asked and floor access was granted. All employees asked the author to go and check the card. Attempt 6 was a failure. Consultants noticed a fake ID and after that made a very good questions to verify who this guy is and if he has rights to be inside. He was ready to call the security that there is an unauthorized person inside. He said that the author's behavior and answers to his questions, a fake ID card and clothes that the author was wearing were the things that made him doubt.

3.3.3 Case 3

This case was almost the same as in a case 1 but this time the author did not even try to hide a possible ID card. He Just walked through the floors without an ID card nowhere to be seen, not even wearing and tailgating to other floors when it was possible. This case was performed twice over three days. The ID card was not worn at all on those days. Not even when the author went to get a coffee or walked in the building and on the floors. Table 7 summarizes this case. The first column indicates which scenario is in question, the duration shows how long the scenario took and the information summarizes that scenario.

Table 7. Case 3 results

Test scenario	**Duration**	**Information about attempt**
1	1	Moved from end to end on the floors. Greetings from familiar employees but no questions or other interruptions. Tailgated sometimes to another floor.

2	2	Same as above but duration was longer.
Related to the case 1 breaches and their information	4	No interruptions when walking. Only got caught once by unfamiliar employee.

The author started this first attempt from the cafeteria where tailgating gave access to the first floor, he just walked and nothing more. He could walk freely without any interruptions and continued walking from floor to floor. Sometimes the personnel who knew the author said hi but nothing more. Once an employee would have given an old computer but after saying that the author was not working right now gave time to continue. Even that did not arise any questions about what is going on or where the ID card is. The whole building was walked through without any serious interruptions. The second attempt went as the first attempt: no interruptions and question asked.

The personnel did not do anything on those days when the author was walking without an ID card. On the third day when he was tailgating inside the building and continuing to get deeper and the other floors, an unfamiliar personnel member noticed the missing ID card. The employee allowed the author to enter to the floor from the stairs but followed and asked for the ID card and even re-checked it.

3.4 Information from simulated phishing emails

Phishing emails are a very popular and effective way to get information or lure a person who is unaware to open a malicious attachment or visit a malicious website. These emails might be so good and well done that even professional security person could be fooled. Simulated phishing email could help to recognize and teach the personnel to see them and report them. These are only for educational purposes and not real ones; however, they are like real ones so everybody can see and learn about phishing emails.

Table 8 shows the information of simulated phishing email from the company's report for about a four-month period. The first column indicates the name of the phishing email, the clicked column shows, how many persons have opened that malicious email and its link or attachments and its per cent; and the reported column informs, how many have reported that email as a phishing email and its per cent. The total column indicates, how many employees have got that phishing email. The table shows only phishing emails the total attendees of which are over 75 and not those with a few total attendees. The reason for this was to gain better results.

Table 8. Information in the simulated phishing emails

Name of the phishing email	Clicked	Clicked %	Reported	Reported %	Total
yammer.mention	19	12 %	87	54 %	161
linkedinJoinNetwork	17	9 %	84	45 %	187
dropboxNewLogin	16	9 %	93	51 %	182
linkedin.ceoConnect	7	8 %	51	60 %	85
linkedin.ceoMention	7	7 %	55	57 %	96
invite.linkedin	12	7 %	61	36 %	169
office365.protectedMessages	12	7 %	99	58 %	170
linkedinVideo	11	7 %	111	69 %	161
office365SharedDocument	11	6 %	98	57 %	173
yammer.coworkerMention	11	6 %	112	62 %	182
whatsappVoiceMessage	12	6 %	112	55 %	204
slackInvite	11	5 %	93	45 %	206
yammer.updates	4	5 %	40	53 %	75
office365ReviewDocument	7	5 %	78	59 %	133
netflixBillingInfo	10	5 %	98	49 %	201
onedrive.sharedDocument	7	5 %	72	49 %	147
facebook.postMention	4	4 %	64	72 %	89
amazonBlockedLogin	6	3 %	102	55 %	184
yammerGroupInvite	5	3 %	72	45 %	159
spotify.freeSubscription	4	3 %	84	65 %	129
airQualityQuestionnaire	5	3 %	88	51 %	174

microsoft.sharePermissions	4	3 %	97	64 %	152
office365AccountDisabled	4	2 %	93	53 %	177
wetransferShare	2	2 %	71	71 %	100
microsoftPasswordUpdate	3	2 %	102	59 %	174
microsoft.SmartScreen	4	2 %	143	60 %	239
yammer.newLogin	2	1 %	83	51 %	163
microsoftSecurityIssues	2	1 %	99	55 %	179
microsoft.sharePoint.brexit	1	1 %	96	65 %	148
passwordManagerLastpass	1	0 %	119	56 %	212
microsoftSafeLinks	0	0 %	125	58 %	216
office365.backup	0	0 %	110	60 %	183

The table above shows that there are many different phishing email types. There are phishing emails related to social media such as Facebook, Yammer and LinkedIn; cloud such as Office 365 and DropBox; Microsoft and many more. This shows that a phishing email could be anything and only mitigation about these is training to spot these.

4 Research analysies

4.1 Research limitations and reliability

The questionnaire gives the baseline about the personnel's security culture and awareness. Its reliability is very dependent on the total number of the attendees and if the answers are genuine or not. If the majority of employees answers this survey, it is much more reliable than if there are only a few. There are very likely attendees who just choose something without thinking and the reliability drops. More attendees are excluded better out those false answers and better reliability is kept.

Although this survey was pointed to all employees of the assigner company, it was clear to the author that most of the attendees were from the HQ. Based on that, he calculated an error margin using the total number of all employees in the HQ which was about 9% with 90% reliability level. The total answering per cent from all

employees in the company was only about 3.5%. Because the total number of the personnel number in the HQ or in the whole company is not known, these per cents maybe be slightly different but they are still close.

The author has been working with the assigner company several years. Physical penetration cases could give false information. To keep better reliability on this, the author has not worked in the company and has not been inside for several months. The purpose of this was employees' memory. They might forget at least that the author was there, and another person makes the author's job. Physical penetration reliability was also improved when the author made penetration cases and targeted personnel which were unknown to him and the author have not ever met them face to face and never worked with them. However, cases that involved being inside, the author did not have many options to keep them reliable. The only way was to observe what known and unknown employees do and examine their behaviour.

The data of the simulated phishing emails is the worst reliability issue. Every week there are more phishing emails sent to the personnel. When writing this, the information of the phishing email could already be obsolete, and all its statistics might have been changed. It is impossible to keep up to date statistics about them and that does not help with the research. The point of this research is to provide some understanding about phishing emails to the company; however, the company needs to check the current phishing email statistics and make a judgement based on that information.

4.2 Survey

Although the survey does not directly answer any research questions, it is still vital to know, how the personnel handle social engineering attacks at least on paper. The questions included many attack techniques of social engineering or what social engineers are after, such as passwords, disclosure of information, pretexting, baiting using USB sticks, tailgating and phishing.

Gaining an employee's credentials is a dream for all hackers and social engineers. Using them gives more attack patterns which could be used to get deeper onto the network and maybe not be noticed at all or noticing will take time. The complexity

settings of a password guarantee that it is stronger than without; however, a person can still make a weak password. The author has seen several times that many weak passwords with complexity settings turned on use the same syntax which is “dictionary word” (many times month and begins with uppercase) + “number” (a year). This kind of password meets all complexity settings but is still weak, such as an example password November2018 on the survey’s question 1. Hashkiller cracked both MD5 and SHA1 hashes approximately a second but SHA256 hash was not successful. This only shows how vulnerable these kinds of passwords are.

Analyzing questions 1 to 3 and calculating answers from the respondents gives information on how bad weak passwords are which are used on multiple different services. 27 persons use a weak password (Figure 5), 26 use the same password on different services (Figure 6) and seven use a same password on work related systems and personal services (Figure 7). Very likely, some of those seven employees use a weak password and very likely use the same password on other services. If a hacker gets the password or its hash on one of them, it may compromise a company and other services as well. In addition, because of using the same password on the many services, the attacker gains more attack points to get that password such as compromising public services, e.g. Facebook and Twitter or using phishing and then using that password to the work systems.

Fire alarm means that everybody must leave the office and go outside. An adversary who is already inside could observe and look for potential targets who leave their workstation open when going to print or a dinner and then trigger a fire alarm. Then one can use an unlocked workstation. There is another action that could be used and that is using research results. According to Ponemon Institute LLC (2019, 12), 26% write down passwords on a paper or sticky note. An adversary can just look for any password list from the employees’ desks and closets when everybody is outside. Finding those two of all employees (Figure 8) who go out and leave the open workstation behind could be very hard; however, not impossible.

Information is an asset on any corporations and that information is handled mainly by people in their heads and workstations. When six of the respondents (Figure 9) say that they or their workstations have not any valuable information, that only indicates that they probably do not know what some valuable information is that

they have and need to protect. The same can be assumed about employees, who think that they or their computer has no valuable information. When a social engineer finds one of those six employees who thinks there is no valuable information in their heads nor their workstation and starts to use persuasion or manipulation, the social engineer will get information because the victim does not understand what he/she gives.

One of the effective ways to get information or lure a target to do something is using authority. Authority combined with being in a hurry and the feeling that there is “no” answer will be devastating combo. This combo and a phone make this hard to see and resist. Although almost 80% (Figure 10) will ask for more details about the request and the caller. In real life, some of those or almost all will be deceived if a caller is a professional, who has made a good reconnaissance and is a social person who can talk and build rapport easily. A prepaid phone is a stealthy device and helps social engineers much to get what they are after. Vishing is a technique where the victim does not see a caller and cannot make a judgement about the person’s behavior, postures and how one talks. The victim must only trust his/her own feelings and listen very closely what and how the caller is saying his/her message. It depends so much on the caller and the victim how successful an attack is. However, the author thinks that a social engineer has an advantage over a victim because the social engineer has time to plan the attack and what is said. This is a reason why the author thinks that most persons give information over a phone and it is more than just that one person (Figure 10).

Baiting with USB sticks is another effective way to get malware to the devices. One study’s results were that 45% opened unknown USB stick’s file, and 98% dropped USB sticks were not in the place were left originally (Tischer, Durumeric, Foster, Duan, Mori, Bursztein & Bailey 2016, 4). People are curious what kind of information USB sticks contain; they like to find the owner or they start to use them. Questions 7 and 10 concern unknown USB stick questions. According to the information of the question 7, 70% do not plug that discovered unknown USB (Figure 11) and according to question 10, then 93% do not plug unknown USB stick what was from a colleague (Figure 14). Between these two results there is a major difference. There are two persons who do not know anything about that USB stick and that makes a stronger

feeling not to use it. However, there is one question about that 93% who do not plug that unknown USB stick which a colleague found. Who really asks colleague about that USB stick? It must be said that not so many. Using an unknown USB stick oneself or for helping a colleague is almost equal about a few per cent. There are always people who use unknown USB sticks without thinking what they could contain. Using an unknown USB stick might be more common in a real life than those 3% or 6%, unless people are aware of danger about these.

Surveys are a nice tool to get information. If done nicely, small talk is used to gain trust, the order of the questions has been thought out before the call and the caller is a professional social person, which then can give plenty of good and possible sensitive information. Question 9 is a vishing survey. According to its data (Figure 11), it can be said that people more willingly give personal information than information that is related directly to the company. About 40% and more give information about their job, education and if they have subordinates. This is more personal information. When the questions start to get more company related, there are more “no” answers. There is a huge difference between those personal and company answers. It seems, people understand more about what information may reveal about the company or they understand questions such as how to walk inside or personal ID number that these do not belong any survey or why a survey even needs to know about these. Again, there is a big “if” when a caller is a professional.

People seem to understand according to Figure 14 what danger may be lurking in unknown websites and unknown software which might be downloaded and installed. Even that the caller is from “service desk” and try to help an employee to remove that malware they understand to think and evaluate the risks what was asked and what they need to do. However, some would ignore this warning. Do they not understand the risks if the malware is real? They can jeopardize other devices and even servers if the malware is programmed to spread over the network just explaining to oneself that there is no way that they could have something. In addition, there are always people who do what others ask them to do. People need to think and evaluate all that another person says, and it is more important over the phone because one does not see the other person who might be an adversary. Every decision that a person does and is related to oneself and action, includes self-

awareness and danger evaluation what could happen if one does it. From the company perspective, there could not be so much this self-awareness thinking because actions do not directly affect the persons themselves but the company and its assets. People need to think all out-of-the-box at work. Actions might not affect directly the person but indirectly they could such as in this case malware or ransomware which could spread over the network and encrypt other devices which then could affect a person such as encrypting server where all employees' salary information is stored and in consequence, employees do not get their pay. It is always better to make sure there is not anything that could be harmful; do not do directly what some other person says and think of a safer way to deliver that potential infected device to local support or the person who one trust.

Spear phishing might be very hard to spot but even harder to spot is lateral spear phishing where a hacker uses hijacked legit other employee or a friend's email account. Most people trust their friends and co-workers and why should they not. According to Figure 15, 3% open that link which co-worker sent. However, more important information in that figure is the percentage of those ignoring it. 26% ignore that message. Ignoring is sometimes acceptable; however, in this case, it is the same as opening that link. Ignoring can just inform an adversary that the email did not work and he/she sends it somebody else. Of course, the adversary does not know what happened that email and hopes that another person opens it. It is always better to verify email from the sender if it looks suspicious or/and inform it as a phishing email. By informing an email as a phishing helps security personnel investigate it, warn the personnel and take countermeasures if necessary.

Questions 8, 11 and 14 are analyzed in subsection 4.3 Physical penetration. In that section, all cases are discussed as well.

4.3 Reconnaissance

There is plenty of information to be found about the company. Social engineering focuses on hacking humans so any information to accomplish that is useful. However, successful attacks need information about everything that company does, how and where to contact it and information on the personnel. A social engineer or

hacker/adversary can build a good topology using that gathered information and start to plan an attack.

When watching Table 1 information gained from the company's website and thinking about this information from the social engineering point of view, some attack scenarios can be thought out; however, more information needs to be collected to plan those. One type of attack could be related to the charity. That action will need information such as how to seek it, who to contact and how. A social engineer could use influence to get that information from one of the charity customers and use that gained information to plan an attack. Another way is just to contact the company and ask the company what to do and how to be a part of the charity. Either way, the gained information might help a social engineer to attack. Another attack scenario might focus directly on the personnel whose information is on the website. Making a phishing email campaign using email syntax might be very effective. There are not so many employees' names or their information on the website so finding more potential targets using social media could be another gathering method. If the plan is to make a spear phishing campaign, then there is much information that needs to be obtained to launch an effective campaign.

Searching information about a target using the Internet and the Google is a recommended step which might give information and help to make attacks possible (Table 2). The Google search gave many potential attack scenarios. Just searching for images gave one case which was launched: using a fake personnel ID card. Another attack scenario could be to pretend to be a tablet manufacturer and use that to lure a victim to disclose information or make one to open an attachment the subject of which might be, for example, new features on the next patch. That information was also obtained from the images. Another two pretext attack scenarios focused on the personnel using a new service provider information or operator who controls the places of sales' network. Both types could use many social engineering techniques. Visiting one of the places of sales and pretending to be from the operator might give access inside. Using vishing and pretending to be from a help desk on a new service provider might fool the personnel because they do not necessarily know a new help desk well. Previous attack scenarios could be potential and only need a good social engineer.

Searching for DNS information was a treasure. All information was visible and there was no hidden information. The Internet DNS search with Maltego information (Table 3) together gave plenty of data. The information shows how all public services link together and their IP addresses as well. Much of the information found just using the Google was the same as on the Maltego; however, it was much faster than a manual search. Interesting information from these were personnel names which can be found from in DNS records and Maltego. Total of five person's names was revealed and because they are from this kind of information, the question is who they are. Searching for information from social media (LinkedIn) gave their job titles and functions. One of them was not working anymore at the company but the other four were. There was not much information one of them. One of them was a network specialist and was linked to multiple IP addresses and blocks on Maltego; another was a DevOps specialist and the last one was an ICT Manager. When thinking about their jobs, they could have or have had access to very valuable information such as network topology, inside servers' names, IP addresses and implemented security devices. This information will make penetration easier and not only talking about social engineering attacks but also for a technical hacker who tries to bypass security from outside.

Maltego provides very good information about the company and its publicly visible infrastructure (Table 3). Not all its information is really for social engineering but for all hackers who try to get access to the company and its assets. The technology with which the websites were constructed might be a good indicator for finding potential vulnerabilities, and subdomains might reveal platform and version numbers e.g. such as Apache if not configured correctly. Moreover, this information would help to find vulnerabilities. Maltego found ports as well which are open for public. In addition, because Maltego is a passive reconnaissance tool, an intruder knows open ports without the use of any active scanning tools such as nmap and can concentrate on those only. However, this information is not enough to really find more information or vulnerabilities and there is need to use active reconnaissance tools as well.

When comparing information from the company and the operator, there is not so much differences. The same attacks scenarios might work with both with little working and changes. More information is needed for both but they both have a

personnel ID card visible and making one's card is not hard. This was the only direct attack type that could be gained from the collected data and it does not need additional information to launch.

4.4 Physical penetration

When comparing the survey's answers and testing cases, most of the data and information are the opposite of the other data such as walking behind of an employee enter a building. The data indicates that most of the employees ask for an ID card before letting unfamiliar person in; however, in the real act all was successful expect the one time when trying to get to the one floor.

4.4.1 Case 1

The success of tailgating depends so much on the security behavior and culture of the personnel. They are the first line of defense against physical penetration and social engineering. Table 9 summarizes the answers of question 8 and their percentage and the results of case 1.

Table 9. Comparing question 8 and results of case 1

Question 8		**Case 1**
Answers	**Answer's per cent**	- Tailgating success from outside 9/9 - Question asked when tailgating in 0/9 - Tailgating success when inside 5/6 Notifications about the case: - Floor access via elevator and ladders by tailgating
I'll let him in, but I'll inform this to company's personnel of security, security company and other related parties.	3	
I stop him and inquire who he is,	83	

whether he has a company ID card and what he is doing, etc. I will not let him continue until I confirm the person's right to be in the premises.		
He must be staff. New employee maybe.	14	

Over 80% would stop an unknown person and ask who he/she is and where the ID card is. However, in the real act in case 1, the success rate was 100% when trying to get inside from outside and no questions were asked. Tailgating was also successful when continuing penetration deeper to the building from the stairs and via an elevator. When more tailgating attempts were carried out and they all succeeded, there was a time to be more reckless and try to find out when and in what situation somebody stops the author.

Analyzing that one attempt where the author was caught by the employee and comparing all successful penetrations to it gives some understanding why that happened. All previous attempts were made by really trying to be someone who has rights to be inside and walk there. Although waiting on the stairs to get inside should be an alarming sign for somebody, nobody did not do anything and the access to the floors was successful. The author’s behavior and body language were the reasons why an employee got suspicious. Looking like somewhat lost, searching for something and in this particular case watching from the stairs when an employee comes and then waiting there using a phone and going to the floor when the employee was going to the lower floor was enough to raise an alarm with that employee, after which the employee followed the author to the floor and asked about his ID card.

4.4.2 Case 2

Using a fake ID card was one of the cases because in the information gathering phase images were found where there was a personnel ID card visible and based on those images, a fake ID was done. There is no need to jeopardize identity if trying to get pictures about ID cards from the personnel. Table 10 summarizes the answers of question 11 and their percentage as well as case 2 results.

Table 10. Comparing question 11 and results of case 2

Question 11		**Case 2**
Answers	**Answer's per cent**	- Card watched closely when trying to access using a fake card (want to really see it) 0/5 - Card watched more closely when hanging on the neck (not wanted to see it better) 2/5 - The author got caught 1/5 Notifications about the case: - Everybody opened the outer door - Everybody asked to go to see the receptionist about the non-working card - Everybody granted access to the elevator and the floor
I examined his card properly so I can be sure that the card is right, and the person has the right to pass. However, I ask a person to go through a receptionist where the card rights can be looked at so that the person can go inside.	89	
I examined his card properly so I can be sure that the card is right, and the person has the right to	1	

pass. After verification I open the door to him.		
I examined her card quickly and when it seems to be right, I open the door to him.	10	
I'll let him in on my own card without any further confirmation	0	

According to questionnaire's answers in Table 10, nobody uses one's own card to open the door without confirmation. Moreover, almost 90% examine the card and ask a person to go to see a receptionist who can check the card and why it is not working. All of those answers to question 11 do not include one important step or option. A fake ID card may be so good and well done that it may fool anybody. If a card is not working, the person should be handled like a visitor and escorted to see a receptionist or somebody else who can check the card. When this kind of security behavior is implemented to any company, it will prevent all social engineering attempts that use non-working fake ID cards or stolen and obsolete card as well.

The real act gave mixed results from the answers of question 11. Everybody used their own card to open the exterior door after the author said that the card is not working, and everybody recommended him to visit to a receptionist to check the card. Everybody used their card in the elevator so the author could get to the floor after saying that he is in a hurry and he will contact the receptionist about the card when in the workplace. Everybody more and less checked the card when it was in the neck; however, nobody really asked to see it. Even in the one caught by the consultant, the breach was successful because floor access was granted. Eventually the author should have been caught by security personnel because the consultant was trying to contact them. The success rate for penetration to the building and the

floors using a fake ID card was 100%; however, that one exposure drops the success rate to 80%, which is still very high. There are two questions about this: how much time security personnel would need to find an unauthorized person and how much time does an employee need to report that breach? During that time, a social engineer could do much damage depending on the purpose.

Analyzing that one expose about using a fake ID card gave much information. From the beginning, there was a feeling that the consultant knew about the breach. After accessing the floor, it was time to talk about situation with the consultant, explain it and ask questions about the breach. The answers to the questions made by the consultant, not wanting to go to see receptionist about a card and the author not having a workstation or backpack were cases which exposed the author. The consultant said that nobody has explained the security policy to him, so he did not know where to contact and how. He did not know how to handle this situation and the breach but he was ready to do something. Only this case shows how important training is and more importantly, how to mitigate physical penetration attempts, how to handle them and what to do when penetration happens.

4.4.3 Case 3

The company's ID card verifies that a person wearing it has rights to be inside and belongs to the personnel. Table 11 summarizes the answers of the question 14 and their percentages as well as the results of case 3.

Table 11. Comparing question 14 and results of case 3

Question 14		**Case 3**
Answers	**Answer's per cent**	- About 7 hours inside without any interruptions - One capture in case 1 Notifications about the case: - When person is known by others, he/she is free to walk - Unfamiliar employees did not do anything
I stay and start to talk to him to get to know the person better.	47	
I say hi and ask where the ID card is.	49	
I'm going to the cafe. The card is probably just under pocket or under the shirt and not visible.	4	

According to Table 11 and comparing its data, the author should have been caught many more times than only that one time in case 1. When thinking about the duration inside without being exposed, a malicious social engineer could have done very serious harm and could have stolen sensitive information. This case was an outsider threat but also an insider thread. When moving inside and between floors, one can think that there were both threat types; somebody knew the author and somebody did not. In addition, with this information, one conclusion can be made; an inside threat is dangerous and maybe even more dangerous than an outside threat. A totally unknown person walking inside is maybe spotted easily by the personnel; however, when the person is known by them, they probably do not understand that this person should not have the right to be there, and absolutely not a person who does not wear any ID card. The personnel who knew the author just greeted and asked for help like they would on normal working day. This kind of

behavior the author met inside without wearing an ID card. This behavior verifies to some point how co-workers trust each other.

4.5 Simulated phishing emails

There is plenty of data in Table 8 to analyze. To make the analysis easier, there are three categories based on the clicked per cent: **low**, **middle** and **high**. Low category includes phishing emails where the clicked percentage is between 0% to 3%, middle is from 4% to 6% and high contains at least 7% and over it. Although real simulated phishing emails were not available to send to the personnel, phishing email's name gave a hint what kind of email it is.

Low level category contains 15 phishing emails. Eight of them involved to Microsoft and its services, two Twitter and the rest is different kind of emails such as Spotify, Amazon and a questionnaire. When looking at the total column of these (total attendees is 239 in Table 8), it can be stated that these are almost all the first phishing emails which were sent. They look like real but have misspellings and when one hovers over the links with the mouse, the links very probably point somewhere else than they should. More advanced phishing emails might include links that seem legit and there is no way to say if it is real or fake unless the person knows the real address which is often unknown.

There are four phishing emails in the low category, which is more or less a surprise; why are those not clicked more: new login on Yammer, account disabled on Office 365, free Spotify subscription and a blocked login on Amazon service. If a person does not have Yammer or Amazon accounts, it should be easy to figure it out that the email might be phishing and should be reported. Occasionally people are deceived by these counting on that they start to think if somebody has stolen e.g. their credentials or their personal identification number (PII), bank numbers and used those to make new accounts. People like to investigate more what is happened and open links with fear. Office 365 disabled case also uses fear and irritation. The person cannot use cloud services such as email if an account is disabled and email is crucial for the work. Free Spotify subscription uses the influence principles scarcity and reciprocation. It is a gift that might have only limited time to get as in "act fast to get

it". The only thing that explains why these are not clicked more, is employees' awareness and education to see things which are not right e.g. email's links; or employees report these just in case because they are unexpected. The same argument can explain all other phishing emails in this category.

Middle category includes nine emails that are older and newer. These newer emails might be more advanced emails to spot. Here are also many different email types compared to the low category where most of the emails were related to the Microsoft. Many of this category affected a person's curiosity such as Slack invite, WhatsApp voice message and Facebook post. Netflix email uses a fear like on some emails in the low category; fear that somebody has hacked one's Netflix account or created one using a person's information and credit card.

The author got one of this category phishing email that can be further analyzed. The email contained a shared site link sent by a "co-worker" and the topic was how Brexit impacts the author's company. Curiosity and fear were keys in that email. What does Brexit mean to the company and how does it affect a person's job? Is there a job after Brexit is finished? The email contained links but hovering over those with the mouse did not really give any useful information unless the person knows the exact links where they should go. The sender's email address was one that was not genuine and indicated a possible phishing email. However, using that verifying any email, there must be an understanding, how domain name syntax is built. Microsoft.com is a genuine domain name used by Microsoft: however, microsoft.eu.com is a totally different domain and not necessarily a part of the Microsoft. It is not easy to see these and most of the employees could not even know what a domain name is or how it is constructed. It is not their job to know. Another clue about phishing email was the sender. The author did not have any clue, who he was or did not find him anywhere.

There are eight phishing emails in the **high** category. A common element can be seen here. Six of eight were related to social media. The other two were DropBox and Office 365. All of these have also one element which is to raise feelings; that feeling is curiosity. Who would not be curious if CEO mentions a person on the LinkedIn or one gets a protected message the subject of which is a promotion 2020 like the author did? Curious is an effective strategy to deceive another person to open that

email's link or attachment. Another effective feeling is using a fear that a new login to DropBox phishing email uses with curiosity. When watching Table 8 data, all LinkedIn phishing emails belong to this high category. There are not any LinkedIn phishing emails on the other two lower categories.

5 Conclusions

Although there are no real research questions about the survey results or personnel security awareness about social engineering attacks and techniques, it is still nice to know the current status at least on the paper. There is no perfect company, no perfect security behavior or in some cases, no perfectly implemented security devices. There is always some area that could be used to launch an attack. The overall status about personnel security behavior and culture in the assigner company is good; however, there are still weak links and the weakest link is people. Most of the personnel would do a very good job defending the company and its assets against social engineering attacks; yet, there are people whose security culture is not so good and using them to get inside is possible. When this is understood, it is possible to teach and educate people to see and prevent social engineering attacks or any attack as well. Education and showing people attack scenarios of social engineering helps them and the company to spot these and the company is a safer working place.

5.1 Is there publicly available information that gives away too much information to launch attacks?

When thinking about all that information that is available for public and if that information gives away information that makes the company more vulnerable for attacks, the answer is yes but nothing very critical was not found. DNS information is very readable and is not hidden or secret. That information gives two targets and searching information from these using social media such as LinkedIn gives information on very potential targets because of their position and the information they could have. Maltego gives more targets as well. However, these targets are not any part of DNS information but they are found and therefore they are somewhere

publicly available when searching using a domain name. LinkedIn is very good for gathering information if a person uses it and keeps it up-to-dated. Its information gave more details of these employees. However, these persons could be found in social media just by searching manually using plenty of time but because they were found by some other way easily and fast gives a starting point where to start looking for more potential targets.

Another attack information were the images showing the personnel's ID card. This information made it possible to create another case for physical penetration phase without trying to get a picture of an ID card from one of the employees with a camera which might reveal an adversary. Because the images are already on the Internet, they stay there. It is more important now for the company to know and understand that those images are available for anybody who knows how to find them. It is better to know all images or any data on the Internet that might give away information about the company so they can make plans for their public information.

5.2 Are there any differences between survey answers and real act?

When comparing the survey results and real act, in this case physical penetration, we can see many differences. On paper, everything looked good but in the real act, it was proven that people behave differently and do things or not, which makes a possible breach true. It is much easier to answer questions where choices are already present, and one only needs to choose the best of all. When a person is dealing with a real scenario and attack, there is limited time to act and all acts should come from the backbone without much thinking. Training, education and security policy will help to accomplish this security behavior on how to handle and what to do. However, it would be more beneficial and suitable to show personnel social engineering techniques and attacks in real act and teach them some remediation and mitigation actions than just order them to read all guides or watch presentations.

Employees must be aware of social engineering's attacks and techniques which are used. Although exposing a social engineering attack when it is happening might be very hard if the adversary is skilled, there are or should be guides and policies which help to accomplish this if followed. However, these guides and policies must be easily

found when required. It would be better if some of those guides or all of them come from mind naturally when needed to provide a good security culture.

5.3 Is there any pattern how employees handle possible physical security breach when a social engineer walks among them?

What employees did or did not do when granted access to the inside of the company, or walking on the floors without a badge were not representative of a very protective culture. There are three patterns that employees used and how they behaved when a social engineer got access to the building and the floors. Most of the employees did nothing to prevent accessing the place or walking without a badge. The outsider threat is dangerous; however, an insider threat could be devastating if the personnel does not understand it and does not know about security policy how to handle persons without an ID badge; no matter if co-workers or not.

The second pattern is trying to inform about a possible breach to the security team even if the breach occurred because an employee granted access to the floor by employee. This kind of security is better than just doing nothing; however, it is still very poor. Time is essential and during the time which it could take to contact the security and the time which it could take to find an unauthorized person, an adversary could have carries out many malicious activities. There is no time to waste and a better solution to prevent that is not allowing anyone to pass.

The third pattern is like something from a security book. Observing and intervening if noticing a stranger inside of the building or there is something other happening which could be malicious and could be a threat. Every employee’s job is to keep the company and its secrets save. If this kind of security culture and behavior is implemented and trained to personnel, all physical penetration attempts by adversaries or ethical penetration testers results in a failure. This culture will help against all cyber threats and any company could say then that they are much safer.

5.4 Are there trends/common elements between the most clicked simulated phishing emails?

Phishing email is a common trend to deliver a malicious attachment to the victim. What makes it even more dangerous, it could be any email or a sender could even be a co-worker or friend. They affect persons' feelings to make them open those. If phishing emails data is accurate and can be used draw any conclusions, it seems that using phishing emails using curiosity and are related to LinkedIn have the most success rate of all. However, all phishing emails that uses social media have a good success rate. People could have many different social media accounts so using them would be the most effective way to deceive them.

This whole study answers to one other question which is how to infiltrate to the company. Employees are a path to inside. Without a good security behavior, they are vulnerable to attacks and not to mention the inside threat. The outside threat is easier to spot and stop; an insider threat is much harder to prevent. It is much harder to spot the attack and say no if a co-worker is a good friend. Training and culture are de facto processes to stop social engineering attacks.

6 Discussion and future work

When studing this cyber threat area, it took time and plenty of reading to really understand all possible techniques and skills which are social engineers' arsenal. All of them needed to think and plan how they can be used by the author and even for some training.

Social engineering is physiological attack which entirely affects humans' nature and mind to think. Using influence on one of the cases was really hard because it was not ethically right of the author; yet, it was still necessary to do. This showed how hard it could be for the personnel to resist it and how helpful people really are.

Training influences princibles, and building a rapport will help not only with a social engineering penetration assesments but also in a real life. Before reading about these for this study, the author did not really know how effective and valuable these are to know. This study and its results showed the real threat of social engineering;

yet, studying and thinking about the influence and rapport made the author a more social and better person to see another person's feelings and how to react to them.

There are many areas which are not included in this research. Reconnaissance includes only information about the company and not really about its personnel. Searching for information about the personnel in the social media and another media could reveal more attack patterns and maybe reveal something more about the company's policies and infrastructure. The information from Maltego was only for the company and it used only Shodan add-on. Maltego could be used to gather information about the employees as well, and there are many more add-ons even in the free version of Maltego which could be used to get more intelligence and perhaps give more valuable information to the adversary.

Another missing area is social engineering techniques. This study focused only on the physical penetration and tailgating techniques which verified some of the survey's questions. The survey's questions include many more techniques such as baiting and vishing which were not studied at all. Studying them might be very recommendable because vishing and baiting are very easy to implement by adversaries. The risk of getting caught using vishing is minimal because of all prepaid numbers and its stealthy attack. Baiting is useful and most often a very succesful delivery method. This can be tested by the company's own security team by using USB sticks and watching their outputs. All of these missing areas can be studied by the security team or for the auditing assesment or penetration testing if not allready done.

During this research and writing this paper, the author has found a few things that he would do differently. All cases were carried out only from the author's point of view. It would have been better when one case attempt had been succesful and one could have talked with the employee who gave access to the premises to really understand why one did it, did one see that attempt and would one do something differently afterwards. Only that one case attempt (using a fake ID badge) included these steps and information from it was a treasure. This kind of information from all cases would have been better to the company in order to understand the behaviour of the personnel and consentrate more on humans' vulnerabilities thusallowing them to build up a better security culture.

This project and research were beneficial to the author. The research needed plenty of reading and thinking what to do and how to do it. The results and literature gave a better understanding about the people and how we behave. After this study, the author can say that he has grown as a person and thinker. New thoughts come about all subjects occasionally which this study include such as what could be done better or differently to get better results. This research scratches only the surface of a social engineering; however, the author hopes that this helps in some way the assigner company to make the company a safer working place. The author wants to thank the company and its CISO who authorized this research to be done. Without him, this would not be the same as it is now and had probably never been done.

References

Alazri, A. 2015. The awareness of social engineering in information revolution: Techniques and challenges. DOI: 10.1109/ICITST.2015.7412088. Publisher: IEEE. Published in 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST).

Alexander, M. 2016. Methods for Understanding and Reducing Social Engineering Attacks. SANS Institute. Accessed on 31 May 2019. Retrieved from https://www.sans.org/reading-room/whitepapers/engineering/methods-understanding-reducing-social-engineering-attacks-36972

Allen, M. 2006. Social Engineering: A Means To Violate A Computer System. SANS Institute. Accessed on 23 July 2019. Retrieved from https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529

Bhadane, A. & Mane, S. 2019. Detecting lateral spear phishing attacks in organisations. DOI: 10.1049/IET-IFS.2018.5090. Publisher: IEF. Published in IET Information Security (Volume: 13, Issue: 2)

CERT-FI. 2018. #kybersää 11/2018 [*#Cyber Weather 11/2018].* PDF on Viestintävirasto's website [*Finnish Communications Regulatory Authority*]. Accessed on 12 December 2018. Retrieved from https://www.viestintavirasto.fi/attachments/tietoturva/Kybersaa_1811_verkkosivut.pdf

Cialdini, R. 2016. Pre-suasion – A Revolutionary Way to Influence And Persuade. London: Random House Books

Diogenes, Y. & Ozkaya, E. 2018. Cybersecurity – Attack and Defense Strategies. Birmingham: Packt Publishing Ltd.

Dolan, A. 2004. Social Engineering. SANS Institute. Accessed on 23 July 2019. Retrieved from https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-1365

Dou, Z., Khalil, I., Khreishah, A. & Guizani, M. 2017. Systematization of Knowlegdge (SoK): A Systematic Review of Software-Based Web Phishing Detection. DOI: 10.1109/COMST.2017.2752087. Publisher: IEEE. Published in IEEE Communication Surveys &Tutorials (Volume: 19, Issue: 4)

Dreeke, R. 2011. It's not all about "me" – The top ten techniques for building quick rapport with anyone. Publisher: Robin K. Dreeke

Gupta,S., Singhal, A & Kapoor, A. 2016. A literature survey on social engineering attacks: Phishing attacks. DOI: 10.1109/CCAA.2016.7813778. Publisher: IEEE. Published in 2016 International Conference on Computing, Communication and Automation (ICCCA)

Hagnagy, C. 2011. Social Engineering: The Art of Human Hacking. Indianapolis: Wiley Publishing Inc.

Hadnagy, C & Ekman, P. 2014. Unmasking the Social Engineer. Indianapolis: John Wiley & Sons Inc.

Hadnagy, C & Fincher, M. 2015. Phishing Dark Waters: The Offensive and Defensife Sides of Malicious E-mails. Indianapolis: John Wiley & Sons Inc.

Hoxhunt. N.d. Phishing 101: How Phishing Attacks and Scam Emails Work. Accessed on 23 July 2019. Retrived from https://www.hoxhunt.com/blog/phishing-101-how-phishing-attacks-and-scam-emails-work/

Jokinen, J. 2018. Miksi toimittajamme pyrki sisään yrityksiin? [*Why our reporter tried to seek in to the companies?]*. Accessed on 27 January 2019. Retrieved from https://yle.fi/uutiset/3-10318734

Jones, C. 2003. Social Engineering: Understanding and Auditing. SANS Institute. Accessed on 23 July 2019. Retrieved from https://www.sans.org/reading-room/whitepapers/engineering/understanding-auditing-1332

Karppinen, K. 2018. Älä sulje puhelinta, jotain pahaa on tapahtumassa – muun muuassa näin valepoliisit pelottelivat vanhusta, jolta huijasivat noin 60 000 euroa [*Don't hang off the phone because there is something bad happening – among other things fake polices scared the old person who got scammed and lost about 60 000 euros]*. Accessed on 28 January 2019. Retrieved from https://yle.fi/uutiset/3-10518736

Karakasiliotis, A., Furnell, S.M. & Papadaki, A. 2006. Assessing end-user awareness of social engineering and phishing. DOI: 10.4225/75/57A80E47AA0CB. Accessed on 11 January 2019. Retrieved from https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1011&context=isw

Kee, J. 2008. Social Engineering: Manipulating the Source. SANS Institute. Accessed on 23 July 2019. Retrieved from https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-manipulating-source-32914

Khonji, M., Iraqi, Y. & Jones, A. 2013. Phishing Detection: A Literature Survey. DOI: 10.1109/SURV.2013.032213.00009. Publisher: IEEE. Published in IEEE Communication Surveys & Tutorials (Volume 15, Issue: 4)

Macmillan speakers. N.d. Page on macmillan speakers's website and under on Bio in Robin Dreeke. Accessed on 25 September. Retrieved from https://www.macmillanspeakers.com/robindreeke

Manjak, M. 2006. Social Engineering Your Employees to Information Security. SANS Institute. Accessed on 27 July 2019. Retrieved from https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-employees-information-security-1686

Mitnick, K & Simon, W. 2002. The Art of Deception. Indianapolis: Wiley Publishing Inc.

Mitnick, K & Simon, W. 2006. The Art of Intrusion. Indianapolis: Wiley Publishing Inc.

Mitnick, K. & Vamosi, R. 2017. The Art of Invisibility. New York: Little, Brown and Company

Mouton, F., Malan, M., Leenen, L. & Venter H.S. 2014. Social engineering attack framework. DOI: 10.1109/ISSA.2014.6950510. Publisher: IEEE

Mouton, F., Nottingham, A., Leenen, L. & Venter, H.S. 2018. Finite State Machine for the Social Engineering Attack Detection Model: SEADM. DOI: 10.23919/SAIEE.2018.8531953. Publisher: SAIEE. Published in SAIEE Africa Research Journal (Volume: 109, Issue: 2)

Neely, L. 2018. Endpoint Protection and Response: A SANS Survey. Accessed on 10 December 2018. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/endpoint-protection-response-survey-38460

Norvanto, E. 2018. Handbook on Cybersecurity. DOI: 10.2855/3180. Publisher: Ministry of Defence of Austria. Accessed on 23 July 2019. Retrieved from https://publications.europa.eu/en/publication-detail/-/publication/63138617-f133-11e8-9982-01aa75ed71a1

Patil, S & Dhage, S. 2019. A Methodical Overview on Phishing Detection along with an Organized Way to Construct an Anti-Phishing Framework. DOI:10.1109/ICACCS.2019.8728356. Publisher: IEEE. Published in 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)

Peterson, C. 2016. 23 Social Engineering Attacks You Need To Shut Down. Accessed on 23 July 2019. Retrieved from https://www.smartfile.com/blog/social-engineering-attacks/#3

Ponemon Institute LLC. 2019. The 2019 State of Password and Authentication Security Behaviours Report. Accessed on 26 July 2019. Retrieved from https://www.yubico.com/wp-content/uploads/2019/01/Ponemon-Authentication-Report.pdf

Robert Cialdini. N.d. Page on Robert Cialdini's webpage and under on Bio. Accessed on 25 September 2019. Retrieved from https://www.robertcialdinibf.com/

Saunders, M., Lewis, P. & Thornhill, A. P. 2009. Research Methods for Business Students. 5th, ed. Rev. ed. Essex: Pearson.

Shuttleworth, M. 2008. Case Study Research Design. Accessed on 24 May 2019. Retrieved from https://explorable.com/case-study-research-design

Singh, V., Mani, A. & Pentland, A. 2014. Social Persuasion in Online and Physical Networks. DOI: 10.1109/JPROC.2014.2363986. Publisher: IEEE. Published in Proceedings of the IEEE (Volume: 102, Issue: 12)

Social Engineering isn't just for the bad guys. N.d. Page on The security stronhold's website. Accessed on 11 January 2019. Retrieved from https://thesecuritystronghold.com/the-variety-of-social-engineers/

Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E. & Bailey, S. 2016. Users Really Do Plug in USB Driver They Find. Accessed on 29 July 2019. Retrieved from https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/45597.pdf

Trochim, W. 2006. Types of Surveys. Accessed on 24 May 2019. Retrieved from http://www.socialresearchmethods.net/kb/survtype.php

Verizon. 2017. Data Breach Investigations Report. Accessed on 10 December 2018. Retrieved from https://enterprise.verizon.com/resources/reports/2017_dbir.pdf

Verizon. 2018. Data Breach Investigations Report. Accessed on 10 December 2018. Retrieved from http://www.documentwereld.nl/files/2018/Verizon-DBIR_2018-Main_report.pdf

What is social engineering? N.d. Page on KnowBe4's website. Accessed on 11 January 2019. Retrieved from https://www.knowbe4.com/what-is-social-engineering/

What is "Social Engineering"? N.d. Page on enisa's website and under on CSIRTs in Europe. Accessed on 24 July 2019. Retrieved from https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/what-is-social-engineering

Appendices

Appendix 1. Survey questions

1. **Do you use a strong password for work related systems, such as your workstation, to log in?**
   A strong password means a password that contains special characters, capital and lowercase characters, and is at least 8 characters long, preferably longer. It should also be difficult to guess or find out e.g. aK6ZZk89F5!!. A weak password is not cryptic and is easy to guess or find out e.g. November2018.

   - Yes
   - No

2. **Do you use the same password for a variety of services such as Facebook or Instagram?**
   - Yes
   - No

3. **Do you use the same password to log in work related systems, such as workstation, and some personal services e.g. Facebook?**
   - Yes
   - No

4. **You are working on your workstation and the fire alarm goes off. What do you do in that situation?**
   - I immediately leave my workplace and head to the meeting place using the exit, leaving my workstation and workplace to the same state where they were when the alarm started.
   - I lock my machine and then leave calmly via the exit to the meeting place.
   - This is, however, a fire alarm test, so I do not leave. Instead, I continue my work because the deadline approaches.

5. **Do you have or does your computer have any valuable information that might interest a hacker?**
   - I have information, but not in my computer
   - I do not have any valuable information, but my computer has
   - Both me and my workstation have valuable information
   - Neither has any valuable information

6. **Your manager calls you from an unknown number. He is ill at home and his voice is about to go away and you do not know exactly what he says. He immediately needs the team's three most recent meeting reports and**

those should be packaged in one file, encrypted and sent to his private email (firstname.lastname@hotmail.com). The number your supervisor is calling from belongs to a member of the family. He has forgotten the computer and the phone on the previous day at work, cannot pick it up and these reports must go through asap. You can send the password for the compressed file as a text message to that number. What do you do?

- He is my supervisor, so I do this, encrypt data and send the data to e-mail.
- You say "Bye" when he has announced the thoughts and closes the phone.
- You start in different ways to confirm the identity of the caller so you can be sure he is who claims to be before you continue the action

7. **You have plenty of data on the computer that you should save. Network does not work, so you cannot save the data on the network. You need some external media to store your data. You do not have enough large enough media for information. However, you will notice a USB stick on the unused table next to you and you will notice that it so big that all the data will fit to it and there will be still space left. What do you do?**
   - I will not connect it to a computer in any case because I do not know the story of it or whose stick is it.
   - Ask your colleague to try the stick and test its functionality.
   - I use the stick because it is the only way to store the data.
   - I will first supply the stick to the security personnel who can investigate it before being deployed.

8. **You are coming to work, and you will discover an unknown man in a suit with a computer briefcase in hand coming after you to inside smiling and thanking you. What do you do?**
   - He must be personnel. New employee maybe.
   - I stop him and inquire who he is, whether he has a company ID card and what he is doing, etc. I will not let him continue until I confirm the person's right to be in the premises.
   - I'll let him in, but I'll inform this to the company's personnel of security, the security company and other related parties.

9. **You get a call. The caller is from a research institute where a research has been purchased by the company related to the personnel; identify strengths and areas of development and utilize information when designing development activities. The study is carried out on the telephone. A prize is awarded to the recipients. Do you answer the following questions about the research?**

	Yes	No
Job	○	○
Do you have any subordinates?	○	○
Have you completed training / courses?	○	○
How would you improve your work environment / the workspace?	○	○
Personal number ID of company	○	○
Have you noticed any disadvantages in your work environment?	○	○
What kind of facilities the company has and how do you walk there?	○	○

10. **Your friend comes to you. He has problems with the network, and he should be able to retrieve some documents for a review. He has the rights to such documents. He has a USB sticks that can be used to store the documents so he can access them. The stick is found on the top of the cabinet. How do you handle it?**
    - ○ I am helping a friend and copying the documents to the stick.
    - ○ I will not help because I am not really interested right now
    - ○ I do not plug the stick into the computer because I am not sure about its origin, neither my colleague

11. **You are coming to work in the morning. You will find that an unknown person is trying to get inside using his own card; however, the card will not work, and the doors will not open. What do you do?**
    - ○ I will let him in on my own card without any further confirmation
    - ○ I examined one's card quickly and when it seems to be right, I open the door for him.
    - ○ I will examine one's card properly so I can be sure that the card is right, and the person has the rights to pass. After verification I open the door for him.
    - ○ I will examine one's card properly so I can be sure that the card is right, and the person has the rights to pass. However, I ask a person go to see a receptionist where the card rights can be looked at so that the person can go inside.

12. **You get a call. The service desk is calling. Virus software has detected a malicious program on your computer, which may be a ransomware, which, when activated, would crypt all the data on the computer and therefore no access to them anymore. Malware can be removed but it must be done manually by remote access. There is a problem with the Service Desk workstation and there is no normal remote connection, so you should install another remote access software from the Internet, and this not require any rights. He asks to download this to get remote control with the machine and remove this malicious program. What do you do?**
    - There is nothing on my workstation because I have not been anywhere where I could get malware and shut down the phone.
    - I go to the page provided by the service desk and install the software. My workstation has data that is not saved to network and if I lose them then too much important data is lost.
    - I refuse to download this because I do not know which page the address provided by this service desk takes you. I say that I will deliver the workstation immediately to the onsite support for removing a malware.

13. **You receive an email from your co-worker. The headline is "Look at this! Make your day much better!" The email has a Youtube link and additional text that says, "the best laugh this day". What do you do?**
    - I trust my co-worker and open a link.
    - I ignore the message and continue working.
    - I confirm from my colleague that the message has come from him. I open the message after I received confirmation.
    - I report immediately a possible phishing message.

14. **You are going to a cafe in the canteen and you notice a person walking toward you and you cannot see an ID card. What do you do?**
    - I athem going to the cafe. The card is probably just under the pocket or under the shirt and not visible.
    - I say hi and ask where the ID card is.
    - I stay and start talking with him to get know the person better.