jamk.fi

Human behavior from Cyber Security perspective

Tommi Tikkanen

Master's Thesis
June 2017
School of Technology
Master's Degree Programme in Information and Communications Technology
Cyber Security

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Description

Author(s)	Type of publication	Date
Tikkanen, Tommi	Master's thesis	25.06.2017
		Language of publication: English
	Number of pages: 69	Permission for web publication: x

Title of publication
Human behavior from Cyber Security perspective

Degree programme
Master's Degree Programme in Information Technology

Tutor(s)
Kotikoski, Sampo

Assigned by
-

Abstract

The purpose of the thesis was to consider issues affecting human behavior and to assess if they could be better considered in the implementation of security practices. The study focuses on human behavior when an employee faces manipulation.

Why does the employee not follow the instructions he receives, even if they protect him? Are there ways to improve compliance with security policies? Can security practices be implemented differently and what should be considered from the subject matter perspective?

Cyber security is the topic in the thesis. The current security thinking is generally based on how to make the object secure, despite the human. Human activity is always a threat to the security chain. All aspects and actions, where human threats can be decreased, even to a smaller extent, are relevant.

The research method is a case-based research approach. The subject of the research is an invented chain of events, however, it is based on known or commonly used practices.

The thesis discovered that training and ready-made approaches are almost the only effective means of protection against social hacking. The onion security thinking is also an effective way to prevent damage from spreading.

Keywords/tags (subjects)
Cyber security, Social engineering, human behavior

Miscellaneous

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Tikkanen, Tommi	Opinnäytetyö	26.05.2017
		Julkaisun kieli Englanti
	Sivumäärä 69	Verkkojulkaisulupa myönnetty: x

Työn nimi
Human behavior from Cyber Security perspective

Koulutusohjelma
Master's Degree Programme in Information Technology

Työn ohjaaja(t)
Kotikoski, Sampo

Toimeksiantaja(t)
-

Tiivistelmä

Opinnäytetyön tavoitteena oli pohtia ihmisen käyttäytymiseen vaikuttavia asioita sekä arvioida, voisiko niitä huomioida aikaisempaa paremmin tietoturvakäytäntöjen teossa. Työ keskittyy ihmisen käyttäytymiseen silloin, kun hän joutuu manipuloinnin kohteeksi.

Miksi ihminen ei noudata saamiaan ohjeita, vaikka ne suojelisivat häntä itseään? Onko keinoja tehostaa tietoturvaohjeistuksien noudattamista? Voiko tietoturvakäytännöt toteuttaa toisin ja mitä tulisi ottaa huomioon aihepiirin näkökannalta?

Kyberturvallisuus on ajankohtainen aihealue. Nykyinen turvallisuusajattelu lähtee siitä, miten kohde saadaan turvalliseksi ihmisestä huolimatta. Ihmisen toiminta on aina uhka tässä turvallisuusketjussa. Kaikilla näkökulmilla ja toimilla, joilla ihmisen tuomaa uhkaa voidaan saada pienemmäksi, on merkitystä.

Tutkimusmenetelmänä oli tapauspohjainen tutkimusstrategia. Tutkimuksen kohde on keksitty tapahtumaketju, joka kuitenkin perustuu tunnettuihin tai yleisesti käytössä oleviin käytänteisiin.

Tutkimuksessa selvisi, että koulutus ja valmiit toimintamallit ovat lähes ainoita tehokkaita keinoja suojautua sosiaalista hakkerointia vastaan. Kokonaisvaltaisesti käytetty sipulimallinen tietoturva-ajattelu on myös tehokas tapa estää vahinkojen laajeneminen.

Avainsanat (asiasanat)
Kyberturvallisuus, sosiaalinen hakkeri, ihmisen käyttäytyminen

Muut tiedot

CONTENTS

FIGURES

1 INTRODUCTION

1.1 Necessity of thesis

The importance of cyber security is constantly emphasized in the modern society. With complex technical attacks and intrusion, criminals are benefit more and more benefit from the information they receive. Even the smallest data can bring great benefits if the data volume is large enough.

If the risk of loss is only $ 0.05$ per individual, it does not seem too damaging, however, if the company, for example, has a risk of losing 0.05$ per customer, it is already a great amount of money. For example, in the United States, 2015, federal statistics show that 70% of adults have at least one credit card. 2015 In the United States, there were about 248 million adults. One credit card was therefore owned by about 174 million people (Gonzalez-Garcia, 2016), which means that the loss of 0.05$ per card generates losses of 8 700 000$. to the credit institution. This is no longer an insignificant sum.

Criminals generally have access to credit information, personnel registers, business secrets, password lists, virtual money, and account information. Most of the stolen information can be sold forward, even more than once. Some of the stolen information can be used to blackmail and sell stolen information to the victim himself. As an example, the home hard disk drive is encrypted and the encryption key is sold back to the victim.

Headlines usually occur where user identifications and credit card information are hacked by breaking into systems. Identities of an individual user are also stolen and used. There are less headlines of cases where the hacker has physically infiltrated the information or has accessed sensitive systems either through the company or its employee through infiltration. This is called social engineering. Investigations by Agari result in the fact that 60% of enterprises were victims of social engineering attacks in 2016. (Perez 2016)

Usually, social engineering is a part of a criminal toolbox that can be used to achieve the desired goal. However, it should be remembered that a human has always been and will always be the weakest link in the security sector and therefore also an attractive destination.

In general, social engineering is too uncertain as a way to work in a modern world where employees are more aware and much more suspicious and educated than the older generations; however, people are at their most vulnerable when they think that they are somehow out of danger. Employees can imagine that they cannot be fooled because they know how to be on guard. It is this kind of omission of self-superiority that is dangerous and stupid. All people can be cheated and all people can be manipulated. Contemporary behavior is influenced by the same basic activities as in the previous generations. If that were not the case, no ads would be made, politicians should not speak and psychologists and psychiatrists would be unemployed.

Social engineering is not just an influence or a joke for doing tricks, for example, to make a victim to get a hacker into a locked server without an ID card. The concept of social engineering itself includes a variety of tools and ways of achieving different goals. The purpose of social engineering can be to get background information or to create some degree of familiarity. By doing this, social engineering can achieve the set goals. It may also be more multilevel. First, for example, the hackers acquire information about the subject of a company's employee, after which the information spells can be utilized in surprising situations. For more details, the reader is adviced to see Chapters 4 and 5.

The goal of social engineering can also be to persuade someone to do something they would not normally do. This does not mean a whirlwind magic that enchants the victim to release an unknown bank vault. This means mainly the company's every day actions, and some people think it is useless violation

of rules, which helps to help someone who is in distress. Chapters 3 and 5 contain more detailed information on this subject.

Social engineering also includes, on a larger scale, the editing of people's opinions. This is usually done by advertisements but also by the state and the media. This type of social engineering does not target a single person or a group of employees but targets a group of people, a nation, or certain target customers. Against this type of Social engineering, it was and is difficult to protect oneself both in the old days and in the modern society, e.g. media activities are a good example. If a person is not on the spot, then what can be certain is that the image from the news, such as a demonstration, is real. In addition, it is generally not possible to get the item as multiplied and generally tell what is most newsworthy.

This was illustrated, in the writer’s opinion, by the best-known Swedish doctor, Hans Rosling, in a TV interview where the theme of the media was an image of reality (Danish 2015). He suggested that an interviewer and only a bust should be shown, even though the feet with fine shoes could be shown. This, however, would not be as interesting to look at, so media show only the most interesting side of the person. This is done with the news or the matters presented by any media. Only media sexy issues are important to show.

Differences in experience between the media and the ordinary citizen can be considered in another way. Even if human beings were at the center of events that the media reports on, they may have a different experience of the situation than the journalist. On the other hand, it is difficult for a journalist to be impartial in the situation. Who is right and who is wrong? Is it the intention of news coverage to directly affect people's opinions? In any case, it is indisputable that social engineering, i.e. affecting people’s thinking or behavior, is commonly used throughout society for various purposes.

Types of human influence can be divided into different ways. Throughout the history of mankind, another person may have tensed other people in one way

or another to make his or her goal fulfilled, e.g. when a clamping tool has been food or drink, when the life of own or one's of relative is affected. Nowadays, the cryptography of files on a home computer can be used. This activity could be described as a direct or immediate influence. In this style of influence, it is certainly not unclear to the victim what the hackers have in their mind and what their tools to achieve their goals are. This style is not a disguised activity. It is not even good to try to hide at least the victim because otherwise there is a risk that the victim will not know what is expected of him and thus, for example, the payment of the ransom is delayed.

Another type of influence could be described as an indirect effect. This has also occurred throughout human history. The purpose is to get people to do the desired things, however, to influence their behavior so that the subjects make their own choice. Such activities include scams, spamming, leadership, or even shoplifting. Studying human behavior and understanding the motives has brought a whole host of more sophisticated ways to influence someone, though of course all the ways have been used. Now, there is no need to possess inherent gifts to guide people but it can be learned, although socially one cannot be very cumbersome or the methods do not work.

This tactful way is used consciously in favor about mass media, politicians and leaders, or even in job interviews. Not a single advertiser threatens the consumers that if they do not buy this vacuum cleaner, they and their relatives must be cautious. Or, that if the consumer does not buy weight loss pills, the advertiser will make him even fatter. Manipulations are made to make the consumer think that he or she chooses to make their own choices. Likewise, politicians are trying to influence people so that they themselves will begin to want support from a candidate. If a human being is forced to support a leader, then this coercion would also bring unpleasant feelings about it.

One can think that if more sophisticated ways of affecting people are known to everyone, then why is the protection not easy? Since this is about human

behavior, there is never a 100% chance of protection unless people stop human behavior altogether.

Protecting, however, helps people to identify some approaches or behaviors and to be skeptical of, for example, exceptional events in the workplace. The subject's learning thus has an inverse purpose to affect the human behavior. In practice, a person who works with other people cannot be suspicious of other people full time.

As can be seen from the previous text, the subject is truly multi-dimensional and challenging; however, why then not think if it is impossible to fully protect yourself against social engineering? Why would it be worth sacrificing time for this style of reflection? Why should one know about basic human behavior when talking about security?

The author is convinced that some of the technical experts should know at some level about human behaviors and their underlying causes. This does not mean that technical experts should become professionals of psychotherapy to understand human behavior. However, it is good to know the basics to figure out what basic means there are to influence human behavior and how effective they are. This should be a good idea for all people, however, above all, technical experts.

The author is convinced that the fight against social engineering has enabled the same idea of the model as the current cyber security thinking has. First, it must be accepted that the fight cannot be overwhelming. After the adoption of this idea, one can begin to solve the possibilities of combating the onion pattern in different layers, which means multi-level protection measures. It does not matter, even if the outermost defensive layers get socially hacked. This opportunity has been considered in the inner parts of the fight and so on. It can thus be assumed that the outer layer can always break, however, a more complex and multi-layered protection style can prevent a damage and even prevent a targeted attack in advance.

How can this onion model be practically implemented in the fight against social engineering? The purpose of this work is to reflect on the background and present some concrete examples of implementations.

1.2 Research objectives and methodology

The purpose of the thesis is to consider the causes of human behavior and to assess whether they can be better considered in the implementation of security practices. The thesis focuses on human behavior and social engineering. The study focuses on how protection is possible against social engineering. In addition, the thesis describes how to utilize the onion type cyber security concept in the case presented.

Why does an employee not follow the instructions he/she receives, even if they protect themselves? Are there ways to improve compliance with security policies? Cyber security is a topical subject today. The current security thinking is about how to remain technically safe. However, human activity is always a threat to this security chain. With all the perspectives and actions that this human being threatens to decrease, it is important.

The research method is a case-based research strategy, and the research focuses on invented examples that could nevertheless be realized. Based on these case studies, the thesis first attempts to verify both the victim's and the author's styles and possible causes and benefits for action. After that, the thesis tries to create, as far as possible, a vision of how the effects of such situations could be protected.

1.3 Framework

As the subject of research is an imaginary series of events, the situations and venues are completely imaginary. However, the reality on the ground to maintain the research, the tools are used as a basis for events at some

existing operating models and technical specifications. Information was gathered from various sources of information, so that a series of possible events could be imagined. As a part of this thesis, the used examples of the operations available have been experienced by the writer, the sources of the sample event chains cannot be listed as sources due to confidentiality issues.

The research project is a fictitious AA Company, which has hundreds of people around the world on its payroll. The main business areas are design and development work, mainly for the automation industry. A social engineer has been given a job to find out what development AA Company is doing to a BB Company or who is an employee in AA Company.

At the same time, if possible, the purpose of the social engineer is to get control over the software of one of the AA Company's devices or servers. For example, what a hacker subscriber can do with the information is the recruitment of key personnel that slows down the delivery of AA Company’s products to BB Company, the first-hand knowledge about the development work done by BB Company, as well as the continuation of enterprise espionage by getting a spyware application into the AA company's systems.

The social engineer’s basic information before the actual activity is limited to the internet data obtained from AA Company and BB Company as well as the mapping of both personnel in social media and other sources, so that approximately 10% of the employees working at different levels are known in each company. At least the name, country and address, how long the firm has been at work and where are known. In addition, know-how, hobbies, contacts, subsidiary functions, telephone numbers and positions of trust are known to the staff. Potentially, some of the employees' financial difficulties, the loss of their relatives or even divorce have been identified through social media updates.

1.4 Thesis structure

The research discusses an imaginary series of events that focus on how a social engineer takes advantage of human behavior to get what he/she wants. At various points in the event series different ways how social engineering can be successful are discussed. However, the intention is that, in fictitious events, a social engineer can progress to his or her goal. At the same time, the event can be considered: Could the event have been possible to prevent or could the the realization of that event be hampered?

This first chapter describes the background of the research and the way it is implemented. In addition, the boundary conditions of the imaginary event and the objectives of the social engineering are described. The next part focuses on what is meant by the term social engineering. What a social engineer should generally be aware of and what kind of every day information can be gathered.

The third chapter covers the most common social tools that social engineers take advantage of. They enable social engineers to interpret their subject and act as needed. The fourth part deals with how a social engineer can collect information. In addition, the fourth section deals with how the collected information can be utilized to allow a social engineer to create a first contact with a target company. The fourth chapter also discusses what situations can be protected, and whether onion security thinking might be useful for situations in a section.

Chapter 5 addresses two example cases in different situations where the social engineering is a possible action. The irst case is the author’s own experience: it is an example how it is possible to make use of an everyday situation. The second case is a fictitious situation where the social engineer designs and implements social engineering attacks and where goal of social engineering has yet to be achieved. That means getting information on the target company and accessing and contaminating the target computer or other

devices. The chapter also focuses further on the fight against social engineering through onion type security thinking to prevent such events.

Chapter 6 summarizes the events and contemplates if the goals set for the research were achieved. There is also discussion if the research could give some new perspectives for a new research topic.

2 SOCIAL ENGINEERING

2.1 Overview of backgrounds and behaviors of social engineers

Social engineering is not a humbug temptation where a victim can be made to obey when, for example, in hypnosis, he/she has to obey all the commands given to him/her. The target is not a stupid or unskilled person. The victim can be any person, even the social engineer her-/himself.

The goal of social engineering is to build structures of small crumbs of information when while getting additional tools to deepen the social engineering actions. It resembles slightly making puzzles where the putting pieces together will be easier as more pieces are gathered. Social engineering uses already-known facts to create some degree of trust on the current site, which will attempt to get the target to reveal some new information. Smaller information is usually useful. The same small information crumb spells are continued every day.

When a neighbor tells, he/she will be traveling overseas the next week or at a bus stop waiting for a poor sleeping night because two of her own kids are sick. Information can be collected even from other people's shopping carts. What other people buy can help to draw conclusions?

For example, if a man buys small baby diapers, it is presumed that he has a baby at home, or when a man buys women's knickers and does not have a ring to indicate his marital status. In that case, one can assume that he is in a constant and stable relationship with the fact that he buys her knickers.

More discreet information can be obtained from shopping carts, for example, by combining the materials purchased; one can conclude, for example, that a person will make Italian food in the next few days or that he/she likes strawberry ice cream. Of course, one can wonder what the benefit of this type of information is.

It is good to remember that people try to identify their environment because it creates a sense of security and is a part of survival. If a social engineer can approach a subject through something familiar, the object is much more open to social engineering because he/she knows how to identify the situation presented by a hacker.

For example, those who have had neonatal babies know how it feels to control the nights because of the baby. In this case, everyone feels sympathy for this because it is easy to identify an emotion. However, if someone complains about fatigue because he/she has played computer games all night, he does not necessarily feel bonding in the same way. Using this information, a social engineer will be more easily able to deepen the conversation if he/she mentions having experienced the same things or knowing about the same things as the target person likes. Even the discomforts experienced by the target person can produce a similar reaction.

Social engineering is, in some cases, very difficult. Generally, social engineers are socially gifted and it comes the easiest for them, since they can use it even consciously. Some things can be learned from books, some should be practiced in real social situations, and some of the special abilities must have a personal tendency to succeed. (Conheady, 2014 53 -54)

A person usually learns most of the social skills and behaviors as a child, for example identifying the residential environment, for example, to interpret the facial expressions or speech rhythms of parents and others, and ways to pronounce words. Also, gesture language is usually learned from the residential environment. (Conheady, 2014 54-55)

Humans have the tendency to identify themselves with the surrounding environment and people. A child has no other option to learn behavioral and social skills than other close people. Children have no innate social skills. However, the child learns different skills very quickly, e.g. facial identification, importance of sound, recognition of speech rhythms, etc. These, especially in the early days of mankind, have made it easier for the child to cope from childhood to adulthood. (Conheady, 2014 54-55)

Thus, people naturally strive to adapt to the surrounding environment as children. This is also repeated at older age. Many people behave differently in different situations. Because of this, many people have so-called work roles and home roles. It may be that one has learned to behave differently with different people, for example, parents or friends.

Different situations also create different needs, e.g. hobbies compared to work environment. In this case, people have learned to behave in the workplace according to the working environment that is correctly and fairly speaking, standard literary language.

If people of the same style are engaged in hobbies, the use of language, for example, can be coarse and not as correct as in the workplace, or when traveling to a completely different city, the locally-learned behavioral pattern may change according to what has been learned earlier.

The author is a good example of how behavior can change depending on the environment and people since he comes from Finland, North Savo. There is a Savo dialect typical of the region, where the sounds are stretched and edited

in a form other than the literary language. In addition, words are pronounced broadly. The author has lived in South Savo, just 200km away from his birthplace. In this living environment, hearing similar talk is fairly rare. The author has also studied in a city where the birthplace dialect is not spoken at all. All this has resulted in the fact that he usually speaks almost literary language. However, when he travels to his birthplace, the speech changes instantly.

The author has not noticed this behavior himself, however, his acquaintances have mentioned this. So, without knowing, the author changes his speech style according to the current environment. So, he tries to adapt to the environment as well as possible. Thus, it can be thought that people adapt to the environment in a way they have already learned if the behavioral model is already taught. Thus, people do not learn to adapt to their familiar environment by observing but have a certain learned pattern which is primarily intended to benefit them.

This primary use of the learned model can also be seen among migrants, especially those who travel back to their native country after many decades. In the new home country, new learned behaviors have been acquired. However, when they return, the patterns and speech patterns that have long been learned will come back.

For example, people who have moved from Finland to other parts of the world use old manners and speech styles as local people of the same age when returning to Finland. This shows in some respects that people also save their intellectual resources without knowing this. They first try to adapt to the familiar environment before using the learned approaches.

The author believes that there are also many behaviors that can be learned from books or by training. Actors learn the different forms of expression and the behavior they use for their work. They are therefore not taught this as a child or under the pressure of their own living environment but in general,

these patters of expression and behaviour are deliberately taught and practiced. Actors tend to focus on some key elements that can be used to create a behavioral nature. A good example is talking with a foreign accent or acting as some expert. In addition, learning a new language, for example, is usually knowledge-intensive learning and not environmental pressure learning.

For social engineering to succeed, the hacker needs to manage his behavior as well as possible. The above considerations are a good idea for a social engineers to become aware of themselves and to develop different conscious appearance styles.

However, the most important skill for a social engineer is the ability to listen to others using active listening. People generally speak openly about their own affairs if they are given the opportunity. This is especially the case if he or she is aware that the other party is genuinely interested in his / her affair.

There is a great amount of personal experiences. The author has previously worked in a very basic workstation helpdesk job. In this case, the remote connections were not as good as today, so repairs had to be carried out on the spot. In addition, the work involved replacing computers and was usually done during normal working hours. In this case, the user often waited in the same room as the machine to be replaced. Often the small talk level of chatting ended up with the fact that the employees started talking about their own concerns or family events very openly, even if the author had never met this person before.

The author is by nature caring, thus, he was also genuinely interested in the employee's experience of their workstation and their electronic services. He assumed that genuine interest in the needs of an employee made it possible for them to speak openly about other concerns, which never bothered him as the thought it is natural that someone else should talk about their own affairs, even to an unknown person. This, however, is an interesting observation he

only understood when he started thinking about my own experiences in the subject area.

A conscious presentation of an interested person does not usually work because another person Instinct it. The other person gets a feeling that makes him uncomfortable. This is a good example of a salesman who has learned a certain style approach when visiting a customer. First of course, his are of course interested in how the general goes and how the day has gone. If a salesman is not genuinely interested in customers as people, it is easy to instill this time.

It is sad to see how some old salesmen are trying to be friendly to their customers. They may feel that they are not really interested in what the customer feels. For example, how has the day gone by or what a customer has experienced last week while visiting abroad. In that case, the conversation ends soon enough or changes to show small talk conversation. Human is very good at interpreting other people's microwaves and body language. I would combine emotional expression or atmosphere with these concepts of interpretation. These interpretations will be further deepened later.

However, the most important thing is that Social engineering requires to be able to succeed. You should be present just in the moment and have fully identified your role. Conscious presentation generally reduces the chances of success. Thus, the roles that occur in different places and situations should be chosen so that they have something of their own. Generally, social engineering consciously targeted and made is not entirely self-made. If you do not use a role to play, it is difficult to adapt to different social situations and achieve your goal. Presenting a role is like pure paper, which can create behavioral patterns and behavioral styles that differ from your individual learned habits.

2.2 First steps of social engineers to reach their goals

The author's opinion is that a social engineer must be purposeful and systematic. As a result, he or she should handle the situation as a project. The projects set objectives and schedules with boundaries; there is also planned progress of the project and the methods. The most important thing is, however, a conclusion on risk assessment. As in any whatever project, the hacker will have to investigate social risk situations and avoid them.

The first real task is to plan how and where to carry out each target. One of the most important issues is to select the item or items, in which they use their skills. It is easier to approach the task if the site has some similarity with the attacker. A 30-year-old hacker cannot proceed directly onto the discussion subject if the subject is a middle-aged woman. It would be hard to find anything that would suit both approached topics in a real life situation.

If the target is of a different age, different sex or with ethnic back-grounds different from the hacker, the hacker will have to do more work in terms of backgrounds. However, one can always find an appropriate subject or a situation that can be utilized. However, identifying with the same is easier if the target is of the same age or in some respects similar. In this case, the social engineer cannot start an easy conversation about child care, a mid-life crisis or even a parachute jump.

It is also important to know the object's routine activities in order to find suitable approach topics. Does the target drink coffee in the mornings before going to the workplace? Does he/she have a regular place where he/she has lunch or where does he/she go shopping? Does the target person go jogging or go for some hobby? Knowledge of the object's routines therefore primarily refers to the object to follow, however, the author's experience is that today even social media can provide plenty of information about the routines of a person's life.

The following discussion is an example in which a hacker uses the knowledge gained for his/her benefit about the target person's life situation. The persons are at the target person’s favourite place to hangout, a local coffee shop where he/she often drinks coffee in the morning. This situation illustrates how naturally the social engineer can get information quickly by phishing. The target called Bill sits alone at the table, and a social engineer who calls himself Harry enters the scene with a coffee mug.

Harry: Excuse me, is this seat here free?

Bill: Yes, it is, just sit down, please.

Harry: The coffee is good here. I need this after a sleepless night. Our little John was awake throughout the night.

Bill: I know; we also have a child that kept us awake the other night. Yes, coffee is needed a lot during these days.

Harry: It seems that our child is teething, her first teeth, you know. These are tiring times, just when I should visit own company customer’s with a salesman and give the technical expert backup. I work as a technical expert for VV company and we have a new app.

Bill: Interestingly, we're in the same field.

Harry: Which company do you work for? Can we introduce you our new app, for example next week?

Bill: I work for XX company. I do not directly know if we can use your application, but I can give you my business card, so please contact me by e-mail. We start our holidays with the family next week but contact my after that, please.

The hacker should remember in a situation such as the last discussion that one is interacting with another person. Generally, when the other person gives information about something, the other party will also provide the same kind of information as seen in the proceedings in the above conversation, and Bill left the conversation in a natural way. This is because he was able to identify himself with the situation. It can also be noticed in the discussion that the

conversation topic can change rapidly. This requires that the hacker comes with a complete role of his life background and the role has been pre-thought. It must be remembered that people always want to adapt to their environment and search for similarities that are inherent in other people. (Handnagy 2011, 219 -221)

It is case-dependent how deeply the backgrounds should be studied. The previous discussion can be entered by knowing the object's employer and industry, as well as what age the target person's children are. Further information is therefore needed, so that a social engineer is able to make contact with the employees in the firm. The contact is not very strong. However, hackers have now the target person's business card, contact information and the information that the employee in question is on holiday the following week.

Preparing a role is important because a social engineer creates a new identity for himself. The more personal level the social engineer is going to discuss, the wider role of the background he/she needs to have. For example, prior to the above example of the hacker's discussion was good because he/she came up with the role of family background and life situation. In addition, he/she must have invented for a work situation and an employer. It is possible that the target checks the background of the social engineer by sending an email, or if he gives fictitious business cards.

These situations of social engineering must be prepared for in advance. Alarm bells start ringing immediately if he/she finds out that the social engineer's company seems not to exist at all. In addition, if a social engineer sends an email, for example @gmail.com address and he has appeared in the role of a big company's employee. Then the trust will be gone soon, and the social engineer has failed in the mission.

A small start-up company, only a few people working; to create the company web site is not a problem at all. A social engineer can come up with a

company background and publish pages in any web property. The social engineer's domain can be registered even without a real company. However, at least in Finland, it is impossible to get the company registration number without the right information. If a social engineer wants to leave traces of themselves as little as possible, he/she can use someone else's, e.g. just a small firm's registration number. In this case, the contradictions can be explained by the fact that there is an alias name or the name of the company is just getting detached from the original company.

E-mail it is easy to fake by using the domain name of the web pages. The domain ID must be correct and sound as formal as possible. For example, firmac.org does not sound quite as reliable as firmac.com. Business cards usually contain a phone number. It is good to have an active number, so the only option is to use a prepaid subscription. If a social engineer has a number of different roles or target cases and has created different contexts to a firm's business card, they should each have their own numbers. Thus, the roles and the companies should be mixed up. (Conheady, 2014, 4)

3 DIFFERENT TOOLS IN SOCIAL ENGINEERING

3.1 Starting with social engineering

Social engineers have a wide range of tools and knowledge to help them to achieve their destination. Knowing the human mind and behavior patterns helps the social engineer to develop their own skills. Some of the skills and knowledge helps them to facilitate the analysis of human behavior. In addition, pieces of information can be combined to achieve the desired result.

In general, the information material used by a social engineer is socially based on behavioral and psychological evidence. The same data is used by psychologists and psychiatrists who use the method for the treatment of patients. In fact, every human being is sometimes used consciously but more

often unconsciously to provide such information. One knows how to interpret whether some person is happy or irritated. The file is interpreted without having to constantly adapt oneself and other people on the basis of its own interpretation service. A social engineer must become aware of this ongoing analysis and know how to exploit their knowledge of the unconscious consciously. (Hadnagy 2011, 31, 33-34)

However, the hardest part for social engineers is to learn how to use the available information for their benefit. The social engineers should know how to consciously use their talent, however, as smoothly as in normal situations. Some of this skills are learned in the school of life lessons while some social engineers have only their natural abilities to manage social situations perfectly. Information on the subject can be studied, however, a book is something else to learn about and social engineers try to implement their roles rather through conscious changes than without much learning.

The author opinion is that even if a social engineer’s social skills were natural, it would be good to know his/her reasons why the social tricks they use work. This may also provide new ways to use their own skills and to deepen their knowledge. An understanding of the mechanisms can produce a new "aha moment" experience that will bring completely new approaches to their current approach and influence the behavior of objects.

The understanding also provides expertise to a security trainer and in general, to normal people as well. It cannot be assumed that every employee has an insatiable thirst for knowledge and behavioral patterns and psychology. Fortunately, for example customer service training usually go through job security and training at some level. The author’s opinion is that it is important that people are given the opportunity to understand how each person can be fooled and manipulated. There is always someone in training, and he/she will begin to see this issue a little differently. The question if this is benefitial depends on the situation. However, there is even a remote possibility that the person no longer just continues to go to the easiest "lever", because he/she

could identify some new avenues with the education examples of social engineering.

3.2 Elicitation

Elicitation means that the discussion is guided using one's own sentences and questions. It is a certain kind of behavior stimulation, in which the conversation partner is shown considerable logical conclusions and questions which the target will answer by continuing the phrases, or behaving in a certain presumption accordingly. The aim is to lead the discussion so that the subject wants to actually answer the questions presented to him. (Handagy, Ekman 2014, 30) The technology is very discreet and risk-free to use. In general, the target does not even understand to divest some important information, because he/she wants to be informed. If someone has a too rough questions, the person using the technique can be described as rude or just too interested in other persons' matters.

Elicitation power is based on several basic aspects of human behavior. The following is a list of reasons that the elicitation activity is mainly based on (Hadnagy 2011, 87):

- *Most people have the desire to be polite, especially to strangers.*
- *Professionals want to appear well informed and intelligent.*
- *If you are praised, you will often talk more and divulge more.*
- *Most people would not lie for the sake of lying.*
- *Most people respond kindly to people who appear concerned about them.*

As can be seen from the list, the list includes a guideline for good manners which is usually taught to children. Be polite, do not lie to people and treat others as one would like to be treated. The author thinks that most people want to be accepted also in terms of their talents or the information they have, or using some other instrument. If the other person is praised, his/her current

business model can be strengthened. This is probably due to the fact that a person feels a part of this group, when he/she was taken into consideration. In fact, all the items on the list regard their guidance of human behavior, so that he/she were better accepted as a part of "the group". Although these behaviors are taught to children there is a wide range of behavior patterns learned in the child's environment.

3.3 Pretext

Pretext is about acting and taking the role. Previous chapters have drawn attention to how important it is to take over the role. The more natural a social engineer feels in their role, the more likely the target interprets the gestures and facial expressions to be correct. This is because it is easier for the human to embrace the role that corresponds to oneself at least to some extent. Another option is to get depth to the role from one’s own empirical experiences. (Handagy, Ekman 2014, 29 -30)

Pretext is not only about acting a role. It is also a way of speaking, as well as the sound priorities, clothing, manners and movement / gesturing. The more long-term the situation of social engineer’s phishing data at a time is, the more carefully he/she must know how to prepare and submit to embrace the role. It could be said that in the building where the people are wearing worn overalls, the builder cannot wear shiny leather shoes and a Rolex watch on his wrist. Also, his / her hands cannot look like the person never worked with a spade. The social engineer has therefore to choose a role, which is actually viable and credible. (Handagy, Ekman 2014, 29-30)

The author’s opinion is that many actors and comedians get into the role so well that when they put the role on wearing a dress or mask or a straight face, they are already within the role. This is perfect since the role of adoption is a skill that can be aspired towards, however, it is learned only with continuous practice and repetitions. This is also called the identification with the role.

The author’s opinion is that for a social engineer it is easier to use roles that are already used elsewhere. Thus, the adoption of a role is easier, and the adoption of a new role takes time. Sure, if necessary, the role of backgrounds, clothing and way of speaking according to the background and the rhythm of speech are necessary to embrace. Social engineers can of course also customize their case by case basis depending on the environment.

3.4 Persuation and manipulation

Persuasion skill is a very useful social tool for the hacker. Persuasion is not about forcing the object to so something he/she does not actually want to do. In this context, social engineer's power of persuasion means mainly appealing to the goodwill of a human or their willingness to help. It is therefore closely linked to the lead-in into the conversation. However, persuasion is different because a proposal or hint is made to achieve the wanted action. Everyone uses persuasion skills surely every single day.

For example, a co-worker asks another if he/she can take over a project because the person him-/herself has so much to do between projects and should taks the child to his/her hobbies in the evening. The persuader would let the other person even choose their vacation timepoint during the holiday season if they now just would agree to take over the project.

Another example could be a situation in which a woman asks her husband to visit the store, so that he could make a man's delicacy. The woman even says that she is too lazy to go because she has had a long day with some main contract concerns.

These examples are rough, however, they reflect well what persuasion is all about. It is not coercion; rather, it is justified by the fact why the object should implement the request and, if necessary, the target should also commission done the service. (Hadnagy 2011, 237)

On many occasions, manipulation can be mixed with persuasion. However, they have a clear distinction. While persuasion aims at appealing to a target's emotions and presents a clear request, manipulation aims at redesigning the other person's perceptions about something. The purpose of manipulation is to keep the person under control. (Hadnagy, Ekman 2014, 32 - 33)

There are very nasty examples in the media, when someone in a family has managed the entourage of manipulation and practices choreographing the lives of others. Narcissistic people use manipulation, so that they could use other people in whatever way they favor. The following quote is in accordance with Handagyn's (2011, 293-294) six different ways to manipulate people if the manipulation does not need to be hidden or is reaching extremes.

> ***Increasing the suggestibility of your target.*** *At its most extreme, sleep or food deprivation increases a target's suggestibility. On the lighter side, subtle hints that build in intensity over time to make your target more suggestible.*
> ***Gaining control over the target's environment.*** *This technique can involve everything from controlling the type and quantity of information to which a target has access to much subtler things like gaining access to a target's social media websites. In a social engineering context, having access to social media allows you to view your target's communications as well as exert control over the information he receives.*
> ***Creating doubt.*** *Destabilizing and undermining your target's belief system can go a long way toward manipulating your target to take an action you want. From a social engineering viewpoint, this must be done subtly. You can't just barge in and start degrading your target; instead, questioning the rules they follow, their job, or their beliefs can affect the target's ability to make rational decisions.*
> ***Creating a sense of powerlessness.*** *This truly malicious technique is used in wartime interrogations to make a target feel a lack of confidence in their convictions. A social engineer can utilize this tactic*

by taking away the target's agency by presenting the "facts" you received from someone with authority, thus creating a powerless feeling.

Creating strong emotional responses in the target. *Strong emotional responses include everything from doubt to guilt to humiliation and more. If the feelings are intense enough, they can cause the target to alter their whole belief system. A social engineer must be careful not to create damaging negative emotions, but using tactics that create an emotional response based on fear of loss or punishment can prove beneficial to your SE goal.*

Heavy intimidation. *Fear of physical pain or other dire circumstances can be used to make a target crack under pressure. Again, most social engineers will not go this route unless they are using corporate espionage as a tactic, but in normal social engineering, this tactic utilizes perceived authority to build strong fear and feelings of potential loss.*

Often, manipulation is not systematic and transparent like the above-mentioned points. Manipulation takes place in everyday life continuously. Good-natured kind of manipulation can be considered, for example, when the man on the street sees that his friend and calls him by name. The guy may turn his head and say something instinctively. Again, this is a manipulation, that is, a person is made to act in the desired manner. (Handagyn 2011, 293-294)

3.5 Mind tricks

Each person assumes opportunities set by their own choices according to their own mind. The author opinion that each one controls miscellaneous desires, preferences and external pressures to behave in a certain way. External influence on human influences is currently very high. The mind is constantly entered by mental images and desires, and behaviors without that people will even realize it. Each one has come across a test in which the

attempt is to deceive people with different looking things. The simplest example is the endless ladder, which causes a 2D plane illusion that the square of the stairs circulates endlessly. More complex tests can be found on the Internet just by searching with words "mind tricks".

On the Internet, one can also find many examples where the targets are affected in some way. For example, during a conversation, a particular word or topic is repeated and then the person is prompted to draw something on paper. The subject will in these cases draw an object or something is used to refer to the object of the manipulation. (The Late Late Show with James Corden)

A common nominator in these cases is that this is not a conjuring trick. In those using the human tendency to use logical reasoning is utilized. In addition, these cases are used for the benefit of humans' adaptation to their environment. Logical reasoning skills are usually used in the style the endless stairs play tricks with the human mind. This is close to magic tricks, which usually rely on just the human ability to logically deduce, for example, the size of the magic box, the location of the ball or even the fact that the magic bag is empty, when shown to the public. However, the magic box has something hidden in it, the ball is moved to another location with manual dexterity or the lining of magic bag contains scarves. The author opinion that these are all based on a certain way to cheat and hide.

A mind trick is in the author's opinion based on a certain kind of forced entry knowledge to influence the decision. Logical reasoning may be utilized in order to have a stronger effect. If a person sees an advertising sign on the street marked with the text "1 + 1 =" he/she can be pretty sure that at the next street corner if one is asked to name a figure between 1-10 the most common answer is number two.

This is due to the fact that our minds will subconsciously decline the task. In this case, the task and especially the mission is captured in response to the

so-called human working memory. This memory part of the working memory is called the short-term memory. In computer terms, it is conceivable that the working memory is computer memory and human long-term memory is a computer in terms of storage. Working memory is constantly exploited. The author's experience is that the oncoming color of the car might not be remembered for some time. If the information is not really relevant, it will disappear from the working memory.

The author's opinion is that mind tricks can also be utilized, e.g. some general information about the temporal example with reference to the religion, the sun, precipitation or mathematics then as already described in the example.

3.6 Microexpressions and hand gestures

Humans are very good at interpreting facial expressions. These micro expressions are made by the small muscles of the face and a person is unaware of them. The most familiar phenomenon is a checkout with a female employee smiling at one when shopping. For some reason the checkout person's smile does not feel genuine. The reason are the micro facial expressions.

People can smile without being really happy, however, this artificial smile often is interpreted correctly. If you are genuinely smiling with joy, it shows clearly. Some say that a smile makes human eyes smile or shine. This is due precisely to the fact that in a true smile, for example, the eye muscles of the micro muscles are working.

Dr. Paul Ekman (Handagy 2011, 149) is a long-time researcher who has studied micro facial expressions for more than 40 years. Although micro facial expressions seem self-evident as such, the mechanism must be known and mastered in order to be able to analyze or present truthful feelings.

Based on research, universal emotions interpreted in a similar way all over the world are as follows (Hadnagy, Ekman 2014,108-135):

- *Anger*
- *Contempt*
- *Disgust*
- *Fear*
- *Happiness*
- *Sadness*
- *Surprise*

People also communicate with their hands consciously, however, often also unconsciously. The human finger may deliberately indicate items, which means talking or showing the outline of an object by moving their hands. There is also the indication of small quantities of items that may be expressed universally using fingers. (Hadnagy, Ekman 2014, 58 - 61)

Humans can unconsciuously communicate the state of their mind with hand and finger movements as well as with different positions of. People can also unconsciously interpret a variety of hand gestures almost as well as facial micro-expressions. For a social engineer, it is important to be aware of the basics of different hand gestures, so that he/she can use them for his/her benefit. It is also important to interpret the object's hand gestures. (Hadnagy, Ekman 2014, 58 - 61)

If a social engineer tries to speak calmly and convincingly, hand movements can make the target person doubt the situation. The suspicion is due to the fact that the subject is receiving mixed signals. Generally, in this case social engineering fails. In order to use hand gestures to support the entirety of expression it is useful for the social engineer to be aware of the movements of the hands and manage them. With the help of a few examples, the social engineer can learn how to gesticulate with his/her hand if he/she really wants

the conversation partner to believe what he/she is trying to communicate to him/her. (Hadnagy, Ekman 2014, 58 - 61)

The author's experience is that generally in meetings there is at least one person who must tap with fountain pens on the table or otherwise produce a rhythmic sound. This usually gives the feeling that the person is nervous, impatient or bored.

When hands are crossed on the chest it usually means that the person is aware of their own opinions, or otherwise prepared to defend their respective positions. The position can be described as defensive or in a way, the person is hugging him-/herself. (Hadnagy, Ekman 2014, 94)

The author's opinion is that fingers crossed on a table or keeping them in the lap so that the arms form a circumference with the shoulder is generally thought to control one's own territory. The person keeps their own space, however, he/she is also more open than the situation with hands crossed on one's chest would be.

> *A manipulator is defined as any movement that involves a manipulation or grooming of body part or article of clothing. Generally, it is caused by nervousness, discomfort, habit or a need to relax. One important point I need to bring up is that just because you notice a person is utilizing manipulators, do not automatically assume this proves deception.* (Hadnagy, Ekman 2014, 63-64)

Figure 1: Wringing hands (Hadnagy, Ekman 2014, 64)

Hadnagy and Ekman (2014, 64) explain that manipulators play with or touch a person's hair, hands, rings or maybe clothes. They say that nervous or unsure people may wring their hands, which is shown in Figure 1. Some nervous people play with their ring as presented in Figure 2.

However, Pease (1985, 51) states that wringing their hands can mean that people expect that something good happens. Pease continues that usually that good to happen is linked somehow with money and receiving it.

Figure 2: Playing with jewelry (Hadnagy, Ekman 2014, 65)

The author’s opinion as that social engineers can consciously interpret these and use them to benefit their own purposes. For example, if they act as a seller who asks either too unsafe questions or questions regarding security, they may show such signs of nervousness; or, if a social engineer acts as the expert and victims show signs of nervousness. In this case, the social engineer can be at peace because it can be assumed that the victim does not know anything about the matter.

Figure 3: One-finger steeple (Hadnagy, Ekman 2014, 67).

The author thinks that there are various signals to indicate that persons are self-confident. Of course, self-confidence is reflected on the whole body; however, the position of the hands plays a surprisingly big role. The position of the hands is relatively easy to control if there is need for that.

Figures 3 presents the hand “steeple” which is considered a self-confident message. Sometimes it may also be that the person who makes the hand steeple is willing to listen; however, yet aware of his own position. The common denominator is the vision of the person's self-confidence. Pease (1985, 54-55) explains that this gestures is an exception to the fact that a nonverbal gesture should be set in context. He continues that particularly

talented, self-satisfied, or slightly facial people seem to prefer this gesture. It is also typical to show director - subordinate relationship, he states.

Hadnagy and Ekman (2014, 69) state that a full hand steeple and the whole-body language can tell that “I am confident in what I am saying despite your challenge”. Pease (1988, 41-42) states that there are two main types of steeple: upturned and down-turned steeple. He continues that the upturned is used when a person is a speaking party and for example, to present some ideas or give orders. The down-turned steeple is usually used when a person is the listening party. Pease (1988, 41-42) also says that based on Nierenverg and Caleron according to their findings, women are more prone to use the down-turned that upturned gestures.

3.7 Neurolinguistic programming

Neurolinguistic programming (NLP) examines how a person thinks and observes the world and how he/she learns new things.
Wikipedia explains Neuro-linguistic programming (Neuro-linguistic programming, 2017) as follows:” NLP’s creators claim there is a connection between neurological processes (neuro-), language (linguistic) and behavioral patterns learned through experience (programming), and that these can be changed to achieve specific goals in life.”

NLP is in itself a very controversial method. NLP is also often referred to as the psychology the success. How could facilitate a social engineer? NLP enables the social engineers to be effectively able to learn how different ways of speaking, voices and choice of words work in sentences. Sometimes it is important to express the social engineer’s words correctly and manage a variety of ways of speaking in order to get the listener's mind to a certain kind of state.

For example, if one used questions as in the phrase "Do you agree on that?", the respondent has of course the freedom to choose; however, if the words

are turned over, the question will appear as an imperative form as "I agree to that, do you?". If the speaker adjusts the stress in the speech suitably, one can include commands very efficiently within the discussion.

The author opinion as that the emphasis on certain sounds is effectively used by advertising people, as well as by speakers. The use of speech sounds can be practiced if one wants to become a master and wants to use social engineering to his/her benefit. Even the orators practice their own speeches in front of the mirror. Secondly, the use of voice and words must be used very carefully and tactfully. With direct commands, hardly anything is achieved, however, with skills to use in appropriate situations, the victim can be fed certain associations with word stress. The most important issue for the social engineer is to be realistic about learning and the speed of one’s learning.

3.8 Modes of thinking

People have many different ways of thinking, which the social engineer ought to identify. If he/she is able to adapt to the thinking of his/her target persons, it is safer for him/her to get their own message through. Psychology studies are not required in order to learn this particular issue. Several research and scientific studies on the subject can be found on the Internet. (Handagy 2011, 140 - 142)

Ways of thinking can be divided in accordance with a variety of different styles. The easiest way is to describe the classification of how a person processes the information received and how he/she usually reacts to it. What does a person usually pay attention to? What are the things he considers important in the surrounding world? An unambiguous way is to consider whether the person is more of emotional or calculating type. (Handagy 2011, 141)

A person may be, for example, rational, i.e. he or she usually thinks very logically and mathematically. In this case, it is very difficult to appeal to this

person by using emotions. The only way which may affect the thinking are the numeric values and facts as well as logically proceeding thought chains. The emotional human being again driven by emotions produced by the surrounding world. This distinction is very rough, and on the other hand, it may be of little use when considering social engineering.

There is also a better classification when as far as a social engineer is concerned. People have five senses of which thinking is directly related to three senses. The senses, which people use to describe the world around them, are also the most vulnerable. They are as follows (Handagy 2011, 142):

- *Sight, or a visual thinker*
- *Hearing, or an auditory thinker*
- *Feeling, or a kinesthetic thinker*

These can be considered as the main headings of this classification. Among these senses the most dominating sense can be found, i.e. the sense that makes a person feel the world around him/her at strongest.

In addition to these main headings, there are countless more elaborate classivications, however, the social engineer does not generally need to go so deep to be able to use that information for his/her benefit. The following paragraph illustrates an example that is compared to each thought model of the above main heading.

It can be imagined that there are three people who each represent their own thought model. They are taken one by one to a room. The room is otherwise empty, however, there is a table with a variety of objects. In addition, the room has a chair on which the test persons sit. In addition, the wall has a clock. Quiet music starts playing in the room. The test persons are in the room, for example one minute after which they are asked what they remember about the room. Visual people are inclined to describe the shapes of objects, as well

as possibly a table and chair in which they sat. They can describe their shapes very precisely. (Handagy 2011, 143)

An auditory thinker in turn may illustrate the general objects on a table, however, focusing more on describing what music was played. They might even describe how, for example, the clock was ticking and noise of the chair when they sat down. (Handagy 2011, 143 - 144)

A kinesthetic thinker describes what the objects felt like, e.g. was the object hard or soft, cold or warm. They may also describe how good the bench felt to sit or how the table surface felt. (Handagy 2011, 144 - 145)

In the previous short example, one can already conclude that there are differences in human ways of thinking as to how the world is perceived, which is why it is very important that social engineers understand different people's ways of thinking, so that they can use their different tools effectively. The social engineer must also be prepared for the fact that he/she is forced to adapt to the target’s way to thinking creatively.

Things can, therefore, usually be indicated using three main styles, for example: The sun is shining bright and the leaves are moving in the wind, the sun shines warm and the wind can be felt in one’s hair or **the sun** is shining and the wind is whispering in the leaves of the trees. All of this reflects the same situation. The author’s opinion is that it is important to be able to express oneself well to the listener for him/her to be able to identify a desired mood.

Social engineers should also learn how to identify the persons with different thought models. Based on the first conversation with a person over small talk, one can quickly deduce what thought model the person has. It has to be added that the environment, mood, or even just the situation itself can influence the person’s presentation of the situation. Still, it is clear that people

adapt a certain main thought model to illustrate the world around them. (Handagy 2011, 146 - 148)

3.9 Interview and interrogation

Interview and examination styles are close to each other, although interrogation can be used with a great deal tougher methods than the means used in an interview. However, the principle is the same: asking the target questions that one expects them to answer and thus gaining the required knowledge.

Interviews are made by journalists as well as statistiscians. This study does not deal with journalist’s interviews. It must be noted that the social engineer can impersonate a journalist if he or she has practiced the role of a journalist and is credible in it, and most importantly, he or she knows the ways how journalists work. A journalist often has access to production and engineering facilities where outsiders have no access.

People generally have an open attitude towards statistic interviews. Information security surveys can be answered without any concern although an outsider is carrying out the survey. Sometimes in an interview people tell more about matters than would be appropriate.

Consultants or sales representatives use the interview style when asking about the customer's environment, and these questions may be often answered surprisingly openly. There are no NDAs or confidentiality issues with the sales representative or the statistician, yet, persons can reveal them a great deal of technical matters in their own circumstances and environment that should no way be revealed to outsiders. The key to openness is the interviewer's interest and the perceived the illusion of a safe and competent questioner.

Interview-style approach is therefore a very effective way of getting information about the company or activities. In general, a successful interview made over the phone does not even stay in the respondent's memory for a long time, thus, clarifying a possible information leak can be impossible. Of course, some of the companies mentioned issues that have been taken into account in the guidance. However, despite the adoption of the guidelines and training, phishing information can succeed very easily with interviews.

Personally, the author has often come across a situation where a sales representative directly indicates that they cannot showcase their services if they do not know the company's infrastructure. It is difficult for a sales representative to tailor their presentation to a potential customer if they do not know anything about the system. These events can present major security risks if the company representatives are not aware of what information can be shared.

Why do company representatives then give sensitive information so easily? There are many reasons, however, they are all based on basic human behaviors. People want to be helpful and to please, so that the person would not be awkward in the eyes of others. Another option is to try to assert oneself, and thus seek attention what their own organization may not give. Here are the two main reasons which are typically the root causes of this type of case. The reasons for this kind of behavior is often more mundane, for example someone is busy, careless or lacks concern. However, these are just triggers that enable the real character traits to operate.

This type of problem should be paid more attention to in the companies. It would be reasonable for companies to have a complete description of the environment, which could be handed over to sales representatives. It would be pre-thought-out, what information about the company's operating environment can be safely shared. Thus, the own company's representative would know exactly what to disclose about the activities of the company, and they would not have to rely on their own memory and experiences in

maintaining the environment. It can also be instructed that work or work place related statistical inquiries or other queries carried out by phone or e-mail are not to be answered. Compliance with this guidance could be, however, if not impossible, at least difficult to control.

For a social engineer, acquisition of this kind of knowledge is easy and effortless. They only have to come up with a suitable set of questions, which can be presented to a subject. In addition, they should consider getting direct numbers to different people. One cannot usually get through the company's call centers with these kinds of matters. The phone is the easiest contact method for this kind of spying. It is immediate and for the respondent the easiest way to answer questions. E-mails generally remain unanswered, or are marked as spam. In addition, the respondent has more time to think about the answers so slipses do occur more rarely.

3.10 Building instant rapport

Confidential and direct relationship with other people is perhaps one of the most important characteristics of humanity. Without the trust in another human being human civilization could never have been built. A couple trusts each other, the employer the employee, bank on the debtor that he/she will pay back their loans. Humanity’s, as well as an individual human’s action is based on trust. One can therefore think that for people a trust relationship is a normal situation to strive in activities between people. A person therefore seeks to establish a confidential relationship to communicate with others.

This is why, for example, social media succeeds in cheating the people and for example, victims can be attracted to appointments more easily. Although a person has never met the other talker, he/she may rely on social media to "meet their" person based on what he/she has written about themselves and their thoughts.

The author has often come across acquaintances who have a friend in the social media they have actually never met in real life. They may use words such as: a trusted friend, easy to talk to, or reliable when talking about the user account, which shows that the human’s will to be a part of a group is so strong that he/she even tries to adapt to a social media profile. Of course, this is usually polarized and anyone can look out for unknown profiles. On the other hand, an unknown profile may take a familiar and safe shape if the messages sent are consistent as well as revealing something about the person.

Human beings are very good at analyzing other people face to face. The first impression of another person is made in a one-tenth of a second. (First impression) The first impression is thus crucial when thinking ahead. The image of another human being is very difficult to change the first impression has been created. An automated analysis of a person can in normal circumstances be a very fine quality, however, when exploited on purpose, it is a dangerous form of manipulation. It is dangerous because it is fast and it has direct access to modify the subject's way of thinking. According to Wikipedia, shaping the image is also affected by age, culture, skin color, language, gender, physical appearance, posture, accent, or the volume or tone in human intervention. (First impression)

A social engineer can quickly create a reliable and fair impression of him-/herself by a correct style of approach. If he/she manages to create a certain image of him-/herself to the victim, it is easier to achieve the desired goal. Presentation of consensus brings trust but also a sense of belonging. A social engineer should have some ready thought out "revelations" about themselves, and the bonding and mutual trust can deepen very quickly. The best method of approach is to begin to talk about the personal issues connected with the role, and perhaps the victim might tell about their own affairs.

After this, the discussion can more easily approach the work related issues. This is because in most cases, one’s own life is considered to be more

important than one's own work so that the approach method in this case is to progress from the protected matter towards the more open issues.

It should also be noted that the social engineer him-/herself is not immune to the effects. This means that the social engineers can accidentally confuse their roles and their own egos, especially if he/she is not an experienced actor. The exact background work certainly may help in making the present role sufficiently deep. Social engineers also have the advantage that they have a precise aim. However, they cannot freeze their own senses and emotions.

The social engineers have the same advantage as the other hackers: the number of attempts can be carried out countless times. Social engineers also have the advantage that discussions with people are not a crime; however, in case of the other hackers, intrusions are criminal activities from the very first session.

3.11 Human buffer overflow

The term "buffer overflow" comes from the computer world. It refers to a situation in which in the computer memory area is written with overlong information. As a result, the storage areas can be written with desired information. For example, malicious software can be written in the memory and referred to in other contexts.

> *Unlike a computer, your brain doesn't crash, but it does open up a momentary gap that allows for a command to be injected so the brain can be told what to do with the extra data.*
> *A human buffer overflow is basically the same principle. The goal is to identify a running "program" and insert codes into that program that will allow you to inject commands and in essence control the movement of thought to a certain direction. (Hadnagy 2011, 229)*

Human memory overwriting, therefore, slightly resembles the same phenomenon as in the computer world. People can be fed so much secondary information in one way or another that they are no longer able to distinguish it or to focus on the primary task. This is proved using a simple test which is shown in Figure 4. In the test, the test person should pronounc as soon as possible colors which the words are colored with. One may not stop but the task must be carried out as quickly as possible. If one succeeds without error, then one should try even faster. (Hadnagy 2011, 230)

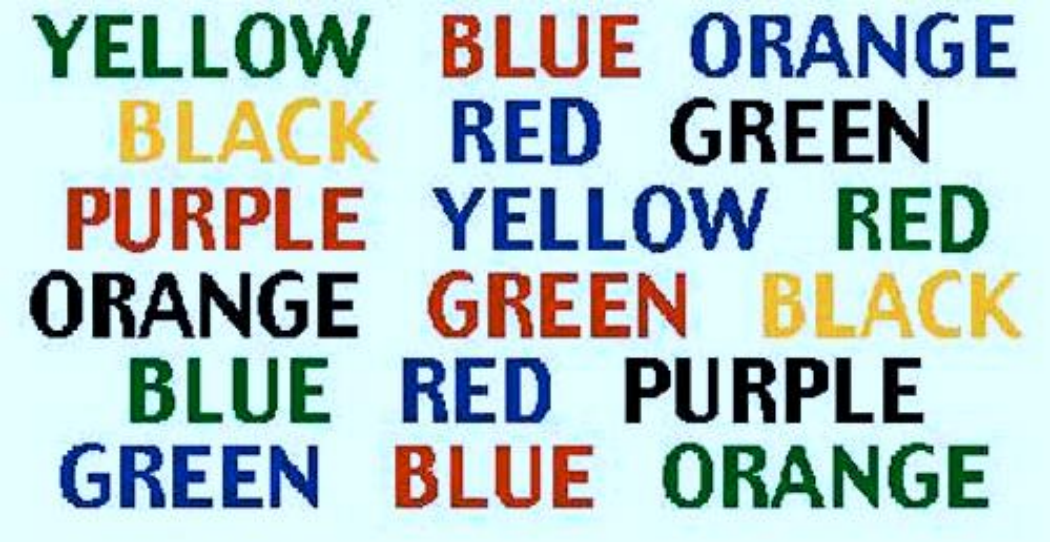

Figure 4: Color test (The Human Buffer Overflow)

The test shows how easily the mind can be overloaded. In general, a human begins to recite the first words and colors. This is a simple way to show how a person can enter the "code" which is the opposite of what a person thinks or sees.

The things above seem at first glance to simplify human behavior and mechanization. Still, using this kind of information social engineers can enter or mix for example the employee's ideas. Every person has a restricted capacity of thought. According to the website, the human brain produces 50,000 ideas every day. (Thoughts)

Therefore, human beings themselves generate an idea every 1.7 seconds. If the production of the idea is overloaded or a human being is simply stressed out, the number of conscious thoughts can be clearly calculated. For the social engineers to exploit this data they already have to have existing tested practices.

The human processing ability is tested in today's society constantly even without paying attention to it. Of course, it is also developed in and for different situations. The military, studies, job interviews, everyday routines, emergency situations, driving a car etc. are all situations or places where one encounters this matter. They all either measure and / or train a certain style of processing ability.

Which more people learn, for example first aid skills, the more likely they are able to help in a situation where help is needed. Training therefore has the ability to increase the processing capacity and concentration. A job interview again estimates a person’s behavior and related practices. The interviewee should focus only on the important issues in an interview. This can be improved through training and experience.

Thus, one can draw a conclusion that studying and practicing the security aspects can at least make social engineers’ job difficult, because employees would have pre-learned behavior patterns for certain situations. The challenge is, of course, that it is impossible to know in advance in what kind of social situation a social engineer can approach the employees. Therefore, it would be very important to find a security training that would work just as much at a general level but also as effectively as the first-aid training.

4 INFORMATION GATHERING AND DEFENSE

This chapter deals with practical examples of social engineers’ tools that were introduces in previous chapter. Social engineers must get for their

commissioner information on the project related issues carried out for BB Company project. Section 4.1. deals with different ways that social engineers use to collect data from their targets. In addition, examples on how the information obtained can be further utilized are dealt with. In the examples, the follow-up information is utilized in order to collect even more useful information.

Section 4.2. discusses phishing control as described in section 4.1.

4.1 Different methods for information gathering

Data collection is an important measure for a social engineer's success. Information must be ready to accept even in large masses. Large masses of data can be obtained for example from different tables, databases, etc. It is not simple to gather and process relevant data from data masses although at first glance it might seem to be so. Processing the date in its various forms is something a social engineer should learn even before he/she is in action to carry out his/her first attack.

Social engineers must have a detailed plan what tools and methods are utilized. They must have good general knowledge of what information can be obtained from public sources. A variety of public sources can provide surprisingly detailed information. (Mann 2008, 213)

For example, company registers or registers by the domain name generally give personal data. In addition, the Internet can easily be applied using certain filters and documents can accidentally or intentionally end up as public documents that are not necessarily directly linked to the company's official web pages. These documents often provide at least general information on the different services and, above all, the names of the authors of the document, and possibly contact information.

The company's public presentations or webinars can also be useful for getting information on the company’s employees. The more technical employee’s contact information is gained, the better. If that is a person in a supervisory role and a representative of middle management in the technical department, direct contact can be really valuable for a social engineer.

Phishing should be focused on the company’s closer locations for several reasons. First, potential targets are close and they are relatively easy to follow if necessary. Meetings or company visits and follow-up operations are easier to perform when one is near. Finally, an old but unfortunately even more profitable way is to visit the company's bins and paper recycling boxes nearby. Unexpectedly, relevant information can be found there that has at least indirect meaning.

Once enough information on contact information and background material on the company’s products has been gathered, the first and the easiest of knowledge phishing attempts can be realized. The collected persons are sent a tailored or a common e-mail. E-mail may have an initialization or softening, so that the role or company created by the social engineer or company could get in touch with these persons more easily.

E-mail can also be an outright phishing message including a link that would take one to an interesting site. However, the site would contaminate the computer and the computer would, for example, make a back gate or other social activities desired by the hacker. In that case, social engineer should not use any site or name that would refer to the imaginary company or background information.

Generally, these emails are either spam filtered or later, the computer's own anti-virus blocks away from the risky site. If such a warning message to the user, the message remains the company certainly had a negative mind, and in this case it should not be used anymore.

Via e-mail message even a factual emain remains easily unopened if the company or person does not know the company or person already. The message can be made more efficient by calling the objects in a few days to agree on a meeting or some similar appointment. In this case the social engineer has to be really ready to hold a presentation if asked. The event should be genuine. Even the smallest thing can arouse suspicion. However, it is easy to hide in the seller's role behind the fact that technically one does not know all about one’s products.

A social engineer can only hope that some of the recipients have read the message, at least glanced it through. E-mail will facilitate contacts in the future, but even if the objects had not read it, it does not prevent the operation. Besides, it can be used if necessary to confirm the own report of the company. People tend to believe something easier if the data comes from two different locations.

Email content should be formatted so that the style of some word combination slogans would be easy to remember. Praise for one’s product is not likely to produce sufficient memory trace. The message must also be scheduled in such a way that targets encounter each otherface to face or over the phone as soon as possible, however, not necessarily on the same day. Generally, an employee forgets a slogan during the weekend, ie. after a week the targets are not able to combine the occasional company representatives with the message. Not even when the object has read the message intently.

After the e-mail, the social engineer can approaches the targets with a telephone interview. The company represented by the interviewer and interviewee must be real but another than that used for sending an e-mail. Otherwise, suspicions might occur. Another possibility would be to call after sending an e-mail and ask for a demonstration and ask questions about the possibility of a meeting.

The best part is if the object assumes that the data has come from his/her superiors. Thus, the target can relax and might talk too much. Disclosures for additional questions may relate to, for example, project management knowledge levels, delivery times or validity of the designers of expertise levels. As such, the questions are generally acceptable if there is a statistical interview.

Next the social engineer can to try information phishing directly in the personal appointments. Approaching the person has to be designed in such a way that it should be as natural as possible and look like a coincidence. This means that the social engineer must be familiar with the object's daily routines: where does he/she go shopping or for a cup of coffee. Does he/she lunch outside the workplace alone or in a group, always in the same bar on any given day a week etc. The social engineer must find the status and situation that occur regularly. In this case, he/she can design the approach as well possible and, where possible, use the background information obtained about the target.

The discussion at a café with morning coffee has been previously after which the social engineer can easily change business cards with the target and how the social engineer got important titbits of information about the target's short-term plans. This example is used to provide a realistic situation so the social engineer has all the chances to take a similar approach.

Due to the example situation, the conversation is now slightly modified and various techniques are analyzed. The subject is still called Bill who sits at the table alone and the social engineer, called Harry in this example, enters the scene with a coffee mug.

Harry: Excuse me, is this seat here free?

Analysis: A demanding question. Can be enhanced with an open hand gesture and looking in the eyes.

Bill: Yes, it is, just sut down, please.

Analysis: A polite man cannot answer in any other way if alone.

Harry: In the morning coffee is so good, is it?
Analysis: This statement, shrouded in the form of a question, in which case the victim usually has to answer the question.
Bill: Yes, nothing can beat a cuppa.
Analysis: Required mandatory answer.
Harry: I need this after a sleepless night. Our little Nina was awake throughout the night. She was only a year old.
Analysis: The first phishing attempt. Based on the same the situation with a deep feeling, as well as a hacker's information on the imaginary role coined by him/her.
Bill: I know; we also have a child who kept us awake the other night. His name is Mike and he is also one-year-old.
Analysis: This is the first data item gained by phishing.
Harry: Familiar therefore to also you, heh. I am the way Harry, nice to meet you.
Analysis: A common experience is utilized, so that the conversation can be smoothly directed to introductions.
Bill: My name is Bill. (the target provides only the required information, still alert)
Harry: Could you help a little? I've started a counter-VAV firm where we produce technical processes. I'm supposed to find here the HOH -company but I have not had time to look for the company's contact information. I thought that you could perhaps know where it is located?
Analysis: calling on the need for help, as well as the knowledge / expertise of the other person.
Bill: Yes, I know, it is located a couple of street corners away in that direction. What a coincidence, I also work in the field as a technical designer.
Analysis: Target knew how to help. In addition, the case has shown bits and pieces close to him, so he gets a little excited on the matter.
Harry: Uh, such good luck! Can I ask in which company you work? Are you familiar with our company?

Analysis: Pretends to be surprised. Shows interest in the target and looks for more similarities in accordance with the normal functioning, although it is known that there are none.

Bill: I work in AA Company. I certainly would not remember that I have heard about your company. However, I've been working for 5 years already. However, I work in product development.

Analysis: The target tells about himself more than is asked, which is based on the normal experience when a person feels a part of some group and safe.

Harry: Would it be at all possible to get to present our products to you? In fact, I changed to this company, because the product was special to me and it actually helps work. I'm just a beginner in the sales, and I do not have many contacts. I would like to come and give a presentation of our product, for you, right?

Analysis of the proposal, the product is praised and the request with it together give such a strong message that it is difficult to decline directly).

Bill: I do not directly know whether we have any use of your product, but I can give a business card. Contact us and I'll see what I can do about it. We start our holidays with the family but contact me later.

Analysis: The target reveals more about themselves than was requested. He has finally opened up because he sees Harry as nice guy and wants to help him as well as perhaps improve his own situation in the company

---

The social engineer found out that the subject is going on vacation next week. He has a technical designer business card with a telephone number, direct e-mail ad-dress and full name. In addition, the social engineer managed to agree upon a contact under the pretext of which he can try to approach other employees of the target company.

In such information in phishing one should not try to get too big a catch at once. As is usual in fishing, in general, small individual fish are caught, however, one of which can become a major catch. In the same style, the social engineer must move in order to avoid growing suspicions.

As described previously, the social engineer can take advantage of a number of different ways to affect the target. However, it must be remembered that a person makes an estimate of another human being in even 30 seconds. For this reason, the hacker must take social failures constructively. They are there to learn from and then one just has to try new targets. The most important thing in his/her work, however, is to keep the objectives in hiding to avoid suspicions.

Social engineer can use the basic knowledge in discussion to guide the discussion. As in the conversation between Harry and Bill, Harry took advantage of the knowledge that Bill has a small child, he is a local person and that he drinks his cup of coffee just in this particular cafeteria. Social engineer has to, however, take care not speak or imply anything that might suggest he knows something about the target directly. If the target has the slightest doubt about the subject that he/she knows something the discussion is then over. As previously noted, the man is very clever in interpreting social messages. This includes the spoken language. If even one phrase contains any kind of information that the guest has not found out in the the discussion, the situation built so well in advance may very well collapse.

4.2 Defense from information gathering

How to prevent the situations discussed in section 4.1? One might think that there is no way to get over the situation because some of the information is obtained, even if the company tightened their operations no matter how much. A good starting point is the already mentioned onion-shaped cybersecurity thinking.

Cyber security must be treated as one large whole, where each separate onion skin brings its own important part to a safe environment. This way of thinking can be applied to considerably complicate the hacker's social activity, although it can never completely block it.

Information obtained from public sources cannot be denied, however, companies usually have some kind of room for maneuver on how accurately the information must be entered. If possible the information is fed with the so-called general data. Thus, the CEO's information is not given in voluntary data fields or when purchasing domain names the technical purchaser's information is not filled in. If a telephone number is required the switchboard number is used. When a company has a clearly thought out, what the level of information is which is to be implemented in public records, it just needs to ensure that it is respected.

The second situation to pay attention to are all the other publications. If the company is large, it is normal that the company has joint document templates and presentation templates that are used. It is, however, to also pay attention to the information given on an individual person. A sales representative in general is supposed to be present as much as possible and easily reached and available at least by phone and e-mail.

However, if there is a technical designer who holds a seminar, it does not necessarily make sense to use his own direct phone number or email address but direct the contacts to the sales representative. The same applies to internet publications and even recorded webinars. If the company is protected to the extreme, the company's design team personnel can use an email address that does not show the employee's name but for example an employee code. With these extreme precautions e-mail phishing is prevented.

It is also good for the person responsible for the security management to check that their own pages, or pages of the projects involving subcontractors do not leak for example some pdf documents, which should not be shared on the internet. The purpose of all these above issues is to reduce the attackers from receiving background sources. If the data is minimal, it is from the attacker's point of view more challenging to approach objects, as the background material does not necessarily give many options for different implementations.

The company should also provide the basics of the concept of information security. The criteria include the orthodox destruction of data in its different formats and securing the removal equipment. The basics also include access control and restriction of access rights if necessary. Furthermore, key issues which need to be in good shape are data security practices, deviations management, and security training.

As noted, the onion method security implements the same principles as normal security. In the onion model, every little aspect is considered equally important, because even a small thing when repeated can lead to surprising consequences. Earlier, the previous section described that the social engineering action could have been much more difficult if data protection had been implemented at every level with vigor. There should have been less background information.

Contact with the employees would have been hard to come by. A telephone interview would not have succeeded if the company had had a common approach for interviews or a business model that would have banned it completely. If the interviews had been participated in, a written list of questions could have been requested before answering. Thus, the defendant's "lapses" would have been likely less and it would not have been possible to add leading supplementary questions.

The most difficult situation is to affect the employees free time in work-related situations. Only continuous training helps here, and, if possible, then practicing. The employees' own activities, especially in their leisure time, are impossible to intervene, however, properly targeted education can awaken the employee to think about matters and thus, in the future they are maybe even a little skeptical and aware of the threats that are completely foreign to them that a stranger can cause.

5 SOCIAL ENGINEERING CASES

The previous chapters have gone through different situations of how human behavior can be influenced. The content of this chapter focuses on an example situation where an employee acts differently from the company's normal practices. Furthermore, this chapter deals with the different possibilities to combat these kinds of social engineering attacks by technical means as well as the author could. 5.1 section goes through a variety of ways to utilize social influence and the author present case. It also covers the various emotions which should be relied on and which have been discussed partly through Chapter 2.

5.2 section is an example of what goal a social engineers sets to get into the business office and use his/her own USB stick to use on the company's computer as the assignment required in section 1.3. Section 5.3 goes through a variety of techniques, and especially the technical means to prevent a hacker from using the social method described in section 5.2.

5.1 Case 1

Social engineers have to choose different methods for different situations. In general, social engineers need a number of different efforts to succeed. Several times they also have to change the angle of approach or methodology to achieve their goals. Chapter 4 illustrated how social engineering uses social influence in order to obtain information. Chapter 3 dealt with various aspects that the social engineers must taken into account when trying to influence other people. However, this section deals with the data collection and the effective areas of the individual rather than complete methods. How can one analyze methods of influencing keeping in mind the big picture?

The main parts of the methods could be divided into at least two distinct parts. The purpose of some methods is to indirectly affect in such a way that the social engineers are no longer so focused on their own office. According to

another method, on the contrary, the intention is to concentrate on the target situation.

The implementation of the entities of the first method is usually done by causing some abnormalities which can be timed just on time for the situation when the social engineer needs. This can be called paying attention to the wrong issue. The abnormality may be a false fire alarm, an elevator getting stuck or even a power outage. In fact, abnormality depends a great deal on where and what type the object status is.

The author presents a case about an abnormal situation causing abnormal action of an employee. He was going to a job interview to a multi-level office building. The lobby had receptionist as is the case in many office buildings, where it is desired to restrict the free passage of outsiders inside the building. When he came to the receptionist's desk, the receptionist was a little frantic.

The author explained this reason to enter the building, an interview in Mr. X's office on 3rd floor. The receptionist keyed in the computer and after a while said that the system has crashed and that he cannot announce the author normally. He was also unable to check whether the author had been announce to arrive. He gave a note to be filled in, in which the name, cause of the visit and the company data if representing the company were asked. The information of the author he could not check anywhere. He was agonized with the system and said that the author can definitely go on the elevator to 3rd floor on his own and from there to the door of the enterprise.

Sure, there were security cameras on the different floors so the company could keep track of the author's movements. Still, he had managed to walk on his own to closed floors without an escort with a visitor card. He was not yet technically inside the company, so he could have installed for example a spy device in the elevator and use it to track the movements of the company personnel and internal elevator speeches, e.g. when staff were going to lunch.

All this was only due only to the fact that the receptionist's system did not work, so he was not able to inform anyone and not check the accuracy of the system. The biggest mistake was, however, in that no one in the lobby security personnel escorted the author to the company's premises. Judging by the speeches of the representative of the company, however, this would have been such a common and agreed approach. Thus, the deviation caused the attention to focus elsewhere and the receptionist adjusted the agreed operating models in order to cope with the situation more quickly.

Other approaches could be called appealing to the emotions. The aim is therefore to identify the target presented with the situation by a social engineer so much that the target does something that is different from their own free will.

This is strongly associated with at least the techniques used in section 3.3 and 3.4. The aim is to get the target to focus on the situation or report so that the target would feel, for example, compassion, sympathy, or bonding, depending on what would be appropriate to the social engineer's intentions. Thereafter, the target would be more exposed and uninhibited to implement the social engineer's requests.

5.2 Case 2

5.2.1 Background

The social engineer's goal is to get company information about the project, reach the inside of the target company and get using one means or another his/her contaminated USB memory stick used on the company computer as the assignment required in section 1.3.

In this case, the social engineer would have reached the desired situation, and the company would have received a polluted computer. The goal is clear, however, the choice of means is not easy. The selected point is the office of

the company, in which the designer found in the coffee shop works. In this case, the social engineer can take advantage of this information and be sure that the person is actually working just in the office in question.

The social engineer’s sidekick has inquired about the office building in advance. The social engineer should not himself inquire about the building because he would be identified when the actual attack occurs. The assistant has found out that the company can be accessed through the back door entrance. On the other hand, accessing and moving in the company's indoors is not allowed without an access pass and visitors are not allowed to walk there without escorts. In addition, the lobby does not have free access to any space without the receptionist in the lounge opening doors. Opening the doors takes place in the receptionion. In addition to an outside door and guards, the door from the lobby is only accessible by elevators as well as some kind of conference room.

It is likely, therefore, that the company's office premises cannot be, at least are not easily accessed, be accessed even though the social engineer had some kind of a contact there. However, the intention is to take advantage of a situation where the designer is sure to be on vacation.

Another possibility would of course be to utilize the contact and try to get in as a sales representative. Even a discussion from a week ago might seem to the designer quite a distant situation. Besides, the emotional bond between the social engineer and the designer with their shared experiences has already been dissolved in a week.

It would also be possible to use force, that is, to physically break into the premises in order to achieve this goal. However, the spaces are protected and burglar alarms and security cameras are frequent, so this behavior is not acceptable.

It would also be possible to find out more about the company's employees and get, for example lists on the basis of the employee tax information to enable to determine the so-called underpaid security threats. These usually refer to persons who may be angry at the company anger to being underpaid for years. In this case, a person might have lower loyalty to their employer and for a suitable amount of sum this person could even harm their employer. Finding a person such as this can be very time-consuming, because the person's life other than work should also be found out. Is he/she happy, does he/she have game addictions or other vulnerabilities? It should be noted that the majority of low-income employees are equally loyal towards their employer as any other employee; therefore, a company like this can be very risky for the social engineer's point of view. Because thre is not much time available and the social engineer does not want to arouse any extra attention, the above-mentioned activities are not acceptable.

5.2.2 Sequence of events

In this case the social engineer wants first additional information on the activities of the organization. The social engineer approaches the targets with a telephone interview. Questions can be customized, for example, for the industrial managers more practices and staff oriented. Technical people should be asked questions, through which the social engineer gets an idea of the technical skills and possibly refers indirectly to the subject of the technical development.

The executives should also be asked a few technical questions. If and when actually a senior technical person does not know how to answer the question, the social engineer can persuade him/her to give a technical person’s contact information so that the issue can be discussed in more detail. In this case, it may happen that one gets the background information, contact information of the technical person as well as a permission to interview him. This situation can be exploited for information access.

The social engineer gets some kind of technical attributes from some other sources for concerning the environment and the ongoing publishings. He/She makes a few technical questions to which the company's management person does not know the answer. The social engineer appeals on the phone to the fact that research results cannot be used if he/she does not get any answers to technical issues, and he/she suggests that the interviewee could give the contact details of someone involved in the case to get their statistics as well. The management person provides the contact information of the technical team leader and asks the social engineers to call him/her.

The social engineering waits for half an hour in order to possibly make sure that the manager's message to the team manager has had time to reach him/her. This social engineer tries to ensure that the next target knows about his/her agreement with a management person and that the team leader is friendly towards responding to interview questions. The social engineer feeds the team manager technical and environmental information in the discussion that he has collected in the interviews with other objects. Thus, he seeks to create an atmosphere of trust and to show the team manager that the interviewer already knows a great deal about their surroundings.

Now the social engineer should not reveal that he has collected information from other employees. The best part is if the object assumes that the data has come from his/her superiors. Thus, the target can relax and might talk too much. Disclosures for additional questions may relate to, for example, project management knowledge levels, delivery times or validity of the designers of expertise levels. As such, the questions are generally acceptable if there is a statistical interview.

When one wants information and the situation has turned out suitable for the social engineer, he/she finds out from the team leader the following:

- projects under way: a few small and one big one that takes most of the designer’s current work input

- Project management utilizes especially for the demanding projects external consultant companies
- John Smith who is responsible for the designer team has university education. He is assisted by five other designers who are vocational-level designers. However, Bill Scoth is studying at the university for post-graduate education, yet, his current work situation prevents the studies
- In general, delivery times are kept, however now, in exceptional circumstances the projects for small customers are stretched. The situation will, however, ease during the first half of the next year.

The above issues can be raised during the interview. One might think that such things are not to be revealed to a complete stranger in an interview. However, one needs to keep in mind that in the eyes of the interviewer, the team leader has already "accepted" him/her in the group as his/her boss has given permission to the interviewer to ask him questions. In addition, the social engineer has gotten very lucky that the team leader when thinking of employees talks with names. Thus, he gets a few key persons' names and titles.

The social engineer has already received some of the information that he/she wanted to know. Details still need to be secured.

Currently however, the conclusion is that the most likely John Smith and Bill Scoth or one of them is involved in a large AA company project, which in turn is assigned by BB Company. It is also known when the project probably should be ready. It is also known that the project is likely managed by an external expert. If the external acts as a project manager, getting the project has just become possible without trying to phish it directly from the company. Admittedly, one needs to test from which source the project information could be obtained easier.

Next, the social engineer needs to try information phishing directly in personal appointments. In this case, the social engineer has the same conversation which is described in section 4.1 and he gets the same information.

Before the next step, the social engineer's assistant calls the company lobby receptionist and mimics the expert who the social engineer previously met. The assistant uses new AI technique, which can mimic any voice (Gholipour, 2017). The assistant tells that he is now on holiday and has forgotten his meeting. He requests that the lobby receptionist tell his guest that he is sorry. Also, he requests the lobby receptionist to help this guest in the best possible way with the matter related to their project.

Then the social engineer decides to try directly influencing the security men in the lobby. Because the company owns the entire office building, it is likely that the lobby computers are in one way or another linked to the company's systems. The social engineer attacks as follows:

- Social engineer presents him-/herself as a consultant, who has come to see the expert who he previously met with. He claims that the meeting has been agreed upon with the expert, in which they would go through a papers on the USB before he/she would take them to the organization that has ordered something from him.
- The lobby receptionist will review the situation and propose that there is no meeting and the expert is not available. The social engineer acts as agonized and beaten using gestures, facial expressions and word stress. He/she asks if this the just the week that the expert is on holiday and he/she is sure to have confused the weeks.

  He/she explains that the matter cannot be resolved with anyone else since the others have not been involved in the case. He pretends to be desperate and explains that today was the very day when he/she has to return the paper on USB stick to the ordering company and he meant to print it with the expert. The social

engineer has also invented a story about being new in a company and on trial. Keeping the other company happy is so important to him and he cannot possible go back to the office to print out his files.

- If a social engineer succeeds in the first social situation, he or she can obtain a receptionist to print the transcripts on his own computer. In this case, the infected memory stick is used in a company computer and though it, it is likely likely to access the rest of the infrastructure.
- The lobby receptionist can also be kind enough to advise the social engineer to the nearest bookstore or Internet café where the files can be printed. In this case, the social engineer thanks him/her and shows gratitude. After this, he/she can ask if he/she could swiftly get to visit the restroom. This, he hopes to gain him the negotiation mode.
- The receptionist emotions have been appealed to by the story, and he/she already feels that he/she is valued in the eyes of the visitor, because he/she has saved his day. As a result, he/she opens the door to a conference room and advises where the bathroom is located. Since the conference room is empty, the lounge clerk does not feel he/she is doing anything wrong. The social engineer can now access the restroom and since the clerk has returned to his/her workstation, the social engineer has an opportunity to act in the conference room for a short time independently. Conference rooms seldom have camera surveillance, so no one can see what he is doing. He cannot leave wireless transmitters on the presentation technology to be able to spy the material presented.
  He can leave the correct power outlet power adapter with a microphone and a radio transmitter such as Conheydy (2011, 190) presents. Conheydy also presents (2011, 192) an extension cord that can be installed in the keyboard to record all keyboard presses. The social engineer can also leave in the room a special wireless network base station, in which case he has a chance to find out with

with time among others the computer's status of the wireless network encryption key or MAC addresses of computers used in the room.
These he could utilize for hacking the network or attacking the wireless network. In the best case, the room has a company computer as the presentation computer, which is likely to be connected to the internal network. In this case, he/she can use his/her own memory stick on the computer and contaminate it very quickly.

- On leaving, the social engineer thanks the receptionist and tells that he/she will contact the expert later by e-mail as soon as he returns from his holiday. This is yet another opportunity to send the infected file via e-mail which the expert may open, because the receptionist in the lobby might have left him the information on the visit of the consultant.

Thus, after propagating, the social engineer has been able to infect one way or another the company's computer, or at least has created a good chance for further actions to achieve the goal if not already earlier during the visit.

5.2.3 Defense methods

The same rules apply to social engineering as the rest of the information attacks. It is always easier for the attacker to find exploitable holes as for the defenders to clog them. Data security experts do not never get the systems or functions 100% proof. One attacker is enough to exploit a security hole to achieve the desired goal.

Social engineering is even easier than general hacking because the object is a person who does not behave consistently according to the same logic, which is why it is very difficult to create high defense methods which work every time.

The methods do not work every time because the environment changes. For example, a plan of action is created in case of telephone interviews, maybe just on that day when the telephone interview call comes, the employee does not remember to plan of action. The employee can also be too busy or some other thing prevents him from checking the plan of action. Because of this, it is never possible get 100% proof there where people are working. One just has to accept in security business that one can never be too sure. A small doubt is always in place in everything.

The attack presented in section 5.2.2, however, can be made more difficult with certain technical procedures. Using the onion model of security thinking, means that with multi-level protection measures good protectiong is secured. It does not matter, even if the outermost defensive layers get socially hacked. This model can be used for the protection of the inner parts of the fight. Information security planning can use the onion model to protect network, data, for account management, device protection etc. but for designing the company’s public spaces.

The lobby, which has free access to outside should have seats for visitors. In this case, they can calmly wait for an escort, and do not cause extra movement in the lobby area, which can sometimes cause the pressure on lobby receptionists. In addition, the lobby area is a good place for a restroom since there is no need to allow visitors inside should there be a nature’s call.

The lobby space can also provide a wireless network connection that is completely out of the firm's internal computer network. In addition, the lobby lounge could have a printer be supervised by the receptionist, from which visitors can print out if necessary the last papers prior to the meetings. This will of course cost a little but because the lobby clerk supervises the use, no outsider can take advantage of the free printing.

Arranging these kinds of services to guests is not costly, however, it protects the public area, and it separates the company’s important areas also

physically with the wireless network and other services protected as well. The onion model is realized so that does not mather if the printer or wireless network in public area is hacked because the danger zone is limited.

Conference rooms should not contain a presentation computer that can access the internal network but the staff must be instructed in such a way that each use their own laptop computers for presentations. The presentation equipment must be protected as far as possible so that no additional adapters are easy at all to add without noticing. It is a good idea to check the conference rooms for extra wireless networks time to time.

The lobby receptionist’s computer should be completely disconnected from the company’s own information system. The application used for announcing the visitors and meetings should be located in the cloud. In all doors leading indoors as well as doors between departments should have controlled access.

In addition, the elevators can be included in the access control so that the visitor will always need an escort in order to access the interior of the firm. The lobby receptionist’s official space can be a glazed in such a way that a part of the wall would be a one-sided glass, so the clerk can observe the lobby unprevented, however, the receptionist appears only from waste up in the so-called bust image, which is to prevent that the visitor can analyze his/her gestures.

If a country's legislation allows, visitors should always be asked for identification. However, the policy must be that all visitors are recorded and each visitor must be recognizable as a visitor in the company indoors. This is usually done by hanging a brightly coloured identification card round the neck. In this case, the employees will recognize immediately an outsider.

5.2.4 Summary

The most important part to make social engineering more difficult is to think about action models that are unambiguous. They must also be easy to follow,

so that employees comply with them. The most important part plays the training during which approaches are taught, and the staff is explained why this is the way they should act. It is also necessary to give the staff the necessary training in order for them to understand the dangers of social engineering and at its best, the employees would know how to prepare for unusual situations.

The company should also have an open atmosphere, and even some degree of support for settling civil life difficulties. The firm could have e.g. a practice that those suffering from gambling addiction can get help through occupational health without any blame on them or threating their jobs.

In this case, employees free time pressures could be prevented. They could bring the attention of the company to pressure efforts put on them independently if they already had been discussed openly, and developed an action model should be created that the employees know about. Should such situations occur in a company, it is vital to back up and support the employee and not make him/her feel feel guilty or doubt him/her. This kind of work environment would create the conditions for transparency in their operations, and the risk of efforts to influence the employees could be reduced significantly. Preventing social engineering prevention is, after all, dependent on the employees, that is, every person who works in a company.

Social engineering is possible to prevent but it is the best defense that social engineers' modes of operations are familiar. That is why it is important that social engineering attacks are published in the media so that everybody has an opportunity to learn and protect themselves from similar attacks. Of course, it can be embarrassing for the company which has bee targeted, however, there should be some way to find a method to report on these cases anonymously.

The onion method is a great way of thinking about information security defence. If security planning uses the onion method and if the planning is

careful and all aspects are considered, this will automatically defend the company against social engineering attacks. However, it is important also to design the protection first byputting oneself in the attacker's shoes. It is important to study different human behaviors, which are social engineers' general tools when they attack. If the security experts know the human behavior patters as well as the social engineer, they can better to set themselves in the real attacker's role.

Social engineering very much resembles general hacking. Only one hole in defend is needed for someone to find and exploit. However, they also have differences, since the methods and tools used by a social engineer are generally legal. Of course, illegal email phishing or any phisfing for information or spreading malware is illegal.

Social engineer can talk to an employee as many times he wants and that is legal unless for some reason a retriction order is needed. A social engineer can call the company and collect public data, which is not illegal. That is why social engineer scan make some social preparations and even attacks. If a hacker makes preparations or some attacks they are almost always illegal, which is why the style social engineering uses and that is discussed in this thesis is so dangerous.

6 DISCUSSION AND CONCLUSION

The diversity and interdisciplinary approach of the topic was challenging to implement. The subject itself is very interesting and by immersing in ad hoc situations, the discussion on the subject gives plenty of considerations. The subject gave many own reflections on the security aspect. For myself, it was even a bit of a surprise to notice how easy it is to use the methods of social engineering.

It is also interesting to note that social engineering cannot be criminalized in many cases, because it is based on the normal human interaction. That is why this hackering style is so interesting for me. The deeper one studies something, the more one learns about your next neigbours, also something what is not meant to exploit the information for somenone's own personal goals but it is more about understand others. Social behavior patterns are already used for the benefit of many different matters.

I think, however, that it would be good to teach behavioral science to ICT oriented engineers and especially to the security-oriented students. Engineering studies will often remain technical for obvious reasons. It might be, however, an idea to open up the world to deal with the environment in which engineering students will design the equipment.

From the cyber security point of view, the social aspect has in my opinion a big role, because social engineering is, however, today and in the future the easiest way to get and use encrypted data. In my view, security, and social interaction are important issues and I believe, therefore that research is conducted around the world in the future around the subject.

Interestingly, it could be further researched as to how social engineering could be prevented by using the social engineers' own methods of social engineering in the company's premises, e.g. for example, by manipulating outsiders in different ways.

REFERENCES

Conheady S. 2014. Social engineering in IT security. McGraw-Hill Education.

First impression. Accessed on 17.4.2017. Retrieved from https://en.wikipedia.org/wiki/First_impression_(psychology)

Danish TV. 4.9.2015 Hans Rosling: Don't use news media to understand the world (english subtitles). Accessed on 30.5.2017. Retrieved from https://www.youtube.com/watch?v=xYnpJGaMiXo

Gholipour B. 2.5.2017. New AI Tech Can Mimic Any Voice. Accessed on 30.5.2017. Retrieved from https://www.scientificamerican.com/article/new-ai-tech-can-mimic-any-voice/

Gonzalez-Garcia J. 25.8.2016. Credit card ownership statistics. Accessed on 7.4.2017. Retrieved from http://www.creditcards.com/credit-card-news/ownership-statistics.php

Handagy, C. 2011. Social engineering, The Art of Human Hacking. Indiana: Indianapolis Wiley Puplishing, Inc.

Handagy C., Ekman P. 2014. Unmasking the social engineer. Indiana: Indianapolis John Wiley & Sons Inc.

The Late Late Show with James Corden 1.11.2016. Mentalist Lior Suchard Bends Harry Connick Jr. & Alice Eve's Minds. Accessed on 30.5.2017. Retrieved from https://www.youtube.com/watch?v=J94uO-urSTg

Mann, I. 2008. Hacking the human: social engineering techniques and security Countermeasures. Aldershot: Ashgate. Referenced:22.3.2015. http://www.jamk.fi/kirjasto, Nelli-portaali, ebrary.

Neuro-linguistic programming. Accessed on 10.4.2017. Retrieved from https://en.wikipedia.org/wiki/Neuro-linguistic_programming,

Pease, a. 1988. Body language (Overcoming common problems). Oxford: University Printing House.

Perez R. 30.11.2016. 60% of enterprises were victims of social engineering attacks in 2016. Accessed on 26.5.2017. Retrieved from https://www.scmagazineuk.com/60-of-enterprises-were-victims-of-social-engineering-attacks-in-2016/article/576060/

The Human Buffer Overflow. Accessed on 18.4.2017. Retrieved from http://www.social-engineer.org/framework/psychological-principles/human-buffer-overflow/

Thoughts. Accessed on 18.4.2017. Retrieved from https://mind-sets.com/info/success-conditioning/thoughts/