Social Engineering

A guide in understanding social engineering and related research

Jonas Ellefsen

s315731

2019

ACIT 4100

Research methods and Ethics

Contents

1. Introduction 4

1.2 Thesis statement 4

1.3 Rationale 4

2. Understanding social engineering 5

2.1 Techniques 6

2.1.1 Phishing 6

2.1.2 Dumpster diving 7

2.1.3 Shoulder surfing 7

2.1.4 Waterholing 7

2.1.5 Baiting 8

2.1.6 Pretexting 9

2.1.7 Piggybacking 10

2.1.8 Advanced persistent threat 10

2.1.9 Reverse social engineering 11

2.2 Channels 13

2.2.1 E-mail 14

2.2.2 Social networks 14

2.2.3 Cloud services 15

2.2.4 Websites 16

2.3 Models for classifying attacks 16

3. Research 17

3.4 Literature search 17

3.4.1 Taxonomy 17

3.1 Challenges 21

3.1.1 Psychology 21

3.1.2 Experiments 22
3.1.3 Real-world scenarios 26
3.2 Solutions 27
3.3.1 Policies 28
3.3.2 Training and education 28
4. Conclusion 29
References 30

Figures

Figure 1. 6
Figure 2. 12
Figure 3. 13
Figure 4. 16
Figure 5. 17
Figure 6. 18
Figure 7. 19
Figure 8. 19

1. Introduction

Have you ever received an email asking for your username or password, or even your credit card information? Maybe you know someone who has? In that case there's a high chance they have been exposed to a social engineering attack. In information security, social engineering is used to exploit the people using information and communications technology (ICT) systems. By using a varying set of social engineering techniques, *hackers* can get valuable information from the individuals using a targeted system. People performing malicious activities will be referred to as hackers, attackers or social engineers.

In this essay we will focus on research and literature that is already publicly available to get a complete overview of what social engineering is. The essay is divided into three sections where research methods and ethics will be taken into consideration. The first section will explain social engineering in-depth, presenting a thorough understanding of the history, the approach, and the different techniques used. The next section discusses the challenges and solutions of the topic, in light of relevant literature and research. This section also includes the taxonomy used for the literature review of this essay. The last section, the conclusion, summarizes what has been discussed in context of the thesis statement. Next, we define the thesis statement for this essay.

1.2 Thesis statement

While social engineering attacks are effective in getting user's information, researchers propose counters zeroing out the threats.

1.3 Rationale

We were asked to choose a topic within the field of our specialization. While I have chosen the specialization *Universal Design of Information and Communication Technologies*, I also have a predilection for cyber security. Thinking about those two aspects of computer science, the topic *social engineering* quickly came to mind. I presumed the topic would shine light on user interactions, as well as the user's privacy, and started looking into sources to

confirm my prediction. While doing this I came to the realization that there is quite a lot of research done in this field and decided to name it the topic of my essay.

2. Understanding social engineering

Social engineering is defined as the art of manipulating people to give away access or, confidential or private information to the social engineer. It is known to be more superior than other hacking methods, as you don't necessarily need to breach the system in order to access information (Krombholz, Hobel, Huber, & Weippl, 2015). Having a user of an ICT system reveal credential information to a hacker, can reduce the overall integrity of the system and put other users in danger. If the hacker has unlimited access to a user's profile data, they can identify as that user, asking for more information from other users or even corrupt the system. Generally, the weakest link in a system are the people who are using it (Abraham & Chengalur-Smith, 2010).

According to (Krombholz, Hobel, Huber, & Weippl, 2015) and (Thompson, 2006), Kevin Mitnick is praised as one of the best known hackers in recent time. Mitnick deceived people into giving him the information he wanted. His preferred method of social engineering was questioning, as he discovered that others believe that most people are essentially honest. Although Mitnick had expertise in computer systems, he had more success in requesting information from unknowing individuals (Thompson, 2006).

While today's social engineering is often related to computers, it does not have to do with an ICT system. In fact, social engineering techniques and philosophies was used long before the invention of hardware or software. One example, inspired by (Hasan, Prajapati, & Vohara, 2010), is the Trojan Horse story from the Trojan War where the Greeks made a wooden horse and hid a number of armed men inside of it. The Greeks pretended to retreat, and the Trojans took the horse in to the city of Troy as a monument of victory. The city was later destroyed when the Greeks ambushed them with their forces. Today, the name "Trojan Horse" is used for when a user is tricked into willingly running malware-infected software on their computer (Encyclopædia Britannica, 2019).

2.1 Techniques

Social engineering attacks have been split into four different categories, depending on their approach. The four categories are: physical, technical, social and socio technical (Krombholz, Hobel, Huber, & Weippl, 2015). All social engineering attacks are unique in their own way and have varying factors. However, literature and research have shown patterns that commonly occurs. One of the patterns has three phases: Sabotage, Advertising and Assisting (Nelson, 2001). The pattern is mostly used for reverse social engineering attacks, so we will revisit that pattern in Section 2.1.9.

A more common pattern that can be seen in most social engineering attacks, is laid out in four phases: Information Gathering, Relationship Development, Exploitation and Execution (Hasan, Prajapati, & Vohara, 2010). This pattern was made famous by Kevin Mitnick, see Figure 1.

In order to go through with a social engineering attack, there have been identified techniques to be used to obtain information. The techniques are also known as *Attack Vectors*. The most common techniques used in modern social engineering attacks are listed below.

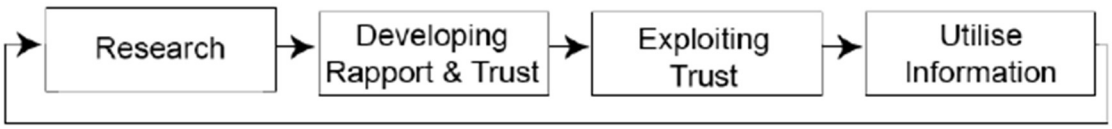

Figure 1. Kevin Mitnick's Social Engineering Attack Cycle (Mouton, Malan, Leenen, & Venter, 2014).

2.1.1 Phishing

A phishing attack is when someone attempts to acquire sensitive data through an electronic communication system, usually email and/or instant messaging, but can also be performed on other *channels* such as social networks or websites. While social engineering attacks often targets small groups of people or individuals, phishing attacks looks to target large groups of people (Krombholz, Hobel, Huber, & Weippl, 2015). In most cases phishing is done for financial gain and the theme is related to banking (Hasan, Prajapati, & Vohara, 2010). As

phishing looks to target a high number of individuals, a low percentage of successfully attempted attacks will still be profitable for the attacker.

Phishing has rapidly become one of the most common techniques of social engineering and hacking in general and is still growing each year. Circa 1.5 million new phishing sites are created every month and these looks to target both small businesses and large enterprises (Retruster, 2019).

Spear phishing

A more thought out process of phishing attempts is called spear phishing. It uses the same principle as phishing, but targets a smaller group of people, often within a particular company. If the idea is to target a company, the attacker collects data from publicly available sources, such as a company's website, and constructs a trustworthy email from the information they have gathered (Krombholz, Hobel, Huber, & Weippl, 2015).

2.1.2 Dumpster diving

In the context of information technologies (IT) and social engineering, dumpster diving is the process of looking through trash cans, garbage containers and paper bins to find useful information such as access cards, identification papers or corporate documents. It could also mean searching through discarded digital data on hard drives or other storage media (Technopedia, 2019). The information can be used to compromise a specific system or user account (Krombholz, Hobel, Huber, & Weippl, 2015).

2.1.3 Shoulder surfing

Shoulder surfing is the process of observing someone's actions. Often includes looking at someone's screen or keyboard while they are typing sensitive information. As the name suggest, the technique mostly includes looking over someone's shoulder (Krombholz, Hobel, Huber, & Weippl, 2015). This social engineering technique especially focuses on stealing confidential information such as passwords, PIN codes or credit card number. The goals for shoulder surfing are, in most cases, financial gain or identity theft (Symanovich, 2019).

2.1.4 Waterholing

As with shoulder surfing, the Waterholing technique is named very logically. In the wild, predators stay close to the watering holes their prey is known to visit. The predator is

waiting at the water hole for an opportunity to strike. In a Waterholing attack the attacker are looking to infect a website that the targeted user, the prey, is likely to have interest in (TechTarget, 2019). As the Mitnick Attack Cycle suggests, see Figure 1, the attack require some research and setup. The attacker needs to identify the websites that are of interest to the victim. This can be done by using other, more traditional hacking methods, such as to track or monitor someone's Internet traffic or browser history.

In recent years, waterholing, alongside spear-phishing attacks, has been the primary social engineering techniques to target larger corporations. The attackers expect employees to visit their company's websites, thus it makes sense to infect those specific sites (Krombholz, Hobel, Huber, & Weippl, 2015).

2.1.5 Baiting

The technique known as *baiting* can have different approaches in the world of social engineering. A physical approach is when a malware-infected storage medium, e.g. a USB drive, is placed in a location where the targeted person is likely to find it (Krombholz, Hobel, Huber, & Weippl, 2015). As with all social engineering techniques we have mentioned this far, there are examples of the baiting-technique being showcased in media. The first one that comes to mind, is a scene from the TV-show Mr. Robot (Esmail, 2015) where a malware-infected storage medium is left on the parking lot of a security company. One of the employees of the company gets tricked into taking the storage medium. He then connects it to his computer. The attacker has succeeded in accessing the system.

USB sticks laying on the ground in the middle of a parking lot. Scene from Mr. Robot (Esmail, 2015).

A different approach of baiting is *technical*. It involves a website or application offering something in exchange for confidential information, such as login credentials or other private data. In the online world social engineers can trick the users into downloading a movie or music for free, clicking enticing ads offering access to streaming services or gifts and prices, or following links prompted from a pop-up window. If the user bites, they may get redirected to a malicious website or install unwanted software on their system (Brunau, 2019).

2.1.6 Pretexting

Pretexting is a technique where the social engineer creates a false sense of trust towards the victim. It can be done by pretending to be someone else, or impersonating a friend, relative, colleague or boss of the victim. Pretexting is often done on Social Networking Services (SNS) where the attacker creates a fake profile of the person they are trying to impersonate. In the process of making a fake profile, the attacker needs to find valuable information such as pictures, names and birthdate of the person they are impersonating. Who the attacker chooses to impersonate depends on what information they are searching for. Whoever they are trying to impersonate, the legitimacy of the scam is key (Algarni & Xu, 2013).

A lot of techniques can be used to establishing trust in a targeted victim. If a pretext is well thought out and well executed, it could be a simple step to gain the trust of the victim (Mouton, Malan, Leenen, & Venter, 2014).

2.1.7 Piggybacking

Piggybacking, also known as *tailgating*, is used to breach security and can have a technical or physical approach. In general, piggybacking is the act of accessing a restricted area without authorization. Authorization can be done in multiple ways, such as knowing a password, having an access card or identification badge, or biometrical authorization such as fingerprint or face id. The most common physical approach of piggybacking is by following an employee of a company to the restricted area, pretending to be someone legitimate like a colleague (Krombholz, Hobel, Huber, & Weippl, 2015).

In a technical approach such as in an electronical system or an ICT system, a user does not properly log off the device they are using leaving it free to use for an unauthorized individual. Another example is a *piggybacked software* where the user gets lured into installing some software containing spyware which will monitor the system they are using (Hasan, Prajapati, & Vohara, 2010).

2.1.8 Advanced persistent threat

Advanced persistent threat (APT) often rely on other social engineering techniques such as (spear-)phishing and waterholing. The technique is intended to compromise a system within a business or enterprise (Krombholz, Hobel, Huber, & Weippl, 2015). The attacker needs to get access to the system through the methods mentioned and will have to do surveillance on the company's networks. APTs are not intended to cause any harm to or corrupt the system. Instead it focuses on stealing data. However, if the attacker gets hold of a lot of data, it may lead to a potential data breach and the attacker can take control of the system (Lord, 2018). APTs require a lot of planning, research and setup in order to be successful.

Like APTs, the last social engineering technique we will explain in this essay, reverse social engineering, also requires a lot of setup to be successful.

2.1.9 Reverse social engineering

The general idea of reverse social engineering (RSE) is that the social engineer does not initiate to contact the targeted victim. Instead, the victim is tricked into contacting the attacker. This often results in the victim having a lot of trust in the attacker. Once they have established a friendly relationship the attacker can initiate the attack on the victim.

RSE is similar to other social engineering techniques, as it uses the same pattern suggested by Mitnick in achieving its goals, see Figure 1. However, (Nelson, 2001) describes the process of RSE in three phases: sabotage, advertise and assist. In order to succeed in conducting an RSE attack, the attacker needs to corrupt or sabotage the system the targeted victim is using in some way. So far we have discussed multiple ways of accessing, infecting or monitoring ICT systems using social engineering techniques. The next phase is advertising. In this phase it is important that the attacker is believed to be a legitimate individual that later can assist the victim. Usually the attacker has gained the trust of the victim through different processes and is trusted as a system administrator or another IT competent person that can assist the victim. If successful the attacker can ask for valuable information such as login credentials to "fix" the problem and might be asked to help the victim at a later time (Krombholz, Hobel, Huber, & Weippl, 2015). RSE is a great way of getting a lot of information from the targeted victim and is very rewarding in the end. It requires a lot of preparation and must be cautiously set up (Gragg, 2002). While there is currently little research done on online RSE compared to other attack vectors, research *has* been done on RSE methods used in social networks.

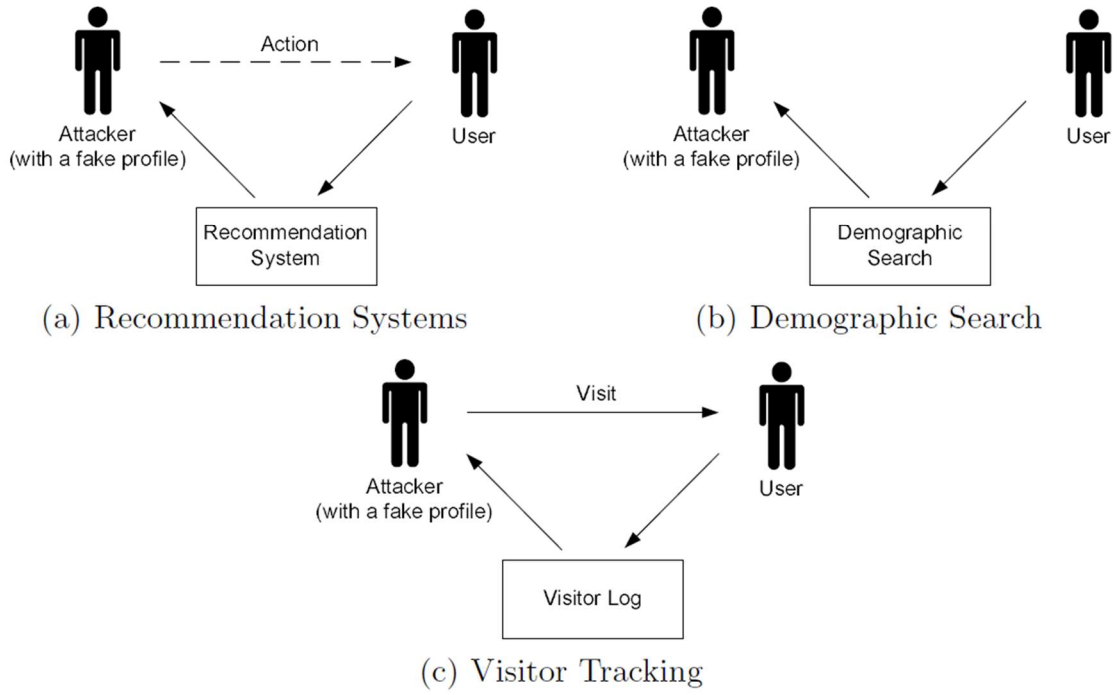

Figure 2. Different types of reverse social engineering attacks (Irani, Balduzzi, Balzarotti, Kirda, & Pu, 2011).

Figure 2 shows three types of approaching RSE in the context of social networks and makes the attacker eligible to execute an RSE attack. In short, (a) is used to exploit the friend recommendation system in popular social networks, (b) aims to attract the attention of users with the same interests and preferences as a generated fake profile and (c) aims to trigger the interest of the target by browsing their social network profile (Irani, Balduzzi, Balzarotti, Kirda, & Pu, 2011). To see how experiments are conducted, see Section 3.2.1.

Today, most social engineering attacks strongly relies on some kind of pretexting. Research has shown that impersonating an existing friend of the targeted victim increases the level of trust online. Because of this, RSE attacks are very attractive in SNS as the social engineer must create a profile, which can be seen as a *persona*, and has great potential to reach a large number of registered users of the system. The goal is to have the victims reach out to the engineer, which makes the attack less suspicious and tends to have more success (Irani, Balduzzi, Balzarotti, Kirda, & Pu, 2011).

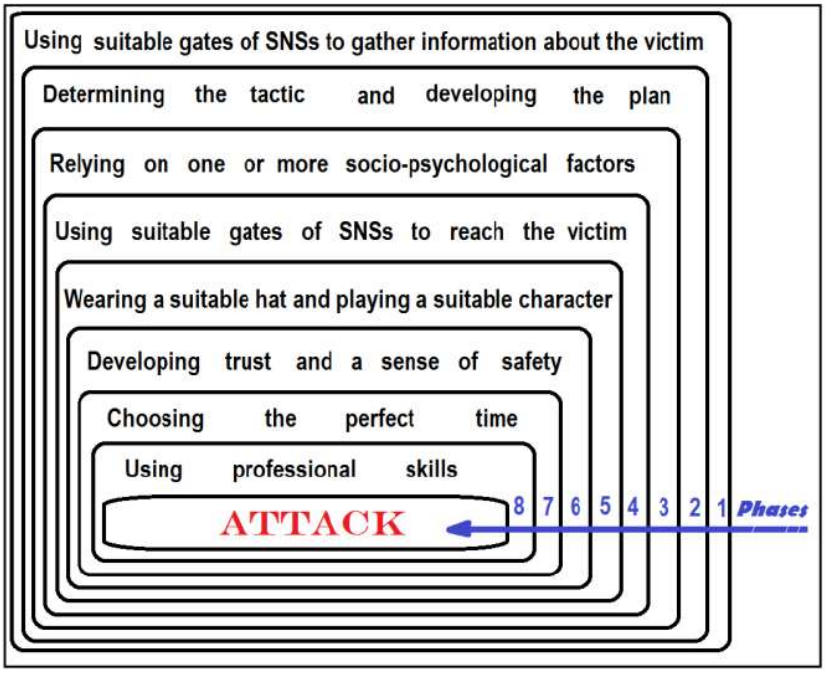

Figure 3. Eight phases social engineers in SNS need to go through to lure the victim (Algarni & Xu, 2013).

2.2 Channels

In our everyday life we are communicating on a wide range of different channels. Both in our private lives and in working environments we are using communication channels such as email and social networks including Facebook, Twitter and LinkedIn. Today's society are depending on us to be highly flexible and available at all times, on all channels (Krombholz, Hobel, Huber, & Weippl, 2015). It is important to note that even though you have created a large number of different accounts on different channels, they are all connected to you. Many believe that their private and professional digital lives are completely separate, but the fact of the matter is that they are indeed connected. People are using their corporate email on their mobile devices no matter what environment they are in, and are indeed using their Facebook while at work (TEDx Talks, 2019).

In recent years there's been a big increase in people working from home, which makes people rely more on cloud-based services, as well as instant messaging and email to make data available to co-workers through online channels. The number of people working remotely has increased by 140 percent (%) since 2005, including full-time employees and part-time workers (Milenkovic, 2019). As the use of online communication channels have become more and more common, and people are free to publish as they like on these

platforms, there have been very little focus on security and privacy. Most people trust their online counterparts (the people they meet online), although they are only identified by an email address, a virtual profile or a nick (Krombholz, Hobel, Huber, & Weippl, 2015). Social engineering software is being sent to users through a variety of channels, which includes e-mail, social networks and software, along with storage media and websites (Abraham & Chengalur-Smith, 2010). See Figure 4 for an overview.

2.2.1 E-mail

Some of the most popular e-mail services to date are Gmail, Outlook and Yahoo Mail (ShuttleCloud, 2016). E-mail is by far the most commonly used communication channel, and thus the most popular medium used by social engineers and cybercriminals to target victims with malicious intent. It is also the biggest platform for phishing attacks (Abraham & Chengalur-Smith, 2010).

2.2.2 Social networks

There is a large variety of social networking services (SNS) who all share common features. Popular SNS such as Facebook, Instagram, Twitter and LinkedIn are being used for communication; instant messages, text messages and on-site messages, and used to share web content including links, blog posts, news and photos (Kallas, 2019). Social networks are generally used to share personal, and sometimes sensitive, information with peers. Most SNS require the user to create an account in order to access the information (Weir, Toolan, & Smeed, 2011). As SNS are huge information-sharing platforms with a lot of possibility for users to tie relationships with other, it makes for a great place for social engineers to harvest sensitive information. The opportunity of creating fake user profiles and hide their identity in a free online environment, results in social engineers using SNS as a common platform for performing social engineering attacks (Krombholz, Hobel, Huber, & Weippl, 2015).

Research done on SNS show that the use of social engineering will continue to increase in the future. The SNS providers and the social engineers exploiting the SNS have one thing in common: they value the information published by the users. While social engineers look to use the information for malicious intent, the providers of the SNS use this information for marketing and advertisement purposes. Although there is awareness about information

being misused, the providers still encourage their users to share personal data (Algarni & Xu, 2013).

Fake user profiles

Upon creating a SNS profile the social engineer can freely choose what *character to play*. They can create any persona they feel like, and choose whatever picture, name, biography and characteristics to describe themselves (Algarni & Xu, 2013).

There are sophisticated methods towards making trusted profiles within social networks. *Profile-cloning attacks* and *cross-profile cloning attacks* looks to identify already existing profiles and remake them in attempt to seem legitimate. In cross-platform cloning the attacker looks to seek out a user's account on multiple platforms and see if the profile exists. The attacker might find two persons: Person A and Person B. The attacker discovers that Person A has a LinkedIn profile and no Facebook profile. Person B has a Facebook account and no Twitter account. The attacker can copy the profile information from one SNS and create a new profile on another, cloning the user profile of another individual. The user profiles seem legitimate and the attacker can start harvesting information on the new profiles (Krombholz, Hobel, Huber, & Weippl, 2015).

2.2.3 Cloud services

Some popular cloud services are Amazon Web Services, Microsoft Azure, IBM Cloud and Dropbox (Software Testing Help, 2019). The use of cloud services has become more frequently used due to the increase of people working remotely. In a company, workers store information on a cloud as back-up or as a medium for sharing files with their co-workers. The level of trust among users of cloud services are often higher than what companies desire.

The most common attacks on cloud services are spear-phishing and Advanced Persistent Threats (Krombholz, Hobel, Huber, & Weippl, 2015). If social engineers get unauthorized access to services such as Dropbox they may share malicious files with other users which can harm their system. Alternatively, they can access confidential or sensitive information.

2.2.4 Websites

In social engineering, websites are used as *water holes* and mediums for downloading malicious software, get login IDs such as usernames or email addresses, and steal passwords from user input. A hacker can copy the content and appearance of a website by accessing the *source code*. It may look the same as another website, but it can run scripts monitoring the user's activity. Users are often redirected to malicious websites from phishing e-mails (Abraham & Chengalur-Smith, 2010).

2.3 Models for classifying attacks

Figure 4 shows the different aspects in social engineering attacks such as targets, attack vectors or techniques, and on what channel they are performed.

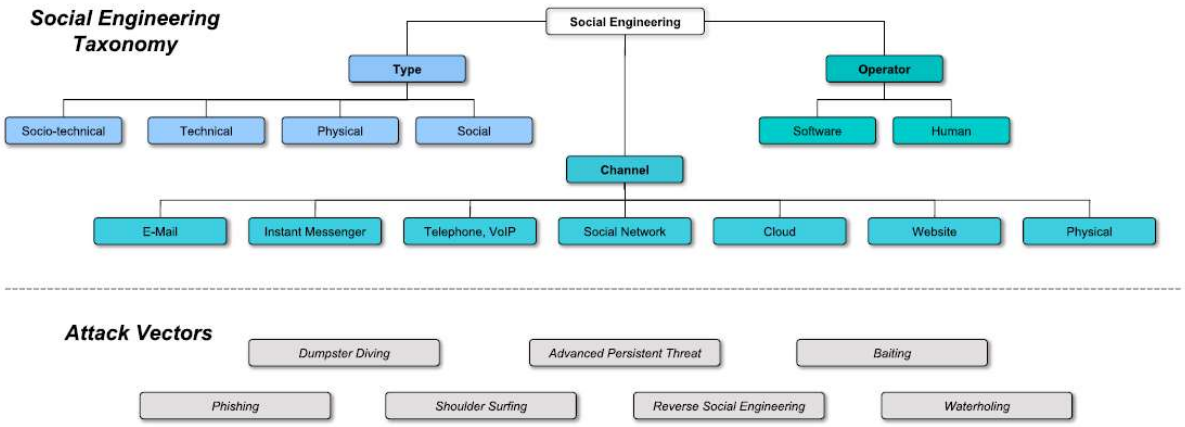

Figure 4. Overview of classification of attack characteristics and attack scenarios (Krombholz, Hobel, Huber, & Weippl, 2015).

In Figure 5 the authors have created a relational model of displaying how a social engineering attack can be conducted. An attack can use different principles and use multiple techniques.

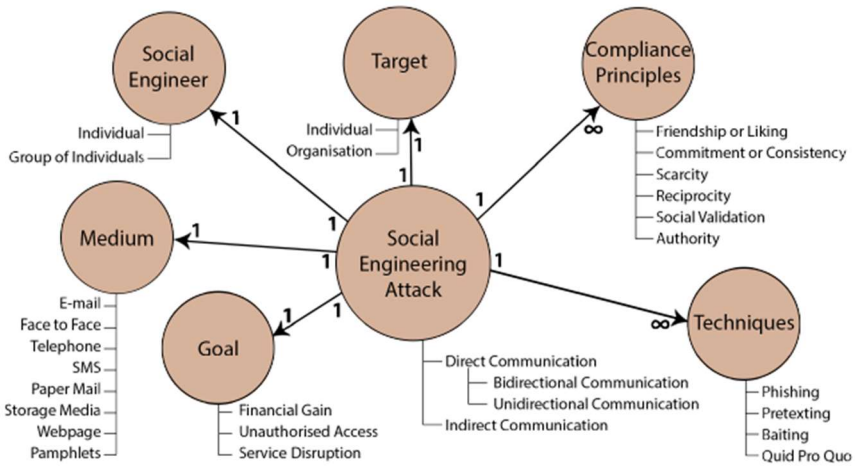

Figure 5. An Ontological Model of a Social Engineering attack (Mouton, Malan, Leenen, & Venter, 2014).

3. Research

In this section I will discuss the research done on the topic, and its subcategories. I will explain the literature search going into this essay, carry out the taxonomy and look at trends in the field of social engineering. Then, look at what has been discovered in terms of research on social engineering. Lastly, the challenges and solutions will be considered.

3.1 Literature search

The literature search was done looking at relevant literature and research available online. The main keyword while searching through the literature was “social engineering”. During the literature search I identified sub-topics that shines light on the different aspect of the main topic. The sub-topics identified were: *Reverse social engineering, counters to social engineering, social networking and online privacy*. We were recommended to use Oria, Scopus and Google Scholar to seek out papers related to the topic. For this essay, Google Scholar was solely used when performing the online literature search. After finding a number of papers, I looked into citations to see if there was a pattern in other papers being citated. If so, they were added to the list of literature. For sorting out the literature that had been found, a taxonomy was created.

3.1.1 Taxonomy

There was a total of 21 papers carried out from the literature search. To get a clear overview of the literature I used a taxonomy created in a spreadsheet (see Table 1). In doing this I

could see patterns in the literature, such as the separation of the main topic from sub-topics (see Figure 6) and what year the papers were published (see Figure 7). The distribution of the topics was meant to give us a general idea of what the contents of the paper were. All papers had to do with the same topic, social engineering, but the focuses and approaches were different.

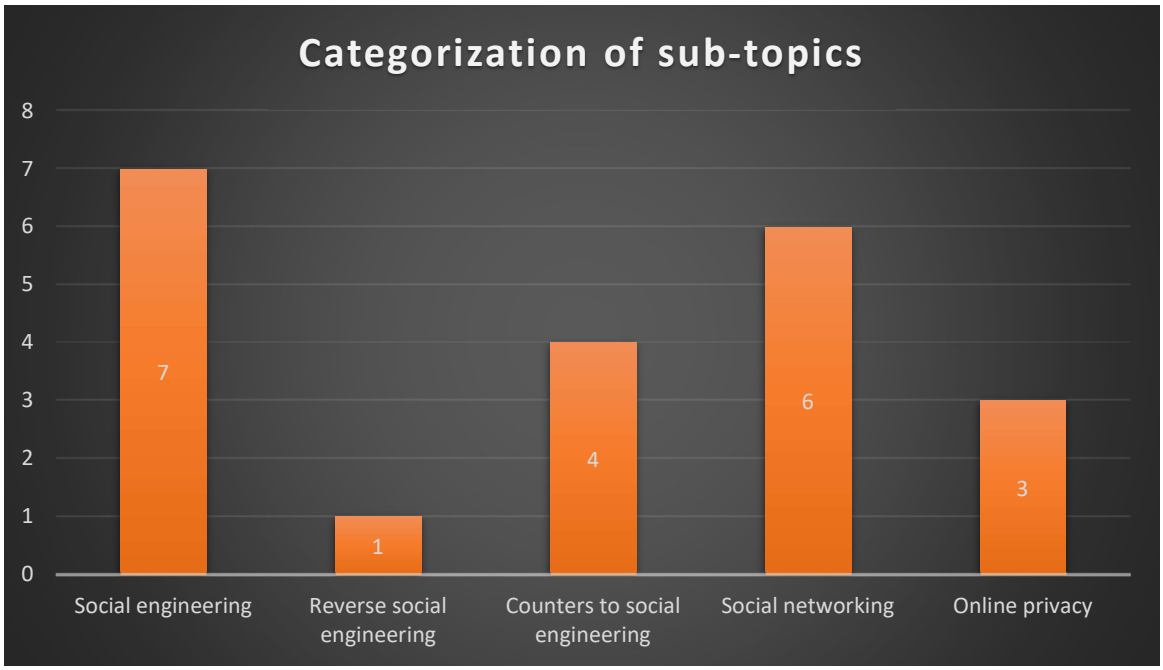

Figure 6. Number of papers categorized by topic. Based on the taxonomy.

The methods used in the various papers had a common theme. Most of the time the authors had carried out or referred to experiments to find the results. The majority of the papers were case studies, followed by user studies. These kinds of studies focus on identifying a case and analysing how users tend to interact with or solve the cases (Heale & Twycross, 2017).

While these studies used experiments in finding results, other studies relied on different research methods. These methods include prototyping through creating ideas and design or listing suggestions for improvements. A list of suggestions was mostly used for studies on counters to social engineering.

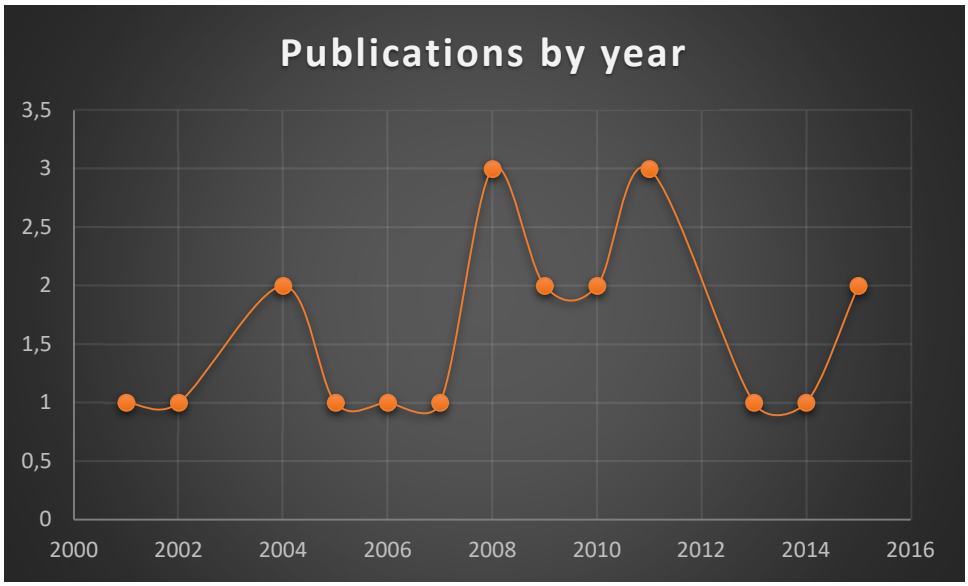

Figure 7. Shows how frequently the papers were published per year. Based on the taxonomy.

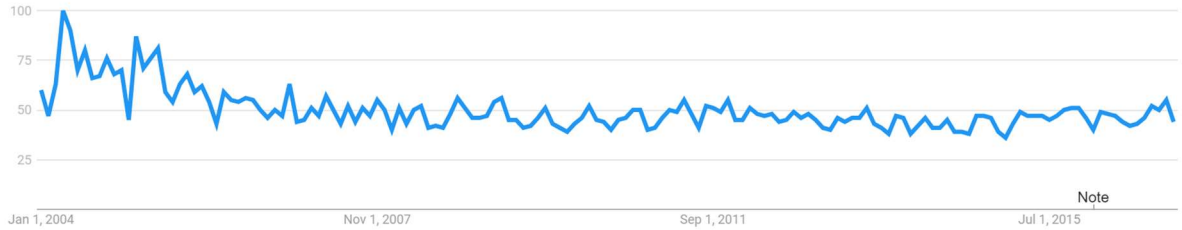

Figure 8. Web search for "Social engineering" worldwide from 2004-2016. Shows interest over time. Retrieved from https://trends.google.com/trends/explore?date=2004-01-01%202016-12-12&q=%2Fm%2F036d5r.

I wanted the taxonomy to include approximately 20 papers as it gives a general idea of the research of the topic and is a sufficient amount of papers in identifying patterns. Table 1 shows all categories in the taxonomy and the information used to easily identify each paper.

In creating and put forward a taxonomy, patterns were identified more easily, and the contents of each paper were not as hard to remember.

Figure 7 shows that the latest articles were published in 2015. When looking at more recent papers, it shows that they have a lower amount of citations than the papers used in the taxonomy. Low citations make the article less trustworthy as the authenticity may vary. Speaking of trust, some of the papers put forward in the taxonomy were more convincing than others. There was a clear difference in time put in to and amounts of research done when comparing one paper to another.

When comparing Figure 7 and Figure 8, we see the graphs for publications and interest in search have completely different peaks. Figure 7 shows peaks in the years 2008 and 2011. In Figure 8 however, the peak was in 2004. Until 2016 the graph has stayed fairly consistently at sub 60%. Although the relevance of this comparison can be discussed, we see that there has not been a high interest commercially for social engineering in more recent years. This could tell us that the general public is not as educated on this topic and has a higher chance of being the victim of an attack.

Table 1. Stripped down version of the taxonomy. The table shows extracted information from each article categorized from the taxonomy.

Taxonomy	
Categories	**Information**
Title	The title of the article
Authors	All authors involved in writing the article
Venue	Journal Conference Workshop Book chapter
Year	In what year the article was published
Topic/category	The focus element or approach of the article
Type of study	User study Case study Security related
Method	Experiments Ideas and design Real life case study List of suggestions
Sentiment	Enthusiastic Informative

	Curious Sceptical
Field	Computer security Human interaction
Summary	The problem, why we should care, what the authors do and the conclusion.

3.2 Challenges

From the taxonomy I identified a general problem proposed by the authors of the articles, regarding social engineering: Computers rely on a human operator and the human mind is easily manipulated. The social nature is to trust one another, which is exploited by social engineers, and is why social engineering continue to exist. Daily, we are facing the problem known as hacking. But because of the detailed research and studies we have been become more familiar with unsolicited messages such as spams and scams. The constant increase in use of social networks has emerged a serious threat in users' privacy. Their personal information is being misused without them even knowing! The growing implications are often overlooked and the social engineering attacks, especially in social networks, have not received any attention.

In this section we will look further into the challenges of social engineering, looking at human behaviour and experiments, and how it impacts us in real life.

3.2.1 Psychology

Research shows that people are known to believe they are good at detecting lies and persuasions, but the fact is that they are performing poorly in doing so (Huber, Kowalski, Nohlberg, & Tjoa, 2009). People have certain characteristics that can be taken advantage of and may react differently depending current emotional state. Social engineers can capitalize on these factors by using personal persuasion and guilt (Nelson, 2001). Using strong emotions may limit the victim's ability to evaluate or think of a counterargument in a certain situation. While being addressed, an individual may be diffusing their responsibility or take a *mental shortcut* to avoid conflict (Gragg, 2002).

There are certain groups employees whose job is to provide others information. People working as support, helpdesk personnel or library staff are often willing to freely give out

information. Per today, there is very little research done on social engineering towards certain groups, such as library staff.

A practical example on social engineering in the context of libraries:

“

Marcy works as a librarian answering calls at the reference desk.

One day *Dave Simpson* from the information services calls. He is saying the branches have been experiencing network problems over the last few days and wants to know if there have been any problems at the library.

Marcy says that everything has been working fine, however, Dave would like Marcy to run some tests to confirm. He then asks her to log off the system, and log in once over. While logging in, Dave asks what username they are using at the reference desk. *Searef*, says Marcy.

Dave explains that kids have been trying to hack into the system and would like Marcy to change the password of the profile they are using. *If you’re uncertain how to change the password, don’t worry, I will talk you through it*, Dave adds. He then tells Marcy to use a secure password and suggests the password *5eaR3f*.

Dave tells Marcy to pass the new password on to the other reference personnel and not to give it to anyone who does not need it. *Have a great day*, he says and hangs up.

“

(Thompson, 2006)

3.2.2 Experiments

Experiments done on social engineering use different methodology, depending on what they are trying to achieve. Therefore, the results may differ. The researchers may be looking to identify the level of trust of the users, what the targeted user groups are, attack vectors used by social engineers, availability of information, user-interaction with ICT systems, and integrity of systems.

Now, we will look at three experiments documented in some of the papers from the taxonomy.

Article: Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression (Livingstone, 2008).

The goal of the experiment carried out by (Livingstone, 2008) was to see how young teenagers express themselves on and interact with SNS. The experiment was done in the participants' homes and used SNS that they were already familiar with and used on a daily basis. Table 2 shows the details of the participants. The participants were given pseudonyms to stay anonymous, but had to quote their name, socioeconomic status and the SNS they used.

The experiment showed that the younger users tend to create a more *superficial* online profile that the older ones. In the article they state that the younger ones tend to "recreate a highly-decorated, statistically-elaborate identity" whereas the older ones favour a plain aesthetic. Users expressed that they tend to leave SNS when upset and prefer instant message such as MSN over SNS for conversations.

Table 2. Participants' details in experiment (Livingstone, 2008).

	GENDER	
SCHOOL YEAR	GIRLS	BOYS
Year 9	Danielle, 13, C1, Piczo Nicki, 14, AB, MySpace Daphne, 14, C2, MySpace, Bebo, ex-Piczo Jenny, 14, DE, MySpace, Bebo Elena, 14, DE, MySpace, Facebook, Bebo	Paul, 13, C2, Bebo, ex-MySpace Joshua, 14, AB, Facebook Billy, 14, C2, MySpace
Year 10	Ellie, 15, AB, Facebook, ex-MySpace,	Ryan, 15, C1, Bebo, MySpace, ex-Piczo
Year 11	Nina, 15, C1, Facebook, ex-MySpace Sophie, 16, C2, MySpace	Leo, 16, AB, MySpace Danny, 16, C1, MySpace, Facebook Simon, 16, DE, MySpace Jason, 16, DE, MySpace

The author does not express why she included socioeconomic status as a part of the details. I myself, am uncertain whether the status should be stated or not. If anything, it may seem

offensive towards a participant being identified with a lower socioeconomic status than a peer.

Article: College students' social networking experiences on Facebook (Pempek, Yermolayeva, & Calvert, 2009).

The next paper was conducted by (Pempek, Yermolayeva, & Calvert, 2009) and the primary goal was to "describe how much time college students use social networking websites, why they use them and how they use them (i.e. to observe/lurk, create, or interact)" (Pempek, Yermolayeva, & Calvert, 2009). The participants stayed completely anonymous throughout the experiment. In total there were ninety-two participants, sixty of those were female. The mean age of the participants was 20.59 years, and the participants had mixed cultural backgrounds. All participants were from a private university that had not been named.

During a 7-day period the participants needed to document their use of Facebook as well as completing checklists. After one week they were given a survey about their Facebook use.

The results varied greatly. On weekdays the use of Facebook ranged from 2 minutes to 117 minutes per day, in the weekend (Saturday and Sunday) it ranged from 0 to 165 minutes per day. In short, the participants used Facebook as channel to communicate with their friends and to establish a personal identity. The participants stated that what they found most interesting about Facebook was:

- Reconnecting with their friends
- Learning information about others
- The possibility of Facebook addiction
- Self-presentation

Article: The Urgency for Effective User Privacy-education to Counter Social Engineering Attacks on Secure Computer Systems (Orgill, Romney, Bailey, & Orgill, 2004).

The experiment in this article is focusing on social engineering and a potential counter, rather than social networks as the two previous ones. The experiment was carried out by (Orgill, Romney, Bailey, & Orgill, 2004) due to the lack of material regarding auditing against social engineering. The experiment was divided into several phases: the *pre-audit phase*, the *intelligence gathering phase*, the *physical access phase* and the actual *audit*. There was

assigned one auditor with a single purpose; “to determine the ease with which a social engineer could obtain information giving him unauthorized access to a network“ (Orgill, Romney, Bailey, & Orgill, 2004). The auditor was only aided with the company’s policies and procedures.

During the process the auditor used the company’s websites to become familiar with the employees in the IT department. He learned to dress in the same manner as the other employees, and while getting to know the facilities and offices he found an employee name badge at a unattended workstation. The auditor even conducted a survey to harvest information about the computer systems, see Table 3. The auditor gained the trust of his peers by conversating and building relationships. He also observed the office areas in the hopes of finding information such as passwords written on post-it notes. For the results of the survey see Table 4.

Table 3. Social Engineering Survey provided in experiment (Orgill, Romney, Bailey, & Orgill, 2004).

Number	Question
1	Name:
2	Username:
3	Password:
4	When did you last change your password?
5	Does your password meet with company standards (containing upper/lower case letter and something other than a letter?
6	Has any other Computer Support employee asked you for your password?
7	If so, when?
8	Do you lock your computer whenever not at workstation?

The survey had a total of 32 respondents belonging to different departments of the company. Department B, D and F had no problem sharing their confidential information, while Department A, C and E were far more cautious in giving out information. The auditor stated that building relationships was an important part of gaining the trust of the employees. Knowing and using the names of the authority in the organization also helped the audit in building relationship with the other employees. The bottom line of this

experiments is that using social engineering techniques has a strong effect in gaining unauthorized access. Only a small part of the organizations' employees refused to or hesitated to complete the survey. Some reported the audit to their supervisor, but the majority had no problem completing the survey or recognize the audit. The audit managed to get huge amounts of information as well as getting access to the organizations' facilities.

Table 4. Results of Survey provided in experiment (Orgill, Romney, Bailey, & Orgill, 2004).

Department	Surveyed	Username	Password	% Username	% Password
A	5	3	2	60.00	40.00
B	4	4	4	100.00	100.00
C	3	2	1	66.67	33.33
D	1	1	1	100.00	100.00
E	2	1	0	50.00	0.00
F	1	1	1	100.00	100.00
G	8	8	6	100.00	75.00
H	8	6	4	75.00	50.00
Cumulative	32	26	19	81.25	59.38

3.1.3 Real-world scenarios

In this section I will describe examples from real-world scenarios where social engineering attacks have been used successfully executed. Techniques such as spear-phishing, pretexting and waterholing have been used in these scenarios.

RSA, 2011

A small group of employees working in the security company RSA, had been sent an e-mail containing an Excel attachment, namely "2011 Recruitment Plan". The e-mail looked convincingly legitimate. However, the attachment contained malware installing a backdoor on the receivers' systems. The attack compromised several machines in the local network (Krombholz, Hobel, Huber, & Weippl, 2015). The exploit costed the company 66 million dollars (Gatefy, 2019).

Apple and Facebook, 2013

A *Java* vulnerability was exploited to infiltrate both Apple's and Facebook's internal networks. A website used by many iOS application developers, "iPhoneDevSDK", was

compromised, redirecting users to water holes causing harm to their systems. The users were connected to their corporate networks, resulting in all devices running on the system being affected by the attack (Krombholz, Hobel, Huber, & Weippl, 2015).

Ethereum Classic, 2017

Ethereum Classic is defined as "a decentralized platform that runs smart contracts: applications that can be run exactly as programmed without any possibility of downtime, censorship, or third party interference" (Ethereum Classic, 2019). In 2017 the website was compromised when social engineers used pretexting to impersonate one of the owners. The attackers gained access to the domain registry, enabling them to complete transactions from the users' profiles (Gatefy, 2019).

Large organizations' ICT systems seem to have a number of security mechanisms to protect the security of their platform and the privacy of their users (Huber, Kowalski, Nohlberg, & Tjoa, 2009). The real-world scenarios show that social engineering is the most successful, and most efficient strategy in compromising large organizations. They also show that the superior channels to perform social engineering are e-mail and websites (Krombholz, Hobel, Huber, & Weippl, 2015).

In the next section we will look at solutions to effectively protect computer systems against social engineering attacks.

3.3 Solutions

The challenges discussed in Section 3.1 show that social engineering can lead to financial harm, identity theft and loss of information. This will affect individuals as well as enterprises and organizations of all sizes. To prevent social engineering attacks from happening, researchers have proposed countermeasures. Looking back at Figure 6 the literature categorized as *social engineering, reverse social engineering* and *counters to social engineering* all put forward suggestions to prevent social engineering attacks. Two countermeasures that are frequently mentioned in preventing attacks, are policies and education.

3.3.1 Policies

Having well-defined policies in an organization clarifies what information can be passed on and to whom. It eliminates the decision-making whether an employee should reveal some information or not. Having awareness-programs helps employees in identifying potential threats and detecting lies or persuasions (Thornburgh, 2004). Procedures such as an authentication system should be implemented. Using smart cards or tokens, or even biometrics to identify users in ICT systems or in facilities, protect against many social engineering threats (Hasan, Prajapati, & Vohara, 2010). In a company, the employees must be familiar with the policies, but also clients and others who sits on corporate information (Nelson, 2001).

Policies should be easy to remember, especially for when employees are communicating via e-mail or phone calls. (Thompson, 2006) suggests a list of basic guidelines for protecting against social engineering:

- Be suspicious when being asked about employees or technical information.
- Do not provide passwords or login names over the phone or via e-mail no matter who's asking.
- All employees must carry proper identification when present.
- When unsure about legitimacy of a request, contact proper authorities.
- Trust your instincts.
- Document and report suspicious communications.

3.3.2 Training and education

To effectively understand and know how to counter such attacks, there must be focus on staff training and education. Education on social engineering should include learning models (e.g. Figure 4 and Figure 5), basic psychology and methods of persuasions (Krombholz, Hobel, Huber, & Weippl, 2015). All users of ICT systems should be aware of common methods of social engineering attacks and cautious of who to trust.

"Once businesses start taking social engineering seriously and applying the social sciences to protect against this threat with a multi-layered defence, social engineering will become a much more difficult, if not impossible, avenue for a hacker to employ" (Gragg, 2002).

4. Conclusion

In this essay, I have described the different factors for understanding social engineering and how social engineers conduct their attacks. I have put forward the conflict between social engineers and society by listing the challenges individuals and organizations might be facing. Based on relevant literature conducted in a literature search, I have proposed solutions in which social engineering can be countered. In conclusion, social engineering is a relevant part of most people's life. It is a threat that all people should be aware of and know how to counteract. This essay shows that there has been done a lot of research in this field, but the importance of social engineering encourages even more studies to be done. The best way to counter social engineering is to inform more people about it and to educate users of ICT systems on the topic.

References

Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, 183-196.

Algarni, A., & Xu, Y. (2013). Social engineering in social networking sites : phase-based and source-based models. *International Journal of e-Education, e-Business, e-Management and e-Learning*, 456-462.

Brunau, C. (2019, September 19). *5 Types of Social Engineering Attacks*. Retrieved from datto: https://www.datto.com/uk/blog/5-types-of-social-engineering-attacks

Encyclopædia Britannica. (2019). *Trojan horse*. Retrieved from Encyclopædia Britannica: https://www.britannica.com/topic/Trojan-horse

Esmail, S. (Director). (2015). *Mr. Robot* [Motion Picture].

Ethereum Classic. (2019). *Ethereum Classic*. Retrieved from Ethereum Classic: https://ethereumclassic.org/

Gatefy. (2019, October 1). *7 real and famous cases of social engineering attacks*. Retrieved from Gatefy: https://gatefy.com/posts/7-real-and-famous-cases-social-engineering-attacks/

Gragg, D. (2002). *A Multi-Level Defense Against Social Engineering.* SANS Institute .

Hasan, M., Prajapati, N., & Vohara, S. (2010). Case study on social engineering techniques for persuasion. *International journal on applications of graph theory in wireless ad hoc networks and sensor networks (Vol. 2)*, 17-23.

Heale, R., & Twycross, A. (2017). *What is a case study?* Retrieved from BMJ Journals: https://ebn.bmj.com/content/21/1/7

Huber, M., Kowalski, S., Nohlberg, M., & Tjoa, S. (2009). Towards Automating Social Engineering Using Social Networking Sites. *International Conference on Computational Science and Engineering*, 117-124.

Irani, D., Balduzzi, M., Balzarotti, D., Kirda, E., & Pu, C. (2011). Reverse social engineering attacks in online social networks. In T. Holz, *International conference on detection of intrusions and malware, and vulnerability assessment* (pp. 55-74). Berlin: Springer.

Kallas, P. (2019, September 2). *Top 15 Most Popular Social Networking Sites and Apps [2019]*. Retrieved from Dreamgrow: https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and applications*, 113-122.

Livingstone, S. (2008). Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society 10*, 393-411.

Lord, N. (2018, September 11). *What is an Advanced Persistent Threat? APT Definition*. Retrieved from Digital Guardian: https://digitalguardian.com/blog/what-advanced-persistent-threat-apt-definition

Milenkovic, M. (2019, October 28). *The Ultimate List of Remote Work Statistics – 2019 Edition*. Retrieved from smallbizgenius: https://www.smallbizgenius.net/by-the-numbers/remote-work-statistics/

Mouton, F., Malan, M. M., Leenen, L., & Venter, H. S. (2014). Social engineering attack framework. *2014 Information Security for South Africa* , 1-9.

Nelson, R. (2001). *Methods of hacking: Social engineering.* Institute for Systems research.

Orgill, G. L., Romney, G. W., Bailey, M. G., & Orgill, P. M. (2004). The Urgency for Effective User Privacy-education to Counter Social Engineering Attacks on Secure Computer Systems. *Proceedings of the 5th conference on Information technology education*, 177-181.

Pempek, T. A., Yermolayeva, Y. A., & Calvert, S. L. (2009). College students' social networking experiences on Facebook. *Journal of Applied Developmental Psychology*, 227-238.

Retruster. (2019). *2019 Phishing Statistics and Email Fraud Statistics*. Retrieved from Retruster: https://retruster.com/blog/2019-phishing-and-email-fraud-statistics.html

ShuttleCloud. (2016, August 11). *The Most Popular Email Providers in the U.S.A.* Retrieved from ShuttleCloud: https://blog.shuttlecloud.com/the-most-popular-email-providers-in-the-u-s-a/

Software Testing Help. (2019, December 8). *15 Top Cloud Computing Service Provider Companies*. Retrieved from Software Testing Help: https://www.softwaretestinghelp.com/cloud-computing-service-providers/

Symanovich, S. (2019). *What Is Shoulder Surfing?* Retrieved from Lifelock: https://www.lifelock.com/learn-identity-theft-resources-what-is-shoulder-surfing.html

Technopedia. (2019). *Dumpster Diving*. Retrieved from Technopedia: https://www.techopedia.com/definition/10267/dumpster-diving

TechTarget. (2019). *watering hole attack*. Retrieved from SearchSecurity: https://searchsecurity.techtarget.com/definition/watering-hole-attack

TEDx Talks. (2019, February 13). *Cyber security | Kieren Lovell | TEDxTartu*. Retrieved from YouTube: https://www.youtube.com/watch?v=_C7sNvIGQzM&list=WL&index=7&t=0s

Thompson, S. T. (2006). Helping the hacker? Library information, security, and social engineering. *Information Technology and Libraries*, 222-225.

Thornburgh, T. (2004). Social Engineering: The “Dark Art”. *Proceedings of the 1st annual conference on Information security curriculum development* , 133-135.

Weir, G. R., Toolan, F., & Smeed, D. (2011). The threats of social networking: Old wine in new bottles? *Information security technical report (16)*, 38-43.