THE USE OF SOCIAL ENGINEERING TO TRICK UNSUSPECTING USERS INTO SHARING CONFIDENTIAL INFORMATION AND EXPOSING THEM TO CYBER ATTACKS

IRM 4729: ASSIGNMENT 4

COLLEGE: CSET

NAME: MZWANDILE MKHOKHA

STUDENT NO: 65278518

21 OCTOBER 2022

DECLARATION

I, the undersigned ..Mzwandile Mkhokha..... hereby declare that the research report titled : **THE USE OF SOCIAL ENGINEERING TO TRICK UNSUSPECTING USERS INTO SHARING CONFIDENTIAL INFORMATION AND EXPOSING THEM TO CYBER ATTACKS** is my own work and all sources that were used for this study have been referenced and credited

Date: 21/10/2022 Name: Mzwandile Mkhokha

Signature: m.m

ACKNOWLEDGEMENT

LIST OF ABBREVIATIONS

ABSTRACT

The field of information security is growing quickly (Mouton et al., 2016). Cyber criminals have found creative ways to gain access to secure information system and confidential information systems using human vulnerabilities. Cyber-attacks executed using social engineering pose a serious security threat to information systems and its users. Throughout history, social engineering has taken various forms and will continue to do so (Barbosa & Morais, 2017). In the context of cyber security social engineering is the "technique" of persuading someone to reveal confidential information, and the action of doing so is referred to as a social engineering attack (Mouton et al., 2016). Since users themselves are the most vulnerable component of information systems, social engineering attacks are stronger to most other types of hacking in that they can compromise even the most secure systems (Krombholz et al., 2015).

Keywords: Social engineering, cyber-attacks, social engineering attacks and information technology

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

1.1 INTRODUCTION

The field of information security is growing quickly (Mouton et al., 2016). Cyber criminals have found creative ways to gain access to secure information system and confidential information systems using human vulnerabilities. Cyber-attacks executed using social engineering pose a serious security threat to information systems and its users. Throughout history, social engineering has taken various forms and will continue to do so (Barbosa & Morais, 2017). In the context of cyber security social engineering is the "technique" of persuading someone to reveal confidential information, and the action of doing so is referred to as a social engineering attack (Mouton et al., 2016). Since users themselves are the most vulnerable component of information systems, social engineering attacks are stronger to most other types of hacking in that they can compromise even the most secure systems (Krombholz et al., 2015).

1.2 PROBLEM STATEMENT

Nowadays, the majority of businesses and banks rely on modern technologies like the internet and smartphones (Bansla et al., 2019). The world is so attached to the Internet. Unfortunately, not everyone makes good use of the Internet (Chetioui et al., 2022). The goal of security technology measures is to improve the security of information systems, however human aspects are a vulnerability that can be exploited by social engineers during social engineering attacks (Conteh & Schmick, 2016). Social engineers utilize the human factor which is the most vulnerable aspect of every institution or organization (Abass, 2018).

1.3 RESEARCH OBJECTIVES

The research has the following objectives:

1. To get a clear overview of social engineering.
2. To find out more about the techniques or strategies social engineers use to obtain confidential information from unsuspecting users.
3. To find methods users and organisations can use to protect themselves from social engineering attacks.

1.4 RESEARCH QUESTIONS

The research intends to address the following questions:

1. What is social engineering in the context of cyber security and information security?

2. What strategies do social engineers use to gain access to confidential information?

3. What strategies can organisations use to protect their users from being victims of social engineering cyber-attacks?

4. What are the risk and vulnerabilities that can be caused by social engineering?

1.5 SIGNIFICANCE OF STUDY

Sensitive information should be used for its intended purpose, measures should be put in place to ensure that confidential information is protected and only authorized people have access to that kind of information. The study aims to help users and organisations with strategies and methods they can implement to protect themselves from social engineering attacks. Users will get a deeper understanding of their role in social engineering attacks and how social engineers take advantage of their human vulnerabilities to obtain information from them. The study will further be referred to by researchers in the cyber-security related field.

1.6 KEY TERMS AND CONCEPTS

Cyber security, social engineering and information security

1.6 CHAPTER SUMMARY

CHAPTER 2: LITERATURE REVIEW

2.1 INTRODUCTION

Social Engineers use different techniques and methods to launch social engineering cyber-attacks, furthermore the success of a social engineering attack depends mostly on the attacker's high level of skillset and the ability to fit the proper technique to manipulate the victim. When cyber criminals are unable to attack systems that are free from technical vulnerabilities they use the human factor to find ways they can use to conduct their malicious activities (Alzahrani, 2020). In addition, the attacker manipulates users psychologically to convince them to violate security measures that are put in place (Alzahrani, 2020). Users remain exposed to the manipulation by social engineers seeking to gain sensitive information or unauthorized access. Moreover, Strategies and methods can be used to protect users from becoming victims of social engineering attacks.

2.2 WHAT IS SOCIAL ENGINEERING?

Staff members are frequently the weakest link in an information security strategy, making technology alone insufficient to prevent information theft (Mouton et al., 2014). In the context of cyber security, it is mainly used to trick victims into revealing sensitive data, to perform actions that violate security protocols, to unknowingly infect systems, or to expose confidential information (Barbosa & Morais, 2017), Conteh and Schmick(2016) further define social engineering, also known as human hacking, as the art of tricking employees or consumers into giving up their credentials and using them to access networks and accounts. Social engineers target people with access to information rather than technical systems, tricking them into disclosing private information or even carrying out their malicious attacks through persuasion and influence (Mouton et al., 2014). Mouton, et al.(2014) furthermore describes social engineering as the "skill" of persuading someone to reveal confidential information, they also define the action of doing so is referred to as a social engineering attack.

Sophisticated IT security systems cannot protect systems from hackers or evade unauthorized access which seems legitimate. Staff members may be persuaded to reveal confidential information, which would then make it possible for unauthorized users to get access to secured systems (Mouton et al., 2014). Humans are very easily persuaded to divulge knowledge or other data that an attacker would find beneficial (Abass, 2018). Social engineers are inventive and crafty, using a variety of methods to distribute harmful software to steal personal data, conduct fraud, or access security networks

(Abass, 2018). Conteh and Schmick(2016) argue social engineering that it's about hackers misleading, coordinating, and skilfully manipulating people's desire to pursue their explorational and curiosities impulses. Barbosa and Morais (2017) furthermore state tha t during the interaction, the victim is unaware of the destructive nature of their behaviour, and the social engineer taps into innocent instincts, not criminal instincts.

2.3 TYPES OF SOCIAL ENGINEERING TECHNIQUES

A social engineering attacker takes advantage of various methods or techniques available to assist him/her attain information that will assist them in launching a social engineering attack. The techniques are classified into two (2) categories being the Human based social engineering techniques and the technical based social engineering techniques. Each of the techniques are described in more detail on section 2.3.1 and 2.3.2 of this paper

2.3.1 COMPUTER OR TECHNOLOGY BASED TECHNIQUES

Technology-based Social engineering is similar to conventional hacking techniques. The goal is to trick users into thinking they are interacting with a genuine computer system using any software or application (Singh, 2012). Abass (2018) further states that the other objective of the technology-based technique is to persuade users to diclose sensitive data. According to Ghafir et al. (2016) computer-based or technology based attacks rely deeply on technology to manipulate and trick a target or potential victim into submitting information required by the attacker to execute his malicious deeds.

2.3.1.1 PHISHING

Phishing is a common online threat in which an attacker tries to trick victims into providing personal data, such as passwords or credit card details, into a fraudulent website that is under the attacker's control (Krombholz et al., 2015). Barbosa and Morais (2017) further note that malicious emails that appear as if they are from a legitamate source can be used to extract personal information from users. Scams of this sort that are more complex usually take advantage of psychological vulnerabilities in their victims to deceive them and establish a sense of urgency that interferes with clear judgment (Barbosa & Morais, 2017). According to Krombholz et al. (2015) there has been a demostration that social phishing, which uses “social” infromation that is specific to the target, can be extremely effective comapared to traditional phishing.

Phishing attacks aim to spread across many victims as possible by focusing on the masses (Barbosa & Morais, 2017). A spear-phishing attack can only be carried out after conducting initial research, and the message's content must at least be somewhat customized for each target. Cybercriminals can utilize social networking sites to gather data on potential victims and use that data to construct highly personalized communications that look to have been written by close friends (Barbosa & Morais, 2017).

2.3.1.2 POP UP WINDOW

The user is deceived into re-entering his/her login credentials in response to an window that looks legitimate that has a message indicating that the connection was lost, a malicious program runs on the background to get the victims login credentials. Pop-up windows can run malware software without the knowledge of the victim (Salahdine & Kaabouch, 2019)

2.2.2 HUMAN BASED SOCIAL ENGINEERING TECHNIQUES

Abass(2018) describes that with the human based technique the attacker takes advantage of the victims innocence, and the natural human element to want to be helpful and liked to deceive them. Deception and human interaction are key components of the human based social engineering technique (Ghafir et al., 2016). Human-based attacks can be executed in person or over the phone and are entirely reliant on the attacker's art of deception (Singh, 2012). Human based techniques include spoofing, dumpster diving, shoulder surfing, and reverse social engineering. The most common form of deceit is human-based social engineering since voice can be so easily hidden (Singh, 2012).

2.2.2.1 SHOULDER SURFING

Shoulder surfing refers to the practice of directly watching a victim and peeking over their shoulder to gather personal information, usually for the purpose of obtaining authentication data (Barbosa & Morais, 2017) . Alzahrani (2020) further explains that shoulder surfing is a common technique used for social engineering, the intention is for the attacker to get the username or password of the victim as he/she types on the keyboard by looking over the targets shoulder.

2.2.2.2 TAILGATING

Tailgating and piggybacking are used in this kind of attack to access areas they are not permitted to be in (Conteh & Schmick, 2016). The can do this by either impersonating delivery employees or other individuals who might need temporary access, the attacker in this assault exposes those who have the power to grant or obtain access to a restricted area (Conteh & Schmick, 2016). This type of social engineering technique doesn't obtain information through email or other online medium. Instead, the hacker has a direct communication with his victim (Chetioui et al., 2022). The attacker blends in with victim with the intention to make the victim believe that the attacker belong there (Chetioui et al., 2022).

2.2.2.3 DUMPSTER DIVING

Dumpster diving is the act of searching through rubbish, with the intention to find bank statements, personal information or medical data that might be of use to the dumpster diver (Mouton et al., 2014). The proper disposal of documents, hardware, and other materials from which private information can be recovered is frequently not done accordingly by people or organizations, attacker then takes advantage of the flaw to seek for sensitive information (Barbosa & Morais, 2017).

2.2.2.4 REVERSE SOCIAL ENGINEERING

According to Krombholz et al. (2015) Reverse social engineering technique is a technique whereby the attacker pretends to be someone trustworthy with the intention of attracting the potential victim to appraoch him/her, perhaps to ask for help. In order to minimize the chance of raising any suspicions, the threat actor entices the target to start the interaction (Barbosa & Morais, 2017). . The three main components of this indirect technique known as "reverse social engineering", are sabotage, advertising and assisting (Krombholz et al., 2015). The initial stage of this technique is sabotaging the company’s computer system. This can include anything from disconnecting someone from the company’s network to sophisticated software application manipulation. The attacker then advertises that he/she can help solve the problem, when victim asks for assistance the attacker will help solve the issue he/she had caused earlier with the intention of exploiting the user either by asking for the password or installing a malicious software on the victims computer (Krombholz et al., 2015).

2.3 SOCIAL ENGINEERING PHASES

According to Mouton et al. (2014) the social engineering attack cycle developed by Kevin Mitnick is the most commonly used model. The model has four phases: Information gathering, gaining trust phase, exploitaion phase and information utilisation phase. Mouton et al. (2014) demonstrated the Mitnick's attack cycle through the use of a diagram. Figure 1 demonstrates the Mitnick's attack cycle. The phases are further described in sections 2.3.1, 2.3.2, 2.3.3 and 2.3.4.

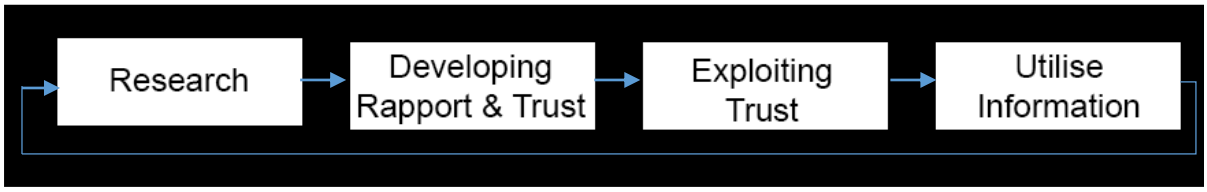

Figure 1 Mitnick's Attack Cycle (Mouton et al., 2014)

2.3.1 INFORMATION GATHERING PHASE

Research is a technique used to obtain information where the target is retrieved. Prior to initiating the attack, the attacker should have as much information as possible about the victim (Mouton et al., 2014). According to Barbosa and Morais (2017) during the investigation or research phase of the social engineering attack the attacker researches and gathers as much information as possible about the people and business models associated with your target. Barbosa and Morais (2017) on their journal quote a well know sentence from Sun Tzu in the art of war: "Know your enemy", Barbosa and Morais (2017) furthermore state that knowledge is power and in the context of cyber security, investing in this phase is invaluable for uncovering potential vulnerabilities. However instead of launching targeted attacks, a skilled social engineer could take advantage of random encounters to open up further possibilities without prior research (Barbosa & Morais, 2017).

2.3.2 GAINING TRUST PHASE

The threat actor initiates contact with the potential victim during this phase, he engages the target, spins the story, creates intimacy, and assumes control of the interaction (Barbosa & Morais, 2017). According to Mouton et al. (2014) if a target trusts an attacker, the target is more likely to provide the information that is requested. Human nature is built on the assumption that everyone is trustworthy—at least until they prove otherwise (Abass, 2018). Abass (2018) furthermore argues that utilizing insider information and typically posing as a more senior member of the institute can help build trust. Lastly, Mouton et al. (2014) state that rapport and trust can be built by utilizing insider information, faking one's identity, leveraging references to people the victim is familiar with, demonstrating a desire for assistance, or acting in an authoritative capacity.

2.3.3 EXPLOITATION PHASE

According to Abass (2018) the attacker's goal in this step is to maintain the momentum of compliance established in the "Gaining phase without raising suspicion. Barbosa and Morais (2017) previously outlined that the goal of the exploitation phase is to achieve the attack's goal, which could be to extract information or to manipulate the target in order to compromise the system. The attacker must research his victim's emotional state and figure out how to exploit it (Abass, 2018). During this stage, the previously established relationship is abused in order to obtain the initially desired information or action, the attacker might do this by requesting for information from the

victim, requesting for a specified action from the victim or, alternatively, to manipulate the victim into asking the attacker for help (Mouton et al., 2014).

2.3.4 UTILISATION PHASE

During the last phase of the attack the attacker starts the real attack without alerting the victim that he is under attack (Abass, 2018). The social engineering completes the interaction with the victim, preferably without making the victim suspicious (Barbosa & Morais, 2017). According to Abass, (2018) leaving the victim feeling as if they did something good is better as it allows possible interactions to continue in future. After the last phase has completed the attacker is typically very difficult to find or track down.

2.4 PREVENTATIVE MEASURES AGAINST SOCIAL ENGINEERING ATTACKS

Cyber security is very crucial in ensuring that information systems, computer software and mobile applications are protected from being attacked by hackers. Conteh and Schmick (2016) state that irrespective of how technologically secure a network seems to be the human element will always be a vulnerability. There are safety measures that can be put in place to lower the risk that can result from a social engineering attack to a level that can be tolerated. Conteh and Schmick (2016) furthermore note that a concept known as multi-layer defence or defence in depth has to be used as a risk mitigation tool. A Defence in depth structure contains a combination of the following precautionary measure: 1) Security policy, 2) Education and training, 3) Network Guidance, 4) Audit and compliance

2.4.1 SECURITY POLICY

A security policy is a document that documents outlines all the rules and regulations when interacting with a computerized system or software. Conteh and Schmick (2016) states that a well written security policy should include both technical and non-technical approaches that are downward driven by executive management, they furthermore states that security should be integrated into their operational objectives.

Ghafir et al. (2016) argue that security policies have a specified lifespan that should ideally include a review date and it should be maintained, most importantly the security policy should relate with the current state. To do this, policies should be evaluated frequently and more often, with at least 20% of them changing each year, and the system as a whole in a 5-year cycle (Ghafir et al., 2016). Policies that are more likely to change should be examined more frequently, the following are some examples of policies that can be put in place to protect against social engineering attacks: information release, access approval, password updates, modems, help desk, employee ID, shredding confidential documents, multi factor authentication etc. (Ghafir et al., 2016).

2.4.2 EDUCATION AND TRAINING

Education and training is the most common way of learning and acquiring knowledge therefore it should be a necessity for first time users of an information system, computerized software or application to be presented with guidelines of how to identify and report suspicious interactions. The will help prevent being a victim of a social engineering attack as users will be aware of various techniques social engineering attackers use (Conteh & Schmick, 2016). More over trainings should be hosted more often to keep users informed on how to deal with potential social engineering attacks.

Users should be wary of tempting offers Bansla et al. (2019) suggest that if users get offers that are too tempting or attractive they should think many times before welcoming it. Through education and training users should be encouraged to verify whether they are dealing with a valid or credible offers or a trap,even googling might help when verifying the legitimacy of offters (Bansla et al., 2019).

2.4.3 PHYSICAL GUIDANCE

There are multiple options that can be implemented to protect physical assets (Conteh & Schmick, 2016). Conteh and Schmick (2016) furthermore suggest that a combination of security guards, mantraps and security cameras should be used to deter intruders from premises is beneficial, access control or biometrics should be used as tools that grants access to people.

2.6 THE ROLE SOCIAL MEDIA IN SOCIAL ENGINEERING ATTACKS.

According to Wilcox et al. (2014) a number of studies have shown that there is a correlation between social engineering and social media sites such as facebook and Twitter, as the worthy personal and organisational information can be found on these platforms (Wilcox et al., 2014). People use social media sites like Facebook and Twitter to post about their daily lives without thinking about the possible risk that could come back to bite them (Wilcox et al., 2014). Attackers collect information like this for their own personal use (Wilcox et al., 2014).

2.7 CHAPTER SUMMARY

A social engineering attack, to put it simply, is a cyber-attack launched by a social engineer, or occasionally a group of social engineers, with the goal of accessing secure information systems and sensitive data. For this form of attack, social engineers rely on their skills and human vulnerabilities. Social engineers utilize a variety of techniques to trick users into disclosing confidential details and sometimes their user names and passwords. One of the most widely used models for launching social engineering attacks is Mitnik's attack cycle; the phases of the model were described and explored in the literature review. Technically secure information systems are vulnerable to social engineering attacks since the relevant stakeholders have no control over the human component or user tendencies.

Despite the fact that social engineering attacks pose a risk to users and information systems, there are a number of techniques and strategies that can be employed to reduce the likelihood of social engineering attacks. Institutions can manage how users interact with their information systems by using a security policy; this will help users understand how they should utilize information systems. Users must receive training and education on how to identify and defend against social engineering attacks. Physical precautions should be put in place to restrict access and establish a tier of users for each facility.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 INTRODUCTION

In this chapter the research process, sampling and data collection methods will be discussed. In addition, advantages and disadvantages of the various data collection methods will also be discussed in this chapter. Furthermore, the method of data analysis were also discussed in this chapter.

3.2 RESEARCH METHOD

Kumar (2014) notes that quantitative and qualitative research methodologies differ both in their underpinning philosophy and to some extent, in the methods, models and procedures used. He furthermore notes that the difference between qualitative and quantitative research are differentiated in terms of methods of data collection, the procedures adopted for data processing and analysis, and the style of communication and findings (Kumar, 2014).

3.2.1 QUANTITATIVE RESEARCH APPROACH

According to Chandra and Harindran (2017) when conducting a quantitative research data is usually gathered and transformed into numerical form in order perform statistical calculations and derive generalize or specific findings from which you can build a hypotheses. The objective is given priority in a qualitative study. There may be a number of hypotheses, but the aim is to choose the one that produces the most pertinent results. Researchers use a number of tools and resources for this, including computers, observation, checklists, statistical analysis software and other relevant resources. Chandra and Harindran (2017) further states that there is a reconstruct procedure to accomplish the analysis task, the aim is to discover various relationships between variables. More emphasis is put on deductive reasoning that tends to shift from the general to the specific also known as top down approach during a quantitative research. One or more reliable observations or rules are combined to demonstrate the validity of the hypothesis (Chandra & Harindran, 2017).

3.2.2 QUALITATIVE RESEARCH APPROACH

Chandra and Harindran (2017) notes that quanlitative research involves recording, analyzing and understanding the core meaning and significance of the revealable variables. The research approach used is an inductive approach, in which the researcher builds a theory or searches for a pattern using the data they have gathered (Chandra & Harindran, 2017). Qualitative research involves moving strategically and conventionally from specific to general and is sometimes called a bottom-up approach. Observations, interviews and focus groups are methods used to collect data in a qualitative research. Chandra and Harindran (2017) perceive quantitative research as counting and qualitative research can be seen as proposing which variables are to be counted.

3.3 SAMPLING AND SAMPLING METHODS

Kumar (2014) briefly describes sampling as the process of selecting few from a bigger group to serve as a basis for estimating or predicting prevalence of an unknown piece of information, outcome or situation regarding the bigger group

3.4.1 RANDOM/PROBABILITY SAMPLING DESIGN

According to Kumar (2014) for a sample to qualify as random sampling or probability sampling it is important that every element in the study population to have an equal and independent chance of selection in the sample. The idea of independence states that the selection of one element in the sampling is not influenced by the selection of another element. Kumar (2014) furthermore argues that for a sample to be considered a random/probability sample both of these conditions have to be met as bias can be introduced into the study if both of the conditions are not met. The advantages of random or probability sampling is that data that is drawn from such sampling can be generalised to the total population as they represent the total sampling population (Kumar, 2014).

3.4.2 NON-RANDOM/NON-PROBABILITY SAMPLING DESIGN

According to Kumar (2014) when the number of elements in a population is either unknown or they cannot all be individually recognized, non-probability sampling designs are used. These sampling designs do not follow the theory of probability when selecting elements from the sampling population (Kumar, 2014). In such cases, other factors must be taken into account while choosing the elements. Both quantitative and qualitative research frequently employ non-random sampling methods (Kumar, 2014).

3.4.1.1 QUOTA SAMPLING

According to Kumar (2014) with quota sampling a researcher is guided by one or more visible characteristic of the population that is of interest to the researcher for example, gender or race. Once a characteristic is identified relevant permission is requested to interview the person, the process continues until the number of respondents has been met (Kumar, 2014). The advantages of using this design include the fact that it is the least expensive way to choose a sample, that no information about the sampling population, such as a sampling frame, the total number of elements, their locations, or other details, is required, and that it guarantees the inclusion of the people you need (Kumar, 2014). The disadvantage of such approach is that the findings cannot be generalized to the entire sampling population because the resulting sample is not a probability one, and the most accessible individuals chosen from one location may not be truly representative of the entire sampling population because they may have characteristics that are unique to them (Kumar, 2014).

3.4.1.2 ACCIDENTAL SAMPLING

Accidental sampling is based upon convenience in attempt to accessing sample population (Kumar, 2014). Accidental sampling makes no attempt to include individuals possessing an obvious/visible characteristic. Data collection is stopped when the required number of participants the researcher decided to have in the sample has been met (Kumar, 2014).

3.4.1.3 CONVENIENCE SAMPLING

Accidental sampling and convenience sampling design are very similar (Kumar, 2014). Convenience sampling is initially directed by the convenience to the researcher this can include anything from easy accessibility, geographic proximity, known contacts, ready approval for undertaking the study, or being part of a group (Kumar, 2014). Data or information required is collected from a specific number of respondents or have the reached desired point (Kumar, 2014).

3.4.1.4 SNOWBALL SAMPLING

Kumar (2014) Defines snowball sampling as the process of choosing a sample using networks. Initially a few people or organisations are selected and the information that is needed is collected from them (Kumar, 2014). They are then asked to identify other people in the group or organisation, and the selected people become part of the sample (Kumar, 2014). The information is then collected from them and they are also asked to identify other members of the group and, in turn, those identified individuals become the basis for further data collection (Kumar, 2014). The procedure continues until a required number has been reached, in terms of the information that required (Kumar, 2014).

3.5.3 "MIXED" SAMPLING DESIGN

Mixed sampling design sometimes referred to as systematic sampling has both the characteristics of both random and non-random sampling designs. A sample frame for your study population is essential in or to apply a mixed or systematic sampling design; It is helpful in instances where the

study population's records are regularly maintained as part of service delivery. With mixed or systematic sampling the sampling frame is split into a number of segments called intervals.

3.4.4 SAMPLING METHODS SELECTED FOR THIS STUDY

Two methods from Non Probability sampling methods were used to select potential individual to participate on this this study namely; Convenience sampling and snowball sampling. The approaches are suitable for study as the aim is to get more access to users who are accessible and are of proximity to the researcher convenience sampling will help achieve that objective. With convenience sampling the researcher can select the target audience based on easy accessibility, geographic proximity, known contacts, ready approval for undertaking the study, or being part of a group (Kumar, 2014).

3.5 DATA COLLECTION METHODS

Most of the data collection methods can be used across studies that are classified as qualitative, quantitative or mixed or systematic methods. According to Kumar (2014) the classification of a study is mostly determined by how a specific method is used for data collection. Chandra and Harindran (2017) state that data collection that is inaccurate can affect the results of a study and eventually this will lead to invalid results.

3.5.1 INTERVIEWS

An interview is fundamentally a person-to-person interaction, either face to face or using other alternatives, between two or more people with a precise purpose in mind (Kumar, 2014). Kumar (2014) further quotes Monette et al. (1986: 156) were they outline that an interview covers an interviewer reading questions to the interviewees and recording the answers.

3.5.1.1 ADVANTAGES OF INTERVIEWS

According to Kumar (2014) a researcher has the freedom to decide the content and format of the questions, how to word them and decide the manner in which the questions are to be asked and in what manner. The interviewer has the privilege of explaining questions that are not properly understood (Kumar, 2014). An interviewer can use information obtained from non-verbal reactions to enhance information obtained from questions and answers (Kumar, 2014). Another advantage of interviews is that an interview can be used with several type of population such as old, children and illiterate (Kumar, 2014).

3.5.1.2 DISADVANTAGES OF INTERVIEWS

Interviews tend to consume a lot of time and are expensive especially in instances where the respondents are of a wider geographic area (Kumar, 2014). The quality of the interaction affects the quality of the data, in addition because every interaction between respondents and interviewer might be unique, the quality of the responses gained from interviews might be different (Kumar, 2014). There is a possibility of the researcher being bias when asking questions or even interpreting the responses obtained from interviews. In addition, when using multiple interviewers the quality of the data might vary (Kumar, 2014). Furthermore the quality of the interviewer affects the quality of the data (Kumar, 2014).

3.5.3 OBSERVATION

Observation is a method to collect primary data (Kumar, 2014). Kumar (2014) further describe observation as a purposeful, systematic and selective way of watching and listening to an interaction

or phenomenon as and when it takes place. An observer gives undivided attention because his/her skill set and experience are very much used for the observation as there is no close contact with the respondents (Chandra & Harindran, 2017). Kumar (2014) furthermore states that observation is useful or appropriate in situations where overall or accurate information cannot be elicited by questioning, this might be caused by respondents who are co-operative or unaware of the answers because it difficult for them to detach themselves from the interaction.

3.5.3.1 ADVANTAGES OF OBSERVATIONS

According to Kumar (2014) observations can be recorded using a video camera or other electronic devices that has the functionality to record a video and then later analyse the recording, this gives the observer the privilege to watch the video a number of times before interpreting an interaction or formulating any conclusions from it and other professionals can be invited to the interaction to arrive at more conclusions that are objective.

3.5.3.2 DISADVANTAGES OF OBSERVATION

Kumar (2014) argues that an individual or group may change behaviour when they become aware that they are being observed. If change of behaviour occurs distortion might be introduced during the use of observation as what is observed might not represent normal behaviour (Kumar, 2014). Furthermore observer bias might be a possibility during observation, if an observer is not impartial he/she can introduce bias and there is no method to confirm the observations and the inferences drawn from them (Kumar, 2014). In addition interpretations from observations may vary from observer to observer (Kumar, 2014). There is a possibility of incomplete observation caused by the distractions the observer might be faced with (Kumar, 2014). For example, the observer might miss some of the interaction while detailing notes.

3.5.4 QUESTIONNAIRE

A questionnaire can be defined a collection of written questions, that are expected to be answered by respondents. The respondents have to read the questions, interpret what is expected from them and then answer the questions (Kumar, 2014). A questionnaire has to be structured in a way that is easier to read and understand as no one is there to explain the meaning to questions to respondents (Kumar, 2014). It is important for a questionnaire to be developed in an interactive style, this will allow the respondent to feel as if he/she is talking to someone (Kumar, 2014). A questionnaire can be administered via mail this method is applicable in situations where the researcher knows the address of the prospective respondents. Another way to administer a questionnaire is through collective administration where the researcher obtains a captive audience such as students, group of people gathering etc. In additions to the previously described questionnaire administration methods an online questionnaire can also be used to administer questionnaires (Kumar, 2014).

3.5.4.1 ADVANTAGES OF QUESTIONNAIRES

A questionnaire is less costly, as respondents are not interviewed, this allows you to save time and both the human and financial resources (Kumar, 2014). The use of a questionnaire is reasonably convenient and inexpensive, particularly when it administered collectively to a study population (Kumar, 2014). Questionnaires provide more anonymity, the anonymity is granted as there is no face-to-face communication between the interviewer and respondents (Kumar, 2014). When asking sensitive questions questionnaires can help increase the likelihood of obtaining sensitive information (Kumar, 2014).

3.5.4.2 DISADVANTAGES OF QUESTIONNAIRES

The main disadvantage of using questionnaires is that its application is limited to a study population who have the ability to read and write. In addition, questionnaires cannot be used to a population that is extremely young or extremely old (Kumar, 2014). Questionnaires are known for their low response rates, this can be caused by respondents who fail to return their questionnaires, and this then reduces your sample size as a result (Kumar, 2014). Since everyone might not return their questionnaires the collected data might not represent the total study population, this then leads to self-selecting bias. Kumar (2014) further notes that with questionnaires there is a lack of opportunity to clarify issues, the quality of the information provided will be impacted if different responders interpret questions differently.

The questionnaire might not serve its purpose where spontaneous responses are required, as the respondents might glance through the questionnaire before answering in some situations, this then gives them the advantage of reflecting on their answers or even re-evaluate their responses (Kumar, 2014). Kumar (2014) further sates that certain the respondents knowledge of further questions might influence the respondents answers to the present question (Kumar, 2014). Other people might influence the answers being asked as the respondent might consult other people before answering som questions. In addition other information cannot be included to a response (Kumar, 2014).

3.5.4.5 DATA COLLECTION METHODS FOR THIS STUDY

For the researcher to be able to distribute questions easier across various focus groups questionnaires will be used as a method of data collection as using questionnaires has the following benefits; A questionnaire is less costly, as respondents are not interviewed, this allows you to save time and both the human and financial resources (Kumar, 2014). The use of a questionnaire is reasonably convenient and inexpensive, particularly when it administered collectively to a study population. Questionnaires provide more anonymity, the anonymity is granted as there is no face-to-face communication between the interviewer and respondents (Kumar, 2014).

3.5 METHOD OF DATA ANALYSIS

Since the data will be collected from questionnaire a data processing software like excel will be used to analyse data and project the data.

3.6 ETHICAL CONSIDERATIONS

According to Kumar (2014) there are plenty of ethical issues to consider with reagards to the participants in a research activity. It is important for a reseacher to obtain an informed consent from the participants before asking questions, as it is unethical to collect information from respondents without their knowledge, their expressed willingness or informed consent. A researcher must be able to justify the relevance of the research being conducted, this will help to avoid wasting the respondents time whis is seen as unethical. Some researchers perceive the offering of inducements as being unethical, however through experience Kumar (2014) argues that most people do not participate in a study with the intention of being incentified but they participate because they see the importance of the study. Kumar (2014) is of the view that giving a small gift to participants as a token of appreciation is ethical. However, giving participants gifts before data collection is unethical.

Certain information can be seen as confidential or sensitive by some people, thus, attempting to seek for the information constitutes an invasion of privacy. According to Kumar (2014) it is important for the researcher to inform the participants of the sensitivity of certain questions, assurance that the information will be handled with confidentiality should be granted. In addition, participants should be given enough time to decide if they want to share the information or not. Diclosing a

information about a respondent to other people for other purposes besides research is unethical (Kumar, 2014). Identifying an individual respondent and the information provided by her is unethical, therefore is important to ensure that the respondents are anonymous (Kumar, 2014).

3.7 CHAPTER SUMMARY

CHAPTER 4: EXPECTED RESULTS AND CONTRIBUTION

4.1 INTRODUCTION AND OVERVIEW

This chapter aims to present the findings of this study in relation to the research objectives. It is expected for the study to critically analyse social engineering and methods used for this kind of cyber-attack, the research also to also get a clear overview how users were to respond to different social engineering techniques and further get a clear overview of the knowledge users have in relation to social engineering and how they can protect themselves from such attacks. In addition, the study will discuss the expected contribution of the study.

4.2 RESULTS

Data was not collected from the relevant focus groups who are expected to contribute because of the time constraint. However, a literature review was conducted in relation to the objectives of this study. Through the literature review the term “social engineering” was described and further interpreted in relation to cyber-security. The various techniques or methods social engineers use to manipulate users into giving them information they might use to get access to secure information systems were also reviewed.

4.3 EXPECTED CONTRIBUTION OF STUDY

This paper will outline a strategy that individuals and businesses can utilize to defend themselves against social engineering related cyber-attacks. The study will add to the body of research on social engineering and act as a resource for academics in the future who are interested in addressing challenges caused by social engineering in the field of cyber-security and information security. Organizations or individuals may use this study as a resource when putting together the material for their information-sharing sessions or workshops on cyber security.

CHAPTER 5: CONCLUSION AND RECOMMENDATION

5.1 INTRODUCTION

5.1.1 RQ1: WHAT IS SOCIAL ENGINEERING IN THE CONTEXT OF CYBER SECURITY AND INFORMATION SECURITY?

Social engineering is taking advantage of human vulnerabilities with the intention to get access to confidential information and information systems that are technically secure. Social engineers take advantage of human element of trusting each other unless there are enough reasons not to trust a fellow being.

5.1.2 RQ2: HOW DO SOCIAL ENGINEERS USE SOCIAL ENGINEERING TO GAIN ACCESS TO INFORMATION SYSTEMS OR INFORMATION TECHNOLOGY SYSTEMS?

A social engineering attacker uses a variety of available tactics or strategies to help them obtain the knowledge they need to launch a social engineering attack. The methods are divided into two (2) categories: social engineering methods based on human interaction and social engineering methods utilizing technology. More information on each technique is provided in this paper's sections 2.3.1 and 2.3.2. The most widely used model is the Kevin Mitnick social engineering attack cycle. The model is divided into four phases: information collection, building trust, exploitation, and information utilization.

5.1.3 RQ3: HOW CAN ORGANISATIONS PROTECT THEIR USERS FROM FALLING VICTIMS OF SOCIAL ENGINEERING CYBER-ATTACKS?

Information systems, computer software, and mobile applications must be safeguarded from hacker attacks, which is why cyber security is so important. No matter how technologically secure a network appears to be, the human factor will always provide a vulnerability. There are safety precautions that can be taken to reduce the potential risk of a social engineering attack to an acceptable level. Additionally, Conteh and Schmick (2016) point out that a strategy known as defence in depth or multi-layer defense must be implemented as a risk mitigation technique.

5.2 CONCLUSION

Despite the fact that social engineering attacks pose a risk to users and information systems, there are a number of techniques and strategies that can be employed to reduce the likelihood of social engineering attacks. Institutions can manage how users interact with their information systems by using a security policy; this will help users understand how they should utilize information systems. Users must receive training and education on how to identify and defend against social engineering attacks. Physical precautions should be put in place to restrict access and establish a tier of users for each facility.

5.3 LIMITATIONS

Financial resources and time was a constraint to further collect data from focus groups hence a literature review was used as a point of reference for the study.

5.4 RECOMMENDATION FOR FURTHER RESEARCH

The Mitnik’s attack cycle model should be discussed and critically reviewed since there has been some changes in the information technology field. Further research might include the role of social engineering in social media, cloud computing, AI and Machine learning.

5.5 LESSON LEARNT FROM IRM PRACTICE

I now know how to evaluate and analyze literature critically. I've now mastered the skill of turning a topic into a purposeful problem statement. I have learned more about various data collection methods, research approaches, and my writing abilities have improved. Moreover, I have learned on how social engineering is used to attack secure information systems.

REFERENCES

Abass, I. A. M., 2018. Social Engineering Threat and Defense: A Literature Survey. *Journal of Information Security,* 09(04), pp. 257-264.

Alzahrani, A., 2020. Coronavirus Social Engineering Attacks: Issues and Recommendations. *(IJACSA) International Journal of Advanced Computer Science and Applications,,* 11(5), pp. 158-161.

AqibHafiz, Batth, R. S. & Jyoti, 2019. Social Engineering Attacks and Prevention: A Mirror Review. *THINK INDIA JOURNAL,* 22(16), pp. 2530-2536.

Bansla , N., Kunwar, S. & Gupta, K., 2019. Social Engineering: A Technique for Managing Human Behavior. *Journal of Information Technology and Sciences,* 5(1), pp. 18-22.

Barbosa, H. & Morais, T., 2017. *SOCIAL ENGINEERING AND CYBER SECURITY.* Porto, INTED.

Chandra, V. & Harindran, A., 2017. *Research Methodology.* 1 ed. India: Pearson Education India.

Chetioui, K., Bah, B., Alami, A. O. & Bahnasse, A., 2022. Overview of Social Engineering on Social Networks. *Procedia Computer Science,* Volume 198, pp. 656-661.

Conteh, N. Y. & Schmick, P., 2016. Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research,* 6(23), pp. 31-38.

Ghafir, I., Prenosil, V., Alhejailan, A. & Hammoudeh, M., 2016. *Social Engineering Attack Strategies and Defence Approaches.* Vienna, Austria, IEEE, pp. 145-149.

HIJJI, M. & ALAM, G., 2021. A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions. *IEEE Access,* Volume 9, pp. 7152-7169.

Krombholz, K., Hobel, H., Huber, M. & Weippl, E., 2015. Advanced social engineering attacks. *JOURNAL OF INFORMATION SECURITY AND APPLICATIONS,* Volume 22, pp. 113-122.

Kumar, R., 2014. *RESEARCH METHODOLOGY : a step-by-step guide for beginners.* fourth edition ed. London: SAGE.

Mouton, F., Leenen, L., Malan, M. & Venter, H. S., 2014. *Social Engineering Attack Frameork.* Pretoria, South Africa, s.n.

Mouton, F., Leenen, L. & Venter, H. S., 2016. Social engineering attack examples, templates and scenarios. *Computer & Security,* Volume 59, pp. 186-209.

Salahdine, F. & Kaabouch, N., 2019. Social Engineering Attacks : A Survey. *Future Internet,* 11(4), p. 89.

Singh, D., 2012. A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model. *International Journal of Information and Network Security (IJINS),* 1(2), pp. 45-53.

Wilcox, H., Bhattacharya, M. & Islam, R., 2014. *Social Engineering through Social Media: An Investigation on Enterprise Security.* Melbourne, VIC, Australia, Springer.