VISHING ATTACK DETECTION MODEL FOR MOBILE USERS.

By

ELIJAH MWANDATA MASENO

RESEARCH PROJECT SUBMITED IN PARTIAL FULFILMENT FOR THE AWARD OF MASTER OF SCIENCE IN DATA COMMUNICATIONS IN THE FACULTY OF COMPUTING AND INFORMATION MANAGEMENT AT KCA UNIVERSITY

November, 2017

DECLARATION

I declare that this dissertation work is my original work and it has not been previously published or submitted elsewhere for award of a degree. I also declare that this contains no material written or published by other people except where due reference is made and other duly acknowledged.

Elijah Mwandata Maseno Reg No. 15/05826

Sign: ________________________ Date: _________________________

Supervisor:

I do hereby confirm that I have examined the master's research project of

Elijah Maseno Mwandata

And have approved it for examination.

Sign: __________________________ Date: ______________________

Mr. Samuel Matende

ABSTRACT

Voice phishing (vishing) is a type of phishing attack where social engineers manipulate individuals during phone conversation into divulging sensitive information. Mobile users are target to most criminals, through mobile phone, users are able to carry out all bank services like cash withdraw, transfer and deposit, mobile phones offer payment services and through mobile phone, one is able to process loans. Social engineers prefer this form of attack because they can easily complicate the call routes, making it had for the investigator to locate them. Research shows most of this attacks are never reported to the relevant authorities because most victim blame themselves for their naivety. Unlike email phishing, which is classified, as tradition way of attack mobile phone vishing is a modern way of attack, less research exist on this area. This study proposed a practical model, which can be used by mobile phone users to detect social engineering attacks. The model seeks to assist user's to quickly and effectively identify if the caller is manipulating them in divulging sensitive information. The study employed a cross sectional survey research design. The sample size was comprised of 20 respondents, who were selected using random sampling. Data was collected using a structured questionnaire for mobile phone users and interview guide for the key informants in Kenya. Qualitative data was analyzed using content analysis while quantitative data was analyzed by use of SPSS using both descriptive. The study findings revealed that the main contributing factors in vishing attacks are psychological factors, technical factors and information sensitivity. Based on this three main factor a model was developed to aid mobile uses in detection of vishing attacks.

ACKNOWLEDGEMENT

I acknowledge the support of my family and my friends who have stood by me throughout my studies and particularly for their unending support.

I pay gratitude to my supervisors, Prof. Patrick Ogao and Mr. Samuel Matende for guidance, support, patience and understanding throughout the research period.

My sincere gratitude also goes to the entire KCA University fraternity for giving me an opportunity to pursue my career there. Also to the lecturers, management and staff of KCA University for their inputs especially in units that were essential in my course and development of this project for their support, patient and believing in me.

Above all, I am inexpressibly grateful to the Almighty God and my Savior

TABLE OF CONTENT

DEDICATION

To my wife Mary, our children Adia and Ethan.

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

CA	**–** Communication Authority.
Vishing	- Voice Phishing.
PIN	**-** Personal Identification Number
SEADM	– Social Engineering Attack Detection Model.
SEAD	**-** Social Engineering Attack Detection Model.
SMS	**-** Short Message Service

CHAPTER ONE.

1.0 Introduction

Among various form of emerging electronic financial crimes, voice phishing is known to cause the most significant degree of damage (Kim and Yang, 2008). Around the world, research on vishing is lacking despite of its impact and Kenya in not an exemption. At the point of writing, no research paper existed in Kenya on this area. This type of attack it is on the increase in Kenya because major money transaction are done on mobile platform, hence the need of this research. On their paper (Kinuthia & Akinnusi, 2014.) Points out that, Information security ensures business continuity, minimize business risk, maximize return on investments and business opportunities through mitigation of various types of attacks. Different form of measures have been put in place to protect Information from malicious attacks technically but despite of all this efforts, security breaches are on the increase because the weakest link in the security chain is over looked. In their research (Luo, *et al.*, 2011) found that a plethora of technological methods had been developed to address various security issues but human factors that contribute significantly to security breaches were comparatively neglected.

According to (Mouton, *et al.* 2014.) social engineering is the science of using social interaction as a means to persuade an individual or an organisation to comply with a specific request from an attacker where either the social interaction, the persuasion or the request involves a computer-related entity. As per definition, the main target are human beings who are persuaded to divulge sensitive information.

iVisher: Real-Time Detection of Caller ID Spoofing number it’s a system developed to authenticate the caller ID of an incoming call and blocks previously reported caller IDs by performing reachability analysis to the display name of a suspicious incoming call (that is, a display name suspected of caller ID spoofing). Most of the hackers tend to masquerade the caller identity.

Telephony fraud prevention was developed for guarding against telephony-based fraud that included, at a telephony device, identifying a caller ID of an incoming call or a dialled number of an outgoing call attempt or a number to be dialled. The identified caller ID or dialled number or number to be dialled were compared against a blacklist of telephone numbers. In the event that a match was found, a warning was presented to a user of the device and/ or the call or call attempt is terminated.

1.1 Background of the problem

Communication Authority of Kenya (CAK, 2016) " fourth quarter sector statistics report for the financial year 2015/2016 shows that the number of mobile money transfer subscriptions stood at 26.3 million while the number of mobile money transfer agents was recorded at 158,727. The total number of transactions during the quarter was registered at 375.8 million with an equivalent of Ksh. 957.0 billion transacted amongst the users.

According to CAK (2016) report, 227.3 million mobile commerce transactions were made, which amounted to the cost of goods and services valued at Ksh. 404.1 billion. Person-to-person money transfers recorded in the period was valued at Ksh. 429.4 billion". During the quarter under review, mobile subscriptions recorded a 3.7 per cent growth to 39.7 million up from 38.3 million subscriptions registered in the previous quarter.

Long are gone days when Mobile phones were only used for calling, In Kenya most of money transactions are carried through mobile phones. Mulwa (2012) found out that with the present dynamic technological developments, electronic information has grown in significance, businesses now conduct most of their day-to-day business undertakings electronically and this has drastically changed the level of information security threat.

According to (Kigen, *et. al.,* 2015) Kenya is at the global forefront of mobile money services as an alternative to traditional banking. These innovations are seen as new payment channels for online services that facilitate easier access to money. These new channels have opened new alternative targets for cyber criminals. Cyber criminals now have shifted their attacks from banks to financial services providers to access bank systems. Most of the Banks in Kenya are in the proses of trying to offer all of their services on mobile platforms. Customers are able to deposit, withdraw, pay and even process loans through their phones.

A study by (Kigen, *et. al.,* 2015) found that social engineering was the second top cyber security issue in Kenya in 2015 after data exfiltration. Several cases have been reported where individuals have been manipulated to give out sensitive information like subscriber identification module (SIM) pin or Money transfer pin, which has led to fraudulent transaction. Even with the increase of social engineering attacks on mobile platforms in Kenya, there is no extensive research that has been conducted, particularly to Kenyan mobile platforms to provide solution thus threatening the integrity of mobile transactions. This study sought to propose a practical model, which can be used by mobile phone users to detect social engineering attacks. The model will assist user's to quickly and effectively identify if the caller is trying to manipulate them in divulging sensitive information.

1.2 Problem Statement

Despite the efforts made to curb social engineering attacks, they are still on the increase. According to Proofpoint Human Factor Report (ProofPoint, 2016) Social engineering became the top attack technique in 2015 for beating cyber security, replacing exploits of hardware and software vulnerabilities. Mulwa (2012) found out that with the present dynamic technological developments, electronic information has grown in significance, businesses now conduct most of their day-to-day business undertakings electronically and this has drastically changed the level of information security threat. (Kigen, et al., 2015) Found social engineering as the second top cyber security issue in Kenya in 2015 after data exfiltration. Mobiles are extremely targeted by cyber criminals as major transaction are carried through mobile platforms and through a call they can get sensitive information which can be used for execution of attacks. Familiarity with long-distance banking and transaction systems can obscure the fact that victims are being deceived, especially without the presence of an individual (such as a banker) who can act as a capable guardian (Police Science Institute, 2014).

Most of the mobile uses in Kenyans fall prey to vishing attacks due limited knowledge or lack of knowledge on social engineers attacks. Vishing attackers take advantage of this in manipulating individuals to give out sensitive information, which can be used against them. The research done by (Bezuidenhout, Mouton, & Venter, 2010) shows that individual make themselves more vulnerable for not expecting to be attacked and most of them will never even know that they were a victim to such attacks. The problem at hand is to successfully detect vishing attacks on mobile platforms by mobile uses.

1.3 Aims and objectives of the project

General Objective

The aim of the study is to develop vishing attack detection model for mobile users.

Specific Objectives

1. To identify factors that contribute to vishing attacks

2. To develop vishing attack detection model for mobile user

3. To test and validate the model for detection of vishing attacks

1.4 Research Questions

1. What factors contribute to vishing attacks?

2. What are the consequences of successful vishing attacks?

3. What can be done to mitigate vishing attacks**?**

1.5 Significance of the study

People are generally susceptible to manipulation in nature and due to this; they form the weak link in the security chain. A social engineering attack targets this weakness by using various manipulation techniques to elicit individuals to perform sensitive requests. As stated by (Mouton, Leenen, & Venter, 2015) the field of social engineering is still in its infancy as far as formal definitions, attack frameworks, examples of attacks and detection models are concerned.

Due to the increase of Information system security incidences, organizations and governments are working towards securing sensitive information to gain the trust of clients and citizens. To achieve this we must invest on research to come up with measures for mitigation of social engineering attacks. Human form the weakest link in information security system and they can easily influenced or manipulated to divulge sensitive information that allows unauthorized individuals to gain access to protected systems.

The biggest challenge at hand is how individuals can successfully detect this vishing attacks. This study aims at coming up with vishing attack detection model to enhance detection of vishing attacks by mobile phone users to successfully detect social engineering attacks, government and financial institution, as a training tool to create awareness on vishing attacks will use the model.

1.6 Motivation of the study

Research on social engineering has not received attention the same attention as the technical comonets of software and hardwares in the Information and technology centre thus the human factor has been on the attack. Many Mobile users in Kenya have been in the receiving side of this vice and cases of social engineering attacks have been on the increase especially with the inception of mobile money transactions services such as M-Pesa, aitel money and equitel. criminals have therefore devised ways of gaining access to individual’s accounts through vishing attacks. The aim of this study was to identify factors influencing vishing attacks and to develop a model that would aid in the detection if vishing attacks reducing on the incidences.

1.7 Scope of the study

The study focussed on phishing attack on mobile devices can be categorized into Bluetooth phishing, Short Message Service (SMS) phishing, Mobile Web/ Application and Voice over IP Phishing or known as vishing. In addition, the research sought to focus on coming up with a model that could be used by mobile users for detection of vishing attacks that would be used by mobile users, Banks, government and service providers to detect vishing attacks.

1.8 Limitations of the study

Phishing attack exist in three major forms on mobile devices namely Voice over IP Phishing or known as vishing, Bluetooth phishing and Short Message Service (SMS) phishing and the study was limited only to vishing attacks . In addition the study was confined only to individuals who had visited the customer care centres seeking help on operating their mobile services and reporting of social engineering attacks.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

The research done by (Luo *et al.*, 2011) found that when people talk about information security, it's very common to think about threats that can be contained with the help of technical countermeasures such as email filters, network filters, anti-viruses and likes; however, there is a more elusive form of danger to which there in no obvious solution. Due to the "good nature" of human beings, they tend to be more vulnerable to social engineering attacks.

According to Centre for the Protection of National Infrastructure (CPNI, 2016) social engineering has been defined based on psychological and security terms by various organizations and people. Cert-UK defines social engineering as "The manipulation of individuals in order to induce them to carry out specific actions or to divulge information that can be of use to an attacker." (Mouten, *et al.*, 2014) Defines social engineering as, the science of using social interaction as a means to persuade an individual or an organization to comply with a specific request from an attacker where either the social interaction, the persuasion or the request involves a computer-related entity. In order to curb Information security incidences we must look beyond the technical aspect of protection and consider the weakest link in security.

Many Mobile users in Kenya have been in the receiving side of this vice, many are time users receive calls from persons purporting to be from customer care of known service provider with series of questions, wittingly persuading individual to give out sensitive information. Time by time this individual send text purporting to be recruiting people for jobs and requesting for cash. In Garissa IFMIS passwords of a senior county staffs were stolen and used to make illegal payments, under the Ministry of Devolution, stole credentials were used to access the system and approve fraudulent tender requests (Kigen *et al*., 2015).

According to Muthengi, (2015) “Cybercriminals have their eyes on the M-Pesa (in Kenya) platform. Users therefore need to exercise great caution and use common sense in the event of potentially fraudulent transactions. Over the years, since mobile money transactions services such as M-Pesa gained ground, criminals have always devised ways of gaining access to individual’s accounts”.

2.2 Social Engineering Attack Framework

According to Mouten *et al*., (2014) proposed a social engineering attack framework based on Kevin Mitnick’s social engineering attack cycle. The attack framework addresses shortcomings of Mitnick’s social engineering attack cycle and focuses on every step of the social engineering attack from determining the goal of an attack up to the successful conclusion of the attack. The authors use a previously proposed social engineering attack ontological model which provides a formal definition for a social engineering attack. The ontological model contains all the components of a social engineering attack and the social engineering attack framework presented in this paper is able to represent temporal data such as flow and time.

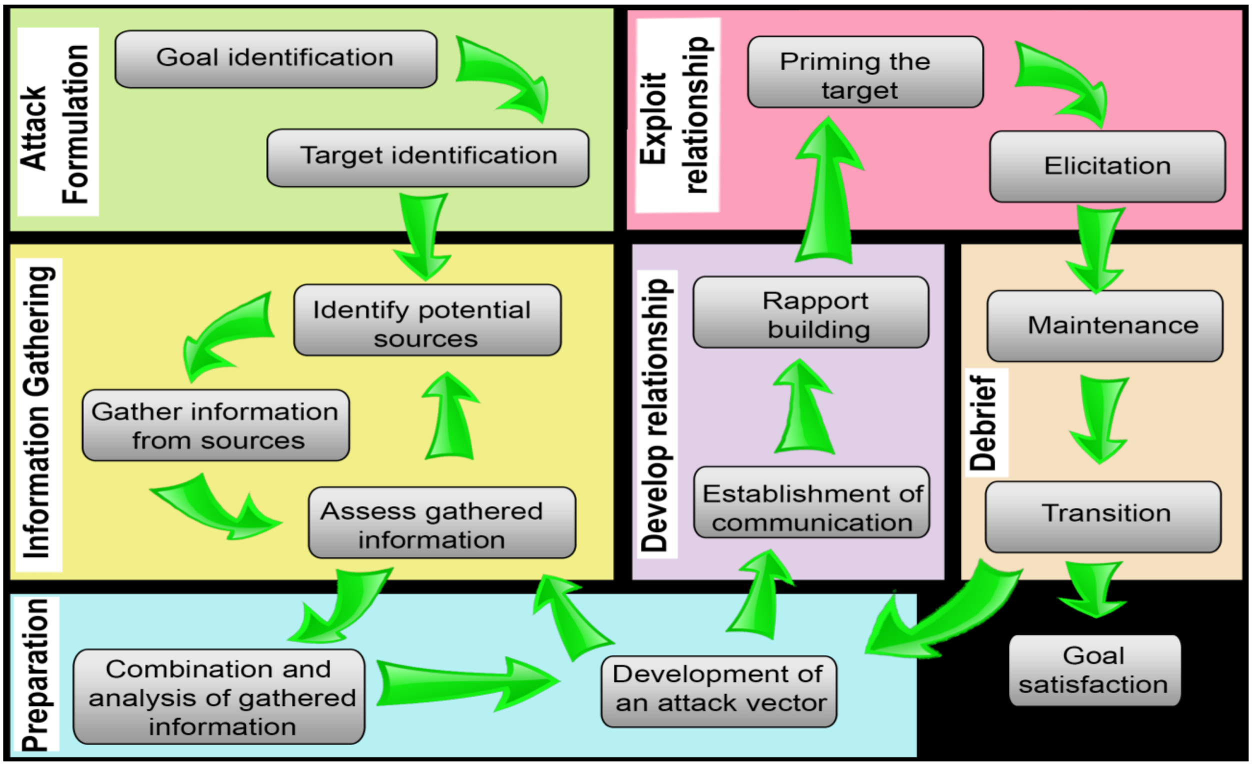


Figure 2.0: Social Engineering Attack Framework (Malan, Leenen, Mouton, & Venter, 2014)

The authors were able to formulate social engineering and a social engineering attack definition; in addition, a social engineering attack framework was developed and verified with real life social engineering scenarios. The proposed framework clarified Miskick's four phases of social engineering attacks that were proposed in his book i.e. Research, Development of rapport and trust, Exploitation and Utilising the information (Mitnick & Simon, 2002) and is more detailed. In this study this phases were well described and further phases were added to clearly define the attack process.

2.3 Social Engineering Defensive Framework (SEDF)

Social engineering defensive framework (SEDF) by Valarie Thomas (Gardner & Thomas, 2014b), was designed to offer assistance by preventing social engineering assaults at the undertaking level. SEDF diagrams defines four important stages for attack counter measure.

The four phases of SEDF are independent of each other and they can be performed according to the need of an organization.

The four phases of social Engineering Defensive Framework (SEDF):

1. Determining exposure: this phase focuses on seeing sites and other available resources as the attacker.

2. Evaluating defenses: this phase can be used to evaluate employee resistance and reaction to simulated attacks.

3. Educate employees: this phase involves teaching employees how attacks are executed and their impacts.

4. Streamlining existing technology and policy: This is through improving effective defensive technologies, which are likely in your environment.

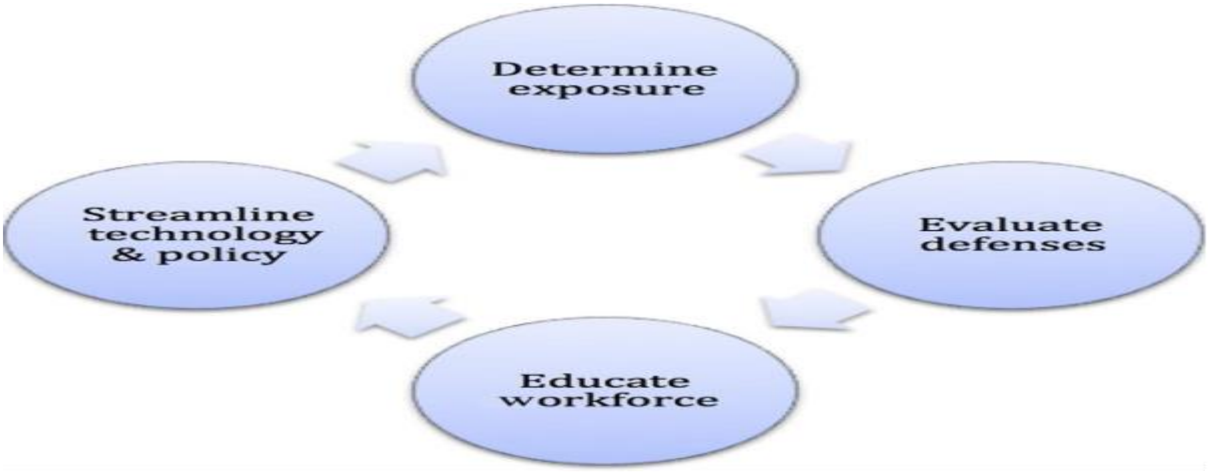


Figure 2.1: Social Engineering Defensive Framework (SEDF) (Valerie Thomas (2014)

2.4 Psychology and Human reasoning

Research shows that social engineers use various psychological vulnerabilities and triggers, to influence the individual's emotional state and cognitive abilities in order to obtain information. According to Bezuidenhout *et. al*. (2010) individual need to have a clear understanding of these triggers in order to recognize each during a social engineering attack. The research done by (Gragg D., 2002) defines the following seven psychological vulnerabilities: Strong Affect, Overloading, Reciprocation, Deceptive Relationship, Diffusion of responsibility and moral duty, Authority and Integrity and Consistency. On their research Bezuidenhout *et. al*. (2010) pointed out is not easy to apply this knowledge to detect attacks due to the human reasoning and decision-making process is extremely complex, and prone to error.

Research shows that human reasoning and decision-making is a complex process, where most decisions that need to be made will not have only one ideal option, and not all people (Stemberg, 2006) will make the same decision. According to Bezuidenhout *et. al*. (2010) individuals will make decision based on the available alternatives and the information they poses on that particular time considering the cost benefit of the outcome. For individual to be able to effectively detect social engineering attacks they must have predefined guidelines, which they can use to make decision.

2.5 Social Engineering Attack Detection Model (SEAD)

Social Engineering Attack Detection Model (SEAD) by (Bezuidenhout, Mouton, & Venter, August, 2010) was designed to be used by call centers workers for detection of social engineering attacks in a call centers environment. The model was designed to quick and effectively determine if the requester is trying to manipulate an individual into disclosing information to which the requester does not have authorization for. The model seeks to assist individuals in decision-making in call centres environment before relieving any information. This can be shown on fig 2.2 Below:

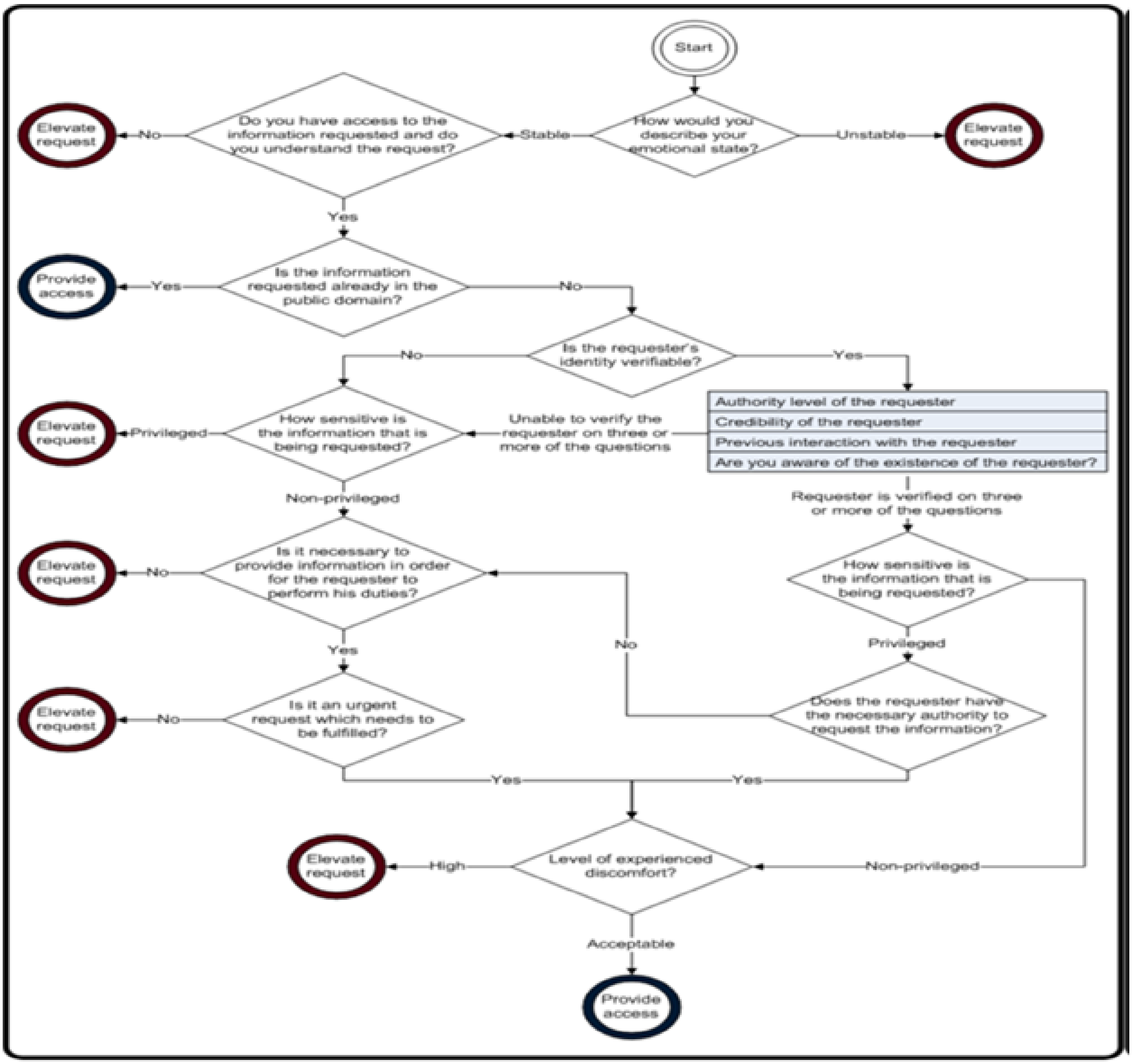

Start
How would you describe your emotional state?
Unstable
Elevate request
Stable
Do you have access to the information requested and do you understand the request?
No
Elevate request
Yes
Is the information requested already in the public domain?
Yes
Provide access
No
Is the requester's identity verifiable?
No
Yes
Authority level of the requester
Credibility of the requester
Previous interaction with the requester
Are you aware of the existence of the requester?
Unable to verify the requester on three or more of the questions
How sensitive is the information that is being requested?
Privileged
Elevate request
Non-privileged
Requester is verified on three or more of the questions
Is it necessary to provide information in order for the requester to perform his duties?
No
Elevate request
How sensitive is the information that is being requested?
Yes
No
Privileged
Is it an urgent request which needs to be fulfilled?
No
Elevate request
Does the requester have the necessary authority to request the information?
Yes
Yes
Level of experienced discomfort?
High
Elevate request
Non-privileged
Acceptable
Provide access

Figure 2.2: Social Engineering Attack Detection Model (SEAD) (Bezuidenhout, Mouton, & Venter, August 2010)

2.6 Mobile Antiphishing Techniques

With research on phishing detection technique, we can contribute to mitigation of phishing attack on mobile platform. Various detection technique have been proposed in different studies. According to Xiang, *et al.*, (2011) they listed two phishing detection techniques such as blacklist and feature-based. (Huh and Kim, 2012) further listed three types of detection techniques such as blacklist, whitelist and heuristic. In addition, (Zhang *et al.*, 2007), listed blacklist and heuristic as common phishing detection. The most implemented detection technique on vishing is the blacklist technique according to the research done by (Cik *et al.* 2013). This technic has its strength and weakness, it can be able to detect vishing attacks effectively but its accuracy depends on the update of the blacklisted telephone numbers on the database. As studied by (Sheng, *et al*, 2009), blacklists are found to be ineffective against zero-hour phishing attacks, and were able to detect only 20% of them.

2.6.1 MobiFish

MobiFish is a lightweight scheme for mobile phones which was designed to verifies the validity of web pages and applications (Apps) by comparing the actual identity to the identity claimed by the web pages and Apps (Wu, .Du, & Wu, 2014). For verification of website, MobiFish uses OCR text extraction tool Tesseract, in order to verify the legitimacy of a website. OCR open source tool known as Tesseract. MobiFish scans the URL to check if it is an IP Address. If IP Address is detected then the user is warned about the possible phishing attack. In the second stage, it scans to check if the website contains any login form, if detected then the tool extracts second level domain (SLD) name from the URL. MobiFish compares the SLD against its brand name using the generated mapping list. OCR tool converts the screen shot of the captured webpage into text. If there are certain sensitive terms in the text then the user is warned. If SLD is not present in the text that is extracted from the screenshot then it is possibly a phishing web page.

2.6.2 MPSheild

According to Bottazzi, Giovanni, *et al.*, (2015) implemented MPSheild as a proxy service on top of TCP/IP stack. It inspects the IP packets that have originated from the mobile application. It extracts the HTTP gets request from the IP packets. The target URLs are extracted from the HTTP get request. The URLs are sent to Watchdog the check whether the URL is blacklisted or not. If yes then warning is sent to the user else the URL is sent to the classification engine where various features are analyzed and the URL is classified as suspicious or genuine.

2.6.3 Telephony fraud prevention

Telephony fraud prevention technique was designed for guarding against telephony-based fraud that includes, at a telephony device, identifying a caller ID of an incoming call or a dialled number of an outgoing call attempt or a number to be dialled. The identified caller ID or dialled number or number to be dialled was then compared against a blacklist of telephone numbers. In the event that a match was found, a Warning was presented to a user of the device and/ or the call or call attempt was terminated (Devinder Singh, *et al*. 2011). The method presents more con’s than pro’s. (Sheng, *et al.* 2009) noted that this technique has less capabilities to protect users. In addition, this method is not suitable to detect new phishing attack as depends on blacklisted telephone numbers.

2.6.4 iVisher: Real-Time Detection of Caller Spoofing

iVisher is a system used to mitigate vishing attacks by detecting whether a given number displayed on a phone screen has been modified by means of spoofing. iVisher authenticates the caller ID of an incoming call and blocks previously reported caller IDs by performing reachability analysis to the display name of a suspicious incoming call (that is, a display name suspected of caller ID spoofing). This analysis uses a gateway (that knows the actual caller ID of the call) in the handling of reachability analysis messages that are attempting to corroborate the actual caller ID and the display name (Song, *et al.* 2014). Modern methods used for vishing attacks don’t need to hide phone numbers to execute attack. According to research done by (Choi, *et al.* 2015) found that when the calls are made internationally, complex dispatch routes are used to present it as a domestic call, which also complicates the investigation process for locating the caller. Moreover, phishing organizations use complex reception routes to evade capture by law enforcement.

2.7 Voice phishing fraud

The situational context and characteristics of voice phishing have not been sufficiently understood, and there is a lack of the theoretical background needed for establishing suitable countermeasures (Choi, Lee, & Chun, 2015). Through script analysis they were able to come up with the sequential steps used in vishing attack. This was a major step in understanding the operation of social engineers. The crime script analysis showed that voice phishing crimes could be divided into the preparation, recruiting telemarketers, script composition, making phone calls, having conversations, deposit and withdrawal, and money transfer stages. They further categorized the process into three according to Clarke and Cornish (1985) who argued that it was appropriate to categorize the process of committing an offense into three steps of pre-crime (that is, offense planning), criminal event (that is, offense strategies) and post-offense (that is, aftermath). These stages are the following:

Pre-crime stage: According to their study, this stage comprised of the following phases:

Preparation

Voice-phishing criminal organizations are comprised of different teams with distinct duties related to Information Technology (IT), telemarketing, script, bank accounts, money withdrawals, money transfers and mobile phones. Each unit performs vital functions for the headquarters. Regarding the specific tasks of each unit, the IT team operates an Automatic Calling Program (ACP) and directs the calls to a consulting agent when a potential victim answers the phone. Individuals who can speak fluent language of the victim constitute the telemarketing team. The script team is in charge of creating diverse scenarios and developing situational responses. The bank account team opens false bank accounts to use when receiving money from the victims. The transfer team receives money from the money withdrawal team and delivers it using an illegal remittance system. Lastly, the mobile team prepares phones under false identities (Choi, et al., 2015).

Recruiting telemarketers

This phase involves recruitment of telemarketers; Voice-phishing criminal organizations invest much effort into recruiting telemarketers who can speak the language of the victim fluently without any accent. This is because even the slightest indication of being a foreigner could plant a seed of doubt in the minds of potential victims.

Research shows that the reason why many Asians participate in the crime by playing the role of telemarketer is because the benefits outweigh the risks (Choi, *et al.,* 2015).

Script composition

Various scripts are composed to allow telemarketers to make apposite responses in a variety of situations. Each script is prepared in detail, and the scenarios are composed according to the agency that the telemarketer is supposed to represent (Choi, *et al.*, 2015).

Criminal event stage: consists of the following phases

Making the phone calls

The IT team to make random calls that are transferred to a telemarketer when a victim answers usually uses an automatic calling program. When the calls are made internationally, complex dispatch routes are used to present it as a domestic call, which also complicates the investigation process for locating the caller. Moreover, phishing organizations use complex reception routes to evade capture by law enforcement. By registering as international telephone businesses or Internet phone businesses, the offenders take advantage of the complicated system that makes it difficult, both technologically and legally (Choi, et al., 2015).

Conversations

The perpetrators pose as legitimate entities, including the police, the prosecutor’s office, financial institutions and public agencies (Choi, et al, 2015).

Post-offense stage

Deposit and withdrawal

An account opened under a false name is used to deposit money from the victim, this When prevents investigators from tracing the transactions. The money withdrawal team shares their information with the telemarketing team. After communication, the withdrawal team pulles out the money deposited by the victims. As the managers of the money withdrawal team use phones under false identities, it is difficult to apprehend them even when the individuals running errands for the organization are arrested (Choi, et al, 2015).

Money transfer

Is the last phase of vishing, where the money is transferred to the country where the vishing organization is located (Choi, et al, 2015).

As it can be noted above these are well organized criminals with all resources need to hack human beings. The government and the citizens need to be informed on this process in order to be able to defend themselves on such. The research done by (Alnajim and Munro, 2008) categories the defense mechanism into technical and training techniques. If we can be able to achieve this, we can easily mitigate vishing in our networks.

2.8 Knowledge Gaps.

Literature shows that vishing criminals are well organized on their attacks, which make even harder for them to be caught prosecuted because they tend to hide any link into their activities. According to research conducted on voice phishing in South Korea, the crime is usually committed through a systematic division of labour, including individuals acting as the managing director, the script writer, the caller, the bank account manager and the people in charge of withdrawing and transferring money. This allows each individual to perfect his or her role.

Blacklist detection technique is the most common deployed technique for vishing detection in mobile devices. The type of detection technique according to research has more con's than pro's. Research shows that this method is not suitable to detect new phishing attack as it depends on blacklisted phone numbers to detect fraud (Xiang, *et al*., 2011). Moreover, this technique is also not efficient in update and verifieing the phishing attack database globally according to the research done by (Huh and Kim, 2012). In addition on their research (Sheng, *et al*., 2009) noted that this technique had less capabilities to protect users.

iVisher detection system was designed to unmask the concealed phone numbers by showing the real name of the caller, according to the research done by (Song, *et al*., 2014). iVisher could not protect users completely. Research shows that with modern technology, one needs not to conceal the phone number but to complicate the calling and receiving process, which complicates the investigation process (Choi, *et al*., 2015).

Human reasoning and decision making is a complex process, individual make decision on the bases of the possible alternatives and the information they have. Research shows people without set of predefined value will make decision based on their current context and the demand of the decision (Braisby and Gellatly, 2005). Therefore a guideline is needed that will help in detection of vishing attacks on mobile platform.

SEADM model was developed with call centre environment perspective and it focused only on such environment to help employees working in a stressful environment to successfully detect social engineering attacks. The model targets to help employees in detection of social engineering attacks, which limits its application area. Social engineer on mobile platform targets personal information which can be used against the mobile user, and the scripts created in this two environments are different hence the need for a model that fits mobile users. On mobile platform the user has no option of elevating the request to a third part for assistance, the owner must take full responsibility of the decisions to be made hence making SEADM inapplicable in such environment.

Mobi-phish was designed to verify the validity of web pages and applications (Apps) by comparing the actual identity to the identity claimed by the web pages and Apps. The performance of the scheme is highly dependent on the accuracy of the external OCR tool used for snapshot to text conversion. This limits its performance. Other URL parameters can be added to improve the performance the tool. MPSheild depends on black listed URL to detect phishing attacks; the list needs regular updates for its performance.

The phishing problem is broad and no single silver-bullet solution exists to mitigate all the vulnerabilities effectively, thus multiple techniques are often implemented to mitigate specific attacks (Khonji *et. al.*, 2013). This study proposes a model for detection of vishing attacks for mobile platform, making use of a decision tree, by breaking the process down into more manageable components, and guidelines to aid decision-making.

2.9 Conceptual Framework.

The research adopted the conceptual model of the major aspects of social engineering-based attack by L. Janczewski and L. Fu (2010) as it meets all the objectives of the study as shown in Figure 2.3 below.

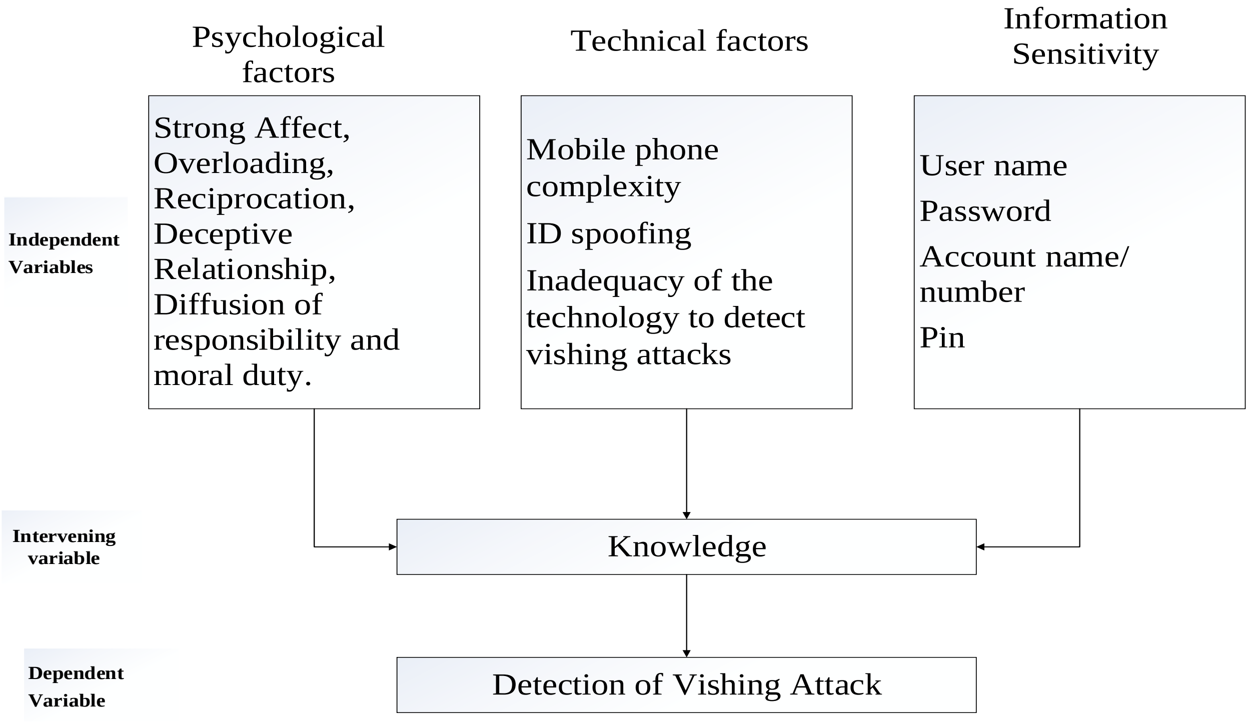


Figure 2.3: conceptual framework

The researcher sought to investigate the psychological vulnerability as proposed by Gragg D. (2002), which defines the following seven psychological vulnerabilities: Strong Affect, Overloading, Reciprocation, Deceptive Relationship, Diffusion of responsibility and moral duty, Authority and Integrity and Consistency. Technical vulnerability that contribute to vishing attacks on mobile platform and finally Information sensitivity, which is key in detection of vishing, attacks. The independent variables were used to form control variables, which will be used by mobile users to effectively detect vishing attacks. Research shows that lack of knowledge is the main contributing factor in the success of vishing attack. People need to be informed to be able to make informed decision in case of an attack.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter presents the methodology used in this study. The research design, target population, sample size, sampling technique, data collection and data analysis has been outlined.

3.2 Research Design

This study used the survey research design, which was cross-sectional because it was carried at one point in time. According Robson (2011), survey research seeks to obtain information that describes existing phenomena by asking individuals about their perceptions, attitudes, behavior or values. For this study, it enabled the researcher to seek information from mobile users and IT managers on their knowledge on vishing attacks.

This research focused on mobile phone users to ensure the availability and genuineness of information concerning social engineering attacks in Kenya. Kothari (2004) points out that an optimum sample is one that has the ability to fulfill the requirements of efficiency, representativeness, reliability and flexibility.

The objective populace for this study includes Mobile phone users; IT practitioner's and service providers in Nairobi County. Thus, the researcher approximates a population of 200 respondents.

3.3 Sampling Design and Sample Size

According to Mugenda and Mugenda (2013), a good population sample lies within 10% to 30% of entire population. In defining, the sampling procedures this research study employed stratified random sampling. Taking an approximate population of 200 respondents, the sample size will be 10/100*200= 20. Therefore, from this formula twenty respondents who are Kenyan citizens (20) were selected as respondents for this study. Proportionate sampling of the respondents with the two major networks i.e. Safaricom and Airtel was done, with ten (10) respondents being sampled from each. Random sampling of the respondents was done with the researcher having to count every 20th person who visited the customer care center for the various networks.

Crouch & McKenzie (2006) propose that less than 20 participants in a qualitative study helps a researcher build and maintain a close relationship and thus improve the “open” and “frank” exchange of information. This can help mitigate some of the bias and validity threats inherent in qualitative research. In quantitative research sampling, the size of the sample is determined by the optimum number necessary to enable valid inferences to be made about the population. The larger the sample size, the smaller the chance of a random sampling error, but since the sampling error is inversely proportional to the square root of the sample size, there is usually little to be gained from studying very large samples. The optimum sample size depends upon the parameters of the phenomenon under study, for example, the rarity of the event or the expected size of differences in outcome between the intervention and control groups (Marshall, 1996).

Based on the above studies, and the nature of this research that mobile platforms use standard metrics across the world, sixteen respondents were good enough to produce better results since from the fourteen respondents the sample size had reached saturation or redundancy. This study therefore, focused on only twenty (20) respondents. However, sixteen respondents were reached. These are the respondents the researcher got relevant data that was used to show the impact of vishing on mobile users.

In addition, the researcher purposively selected bank mangers of various banks, which included Equity bank, Barclays bank, Cooperative bank, National bank, Family bank, Stanbic Bank and Kenya Commercial bank. Who served as key informants to the study providing in-depth information on cases handled in the banks as a result to vishing.

3.4 Data collection tools and procedure

The research used self-administered questionnaire and interview schedules for data collection.

3.4.1 Questionnaire

Data from the respondents was collected by use of a self-administered questionnaire since it guaranteed anonymity and confidentiality. Kothari (2004) stipulates that use of the questionnaire is one of the major ways to elicit self-reports on people's opinions, attitudes, beliefs and values. The questionnaire contained closed-ended questions to provide specific responses and open ended items for in depth information. Open ended questions permit a greater depth of response and give an insight into the respondents' feelings, backgrounds, hidden motives and intentions (Mugenda and Mugenda, 2012).

For the administration of respondent questionnaire, the researcher visited Safaricom and Airtel customer care centre with Nairobi CBD. The researcher approached the clients getting in to be served and engaged them by creating a rapport between the researcher and respondent explaining the purpose of the study. Respondents' consent to participate in the study was sought who upon consenting would sign the consent form and a questionnaire was then handed over for them to fill.

3.4.2 Interview guides

The researcher conducted a total of seven key informant interviews using a semi structured interview schedule. This was done to gather in depth information from the researcher ICT mangers of various banks, which included Equity bank, Barclays bank, Cooperative bank, National bank, Family bank, Stanbic Bank and Kenya Commercial bank. Who provided in-depth information on cases handled in the banks as a result to vishing.

The interviews were done face to face through direct personal investigation; hence the researcher collected information personally by writing. For the administration of interview, the researcher booked an appointment with each key informant who was purposively selected for the study. These face- to -face interviews lasted not more than fifteen minutes and took place at their various work stations and offices.

3.4.3 Pre-testing

Before commencing the study, pre-testing of the study instruments was conducted. The aim of pre-testing was to assist in determining accuracy, clarity and suitability of the research instruments and to check their validity and reliability (Mugenda and Mugenda, 2012). The pre-testing study was conducted among respondents who had visited Thika Safaricom customer care centre involving a total of five respondents who had a high propbability that they could not be duplicated in the main study. Adjustments were made in order to make to make the research instruments more appropriate before the actual field work begun. The responses derived from the pretest were used by the researcher to refine the questionnaire by rephrasing and editing thus ensuring that the questions conveyed the same meaning to all respondents. The pretest enabled the researcher to test the appropriateness of the study tool by ensuring that items tested what they were intended to (validity) and that they consistently measured the variables in the study (reliability). It also helped to estimate the length of time for the administration of instruments.

3.4.4 Validity and Reliability of instruments

Validity refers to the extent to which an instrument measures what it is intended to measure based on objectives (Kothari, 2004).To enhance validity of the research instruments, peer review was done where the study proposal was presented twice at the department. Consistent consultations were done by the researcher together with supervisors and other expatriates who were knowledgeable in model development for IT study. This helped in establishing ambiguous questions and missing gaps in the questionnaire, and corrections were made on research items that were not clear before being used in the actual stud

Reliability of measurement is the degree to which a particular measuring procedure gives similar results over a number of repeated trials thus, pre-testing is a good way to check for reliability of the data collection instruments (Kothari, 2004).Reliability test was conducted for the likert scale items using Statistical Package for Social Sciences (SPSS) where internal consistencies were analysed using Cronbachs coefficient alpha. The results of Cronbachs Coefficient Alpha yielded a value of 0.78 which was acceptable. According to Streiner and Norman (1989), a Cronbach Alpha Value of 0.70 or higher is considered good enough. Thus it indicated that the items selected for measurement of variables were reliable measures.

3.5 Data Analysis and Presentation

This study generated both qualitative and quantitative data. Quantitative data collected was analyzed using the Statistical Package for Social Sciences (SPSS). Descriptive statistics of frequencies and percentages were used to describe and summarize data. Data presentation was done through tables. Information generated was also statistically analyzed so as to elaborate on factors that contribute to vishing attacks. Qualitative data from the Key informants was presented in narrative form, highlighting respondents' voices to compliment some of the quantitative findings.

3.6 Ethical Considerations

Neumann (2003) explains that the term ‘ethical’ is used to mean principle of conduct that is usually considered accurate, particularly by people of a specified group or profession. Research activities may provoke ethical issues concerning the rights of respondents especially the right of privacy. The researcher obtained an informed consent of the respondents before he could issue them with questionnaires. Additionally, the researcher ensured that the respondents were aware of the information needed from them, the reason for seeking the information and its purpose. Anonymity and confidentiality of all participants was maintained.

`

CHAPTER FOUR

DATA ANALYSIS FINDINGS AND DISCUSSION

4.1 Introduction

This chapter presents the data analysis, design and development of the model. The findings are presented according to the described methodology, the conceptual framework and the study objectives such that the research questions are answered. The results in this section are from the analysis of data collected.

4.2 Response Rate

From the questionnaires distributed to the mobile users with IT related backgrounds, 16 of them were filled and returned. This translated to 80% response rate, which the researcher considered appropriate to facilitate in making conclusions and recommendations.

4.3 Socio- Demographic characteristics of respondents

To capture general information, the researcher sought to establish the gender, age, education level and the position of the respondents. Table 4.1 below illustrates the findings, in regard to gender 31.25% of the respondents were female and 68.75% of the respondents were male, this is due to the fact that technology field is male dominated field. Majority of the respondents 62.6% were aged between 30 to 40 years.

The researcher sought to establish the education level of the respondents. The analysis demonstrated that respondents with postgraduate studies recorded the highest percentage of 50%, This covered those who had masters and doctorate. The 25% represents those who are University graduates, holding a degree, 12.5% represents those with collage certificates and 12.5% represent those with high school certificates. In addition 62.6% of the respondents were employed.

Table 4.1: Socio Demographic Characteristics of respondents

Socio demographic factors	Frequency (n=16)	Percentage %
Gender		
Male	11	68.75
Female	5	31.25
Age		
20 – 24 years	1	6.3
25- 29 years	2	12.5
30-34 years	5	31.3
35-39 years	5	31.3
40-44 years	2	12.5
45 and above	1	6.3
Education level		
Secondary	2	12.5
College	2	12.5
Bachelors Degree	4	25
Masters Degree	6	37.5
Doctorate Degree	2	12.5
Work status		
Employed	10	62.6
Self Employed	6	37.5

4.4 Study Variables

4.4. Establish factors contributing to Vishing attacks

The study sought to find out how many people had been victims of social engineering attacks. Majority of the respondents 87.5% had been victims of social engineering attack with 50% experiencing social engineering attacks to a great extent, 25 % to a very great extent. And only 12.5% of the respondents had not experienced social engineering attack.to a great extent been victims of social engineering attacks some with the attacks being successful and others failing.

Table 4.2 Exposure to vishing attacks

Victim of Social engineering attack	Frequency	Percent
Not at all	2	12.5
to a small extent	2	12.5
To a great extent	8	50.0
To a very great extent	4	25.0
Total	16	100.0

4.4.1 Exposure to vishing attacks due to technical factors- Mobile complexity

The researcher sought to establish technical factors due to mobile complexity that exposes mobile phone users to vishing attacks in the country. Majority of the respondents 56.3% reported that their phones had some complexity, 25% too much complexity; hence, the complexity on the use of their mobile phone was making them prone to vishing attacks. These findings are similar to Bruce Schneier (2000) who noted that future of digital systems will be complex, and complexity is the worst enemy of security since the more the complex the system is the harder the user to understand it.

Table 4.3 Exposure due to Mobile complexity

Mobile Complexity	Frequency	Percentage
Very little complexity	1	6.3
Little complexity	2	12.5
Some complexity	9	56.3
Much complexity	4	25.0
Total	16	100.0

4.4.2 Exposure to Vishing Attacks Due to Psychological Factors

Findings reveal that half the respondents 50% and 37.5% attested that psychological factors had a significant and critical potential respectively in exposure to vishing attacks. Social engineers prefer to hack human beings rather than system with security measures in place. This findings were similar to (Bezuidenhout, Mouton, & Venter, August, 2010) who agreed that people lack knowledge on vishing engineering making them more vulnerable. This was supported by the IT managers interviewed agreed that human psychological factors were potentially critical in causing vishing attacks to customer's mobile phone.

Table 4.4 Exposure due to human factors

Human factors	Frequency	Percent
Very little potential	1	6.3
Some potential	1	6.3
Significant potential	8	50
Critical Potential	6	37.5
Total	16	100

Social engineers prefer to hack human beings rather than system with security measures in place by playing with their psychology. They do this by triggering the emotions of their victims either making them to happy or instilling stress, and also disseminating too much information to the victim and not giving them ample time to rationally think through/process the information they have received thus slowly become vishing attack victims. This was attested by one of the respondents who said

> *"I received a call from my equitel line informing me they are calling me on behalf of the bank to notify that my account is being swindled and they wish to help me secure it. I out rightly panicked and was ready to follow all the instructions they gave to help*

> *secure my account. Which we did step by step without any question. Interestingly, the caller did not ask me for the pin. Right after the conversation with caller and hanging up, did I start to think through the entire incidence. I did call the bank which confirmed my worst fears that I had just been conned... it was so depressing of how easily I could fall to such a scam….and yes just to confirm that human factors make us prone to vishing attacks."* Respondent 13

4.4.3 Exposure to Vishing attacks due to mobile banking services

The researcher sought to establish if the respondents who had registered to any mobile banking services exposed them to attacks. The analysis showed that 100% users of the respondents were registered to M-pesa mobile money service hence the highest targeted mobile money service by attackers, 62.5% of the respondents were registered to Equitel mobile money service, 31.25% of the respondents were registered to Airtel money services and 25% to Branch mobile money service.

Table 4.5 Exposure due to mobile banking services.

	Mpesa		Airtel		Equity		Branch	
Extent to services	F	%	F	%	F	%	F	%
Not at all			11	68.75	6	37.5	12	75.0
To a small extent			2	12.5	1	6.25	2	12.5
To a great extent	0	0	1	6.25	1	6.25	1	6.3
Very great extent	16	100	2	12.5	8	12.5	1	6.3
Total	16	100.0	16	100.0	16	100.0	16	100.0

4.4.4 Establishing consequences of vishing attacks

The researcher sought to establish the most experienced loss by mobile users. The analysis showed that 100% of the respondents believed that the financial loss and loss of data were the greatest consequences of vishing attacks as illustrated in Table 4.5. This was followed by leakage of personal information 62.5%. These findings were similar to Janczewski & Fu (2010) that the major loss incurred after a successful vishing attack is available. This was supported by IT managers interviewed who attested receiving a lot of claims of money lost by their clients after encountering a vishing attack..

Table 4.5 Loss due to social engineering attacks.

	Loss of Data		Personal Information		Theft of goods		Financial loss	
Extent to services	F	%	F	%	F	%	F	%
Not at all	0	0	3	18.75	6	37.5	0	0
to a small extent	0	0	2	12.5	1	6.25	0	0
To a great extent	0	0	1	6.25	1	6.25	0	0
To a very great extent	8	100	10	62.5	8	12.5	16	100
Total	16	100.0	16	100.0	16	100.0	16	100.0

4.4.5 Knowledge of Social engineering attacks

The research sought to find out if people were knowledgeable about the various strategies used by social engineers attack. The researcher found that none of the respondent had some or much knowledge on vishing and smshing. Half the respondents 50% had very little knowledge and 50% little knowledge on vishing attacks. 62.5% of the respondent had little knowledge on smshing attacks and 37.5% had very little knowledge on smshing attacks. This finding was similar to (Bezuidenhout, Mouton, & Venter, August, 2010) who found that lack of knowledge is the key contributing factor to the increase of social engineering attacks.

Table 4.6 Knowledge of social engineering attacks on mobile platforms

Knowledge level	Vishing		Smshing	
	Frequency	Percent	Frequency	Percent
Very little	8	50	6	37.5
Little	8	50	10	62.5
some	0	0	0	0
Much	0	0	0	0
Total	16	100	16	100

4.4.6 Establish attack methods used by Social engineers

The researcher sought to establish the commonly used form of attack by social engineer. The researcher found that the mostly commonly used form of attack was vishing with 75% indicating to have experienced vishing attacks to a very great extent, 12.5% to a great extent and 12.5% to a small extent. These findings are similar to (Choi, *et al*., 2015), who noted that most of the social engineer prefer vishing attack due to the fact that they can easily sense the emotions of the victim through the voice.

Table 4.5 Loss due to social engineering attacks.

	Bluetooth		Mobileweb		SMSishing		Vishing	
Extent of attack	F	%	F	%	F	%	F	%
Not at all	11	68.8	8	50.0	5	31.3	0	0.0
to a small extent	4	25.0	4	25.0	4	25.0	2	12.5
To a great extent	1	6.3	4	25.0	6	37.5	2	12.5
To a very great extent	0	0.0	0	0.0	1	6.3	14	75.5
Total	16	100.0	16	100.0	16	100.0	16	100.0

4.4.7 To Establish defence mechanisms used by mobile users.

The researcher sought to establish the mechanism used by mobile users in defending themselves against vishing attacks. The researcher found that most of the users used content based defence mechanism to defend themselves. 75% to a very great extent, 6.3% to a great extent and 3% to a small extent. This finding is similar to Dunham (2009) who found that individual preferred to use content base mechanism in defending against social engineering attacks due to its simplest.

Table 4.6 Defence mechanisms against Vishing attacks

	Content based		Blacklist		Whitelist		Policies	
Defence used	F	%	F	%	F	%	F	%
Not at all	0	00.0	6	37.5	12	75.0	10	62.5
to a small extent	3	18.8	3	18.8	3	18.8	1	6.3
To a great extent	1	6.3	1	6.3	1	6.3	4	25.0
To a very great extent	12	75.0	6	37.5	0	00.0	1	6.3
Total	16	100.0	16	100.0	16	100.0	16	100.0

4.4.8 Detection of vishing attack

The researcher sought to find out if respondents were aware of being in a position to detect a vishing attack beforehand. More than half of the respondents 68.8% revealed that they did not have the ability and it was difficult to detect vishing attacks. Whereas only 31.2% said they were in a position to detect vishing attacks as illustrated on Table 4.7 below and respondents responses.

"No I think its hard to detect a vishing attack because the callers talk with a lot of confidence and they seem to be able to relay information that looks so real and quite applicable to your situation and seem to be quite knowledgeable." Respondent 3

“Yes; I am able to detect a vishing attack since they are over confident and once you try to enquire more information about the matter they seem to be agitated or once you request for time to think/consult they are hesistant ” Respondent 8

Table 4.7 Ability to detect vishing attacks

Ability to detect vishing attack	Frequency	Percent
Yes	5	31.25
No	11	68.75
Total	16	100

4.5 Model development

Based on the analysis on the information gathered from the questionnaires and key informants a model was developed. Psychological factors, technical factors and information sensitivity factors come out as the main contributing factors to vishing attacks. Psychological awareness and information security training emerged as main control factors in defending against vishing attacks. To develop the rule-based model, the researcher followed the following steps as proposed by (Robert *et. al*. 1990)

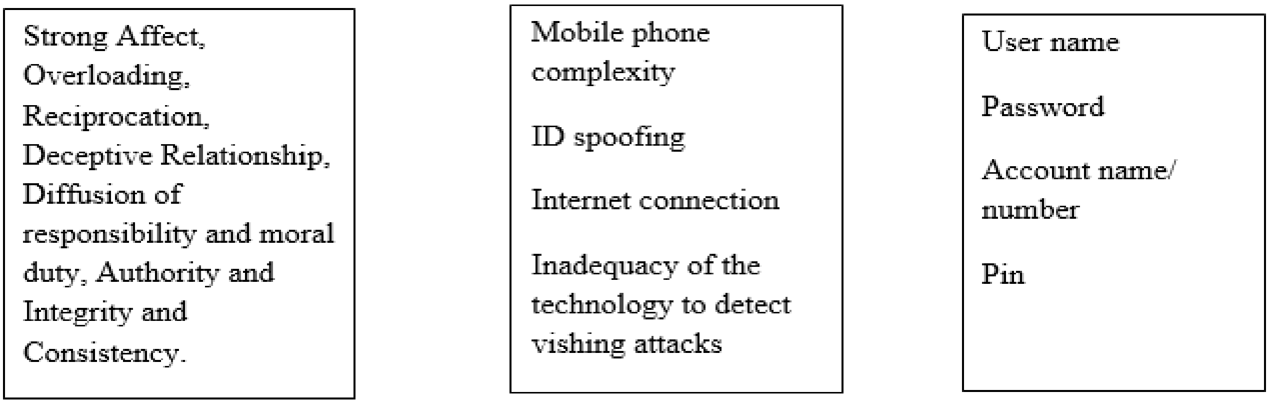
1) Segregating Control Variables:

Through literature review and data, analysis the research found that technology and people formed the two major vulnerability that could be easily exploited by social engineers on mobile platform. The researcher added information sensitivity as key factor in detection of vishing attacks.

SEADM developed by (Bezuidenhout, Mouton, & Venter, August, 2010) used only the psychological and information sensitivity vulnerabilities in detection of social engineering attacks. In addition to this vulnerabilities the researcher added technical vulnerability for detection of vishing attacks.

The researcher was able to flag and separate the following variables to be used as control variables:

Independent Variables:



Strong Affect, Overloading, Reciprocation, Deceptive Relationship, Diffusion of responsibility and moral duty, Authority and Integrity and Consistency.

Mobile phone complexity

ID spoofing

Internet connection

Inadequacy of the technology to detect vishing attacks

User name

Password

Account name/ number

Pin

Intervening variable:

Knowledge

Dependent Variable:

Vishing detection

2) Selection of rules to facilitate in decision-making: The rules have condition and action parts, if and then. On the bases of the available independent variables, the researcher was able to come up with the following rules:

Rule: Emotion

Rule: Script

Rule: Request

Rule: level

RULE phone_no

These rules were implemented with the use of if and then condition to aid in decision making during phone conversation.

3) Dividing the Rules into Groups: The researcher partitioned the rules based on the flow of data between them. The flow of vishing attacks follows a particular pattern, from research, developing trust to the execution of the attack. The rules were organized according to this pattern.

```
Group: Strong affect
        Rule: Emotion
Group: Overloading
         Rule: Script
Group: Sensitivity
        Rule: Request
Group: Security
        Rule: level
Group: complexity
        Rule: level
```

4) Identify Local and Nonlocal Facts: A software tool characterizes each fact as either being produced and used entirely within one group (a local or intragroup fact) or being produced or used by two or more groups (a nonlocal or intergroup fact); the latter are flagged.

5) Write External Descriptions for Nonlocal Facts:

The developer of each rule group that produces intergroup facts then provides an assertion or description of the ex- ternally visible properties of each such fact.

```
(GROUP IDspoofing
         (RULE phone_no
               (IF (phone_no = Not recognized)
                   (phone_no = hidden))
```

```
                             (THEN (IDspoofing=likely)))
 (GROUP Complexity
            (RULE level
                    (IF (level =
mplexity = Exploited))

(GROUP Overloading
            (RULE Scrip
                    (IF (Script = Not clear)
                         (Script = Not clarified))
                               (THEN (Overloading)))
(GROUP Strong affect
           (RULE Emotion
                    (IF (Emotion = Unstable)
                          (THEN (strong affect = triggered))
 (GROUP Information
            (RULE Request
                    (IF (Request = password)
                             (Request = pin))
                                  (Request = Username)))
                                      (THEN (Information = sensitive))))
(GROUP Vishing
                    (IF (Strong affect)
                             (IF (overloading))
                                      (IF (Sensitive)))
```

(THEN (Vishing))))

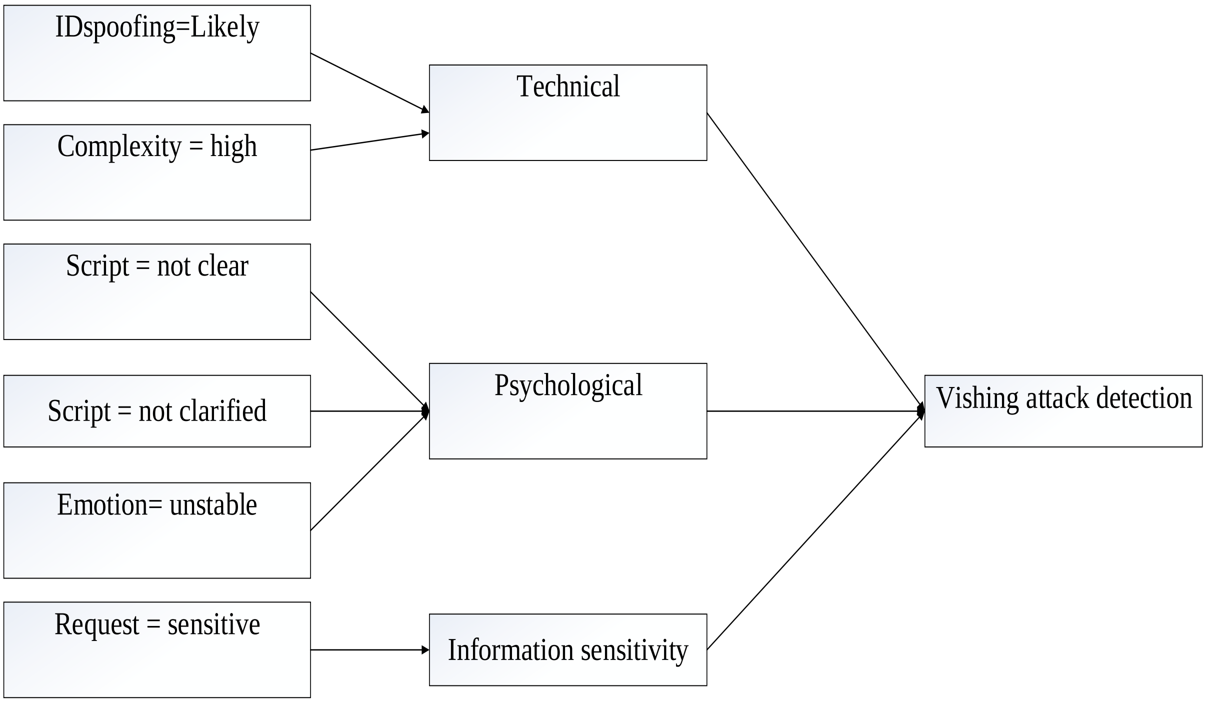


Figure 4.0: Vishing attack detection model.

a) Mobile phone complexity and IDspoofing

This are some of the technical vulnerability that social engineer exploit in vishing attack. If user’s mobile phone lacks security measure like ant spoofing software, hence the security level of the mobile phone is law. Due to lack of security, any call made will be assumed to be a security breach. Literature review and data analysis shows that the more complex mobile phone is the harder to understand it, social engineer take advantage of this to manipulate individuals. IDspoofing is the technology used by social engineer to masquerade their phone ID. It is important to check the identity of the incoming call; this allows you to be alert and anticipate what to expect. The phone numbers on your phone book will show up with the identity of the caller. If the technical security is law, the mobile phone complexity is high and the caller ID cannot be verified then this may be a technical breach, the user should be alert on a scenario.

b) Emotion and Script

Throughout the phone, conversation individual should be conscious of, and able to evaluate their emotional state, on an ongoing basis. Emotions are critical as they influence individual decision making.

In the same manner, the individual should evaluate the emotion the requester elicit within themselves, as the psychological vulnerabilities, that might be triggered by a social engineering attack, is directly aimed to create certain emotional states in order to obtain information.

The research done by (Bezuidenhout *et. al*. 2010) noted that the awareness and consciousness of one's emotional state was not an easy task, or even always a possible task for all individuals. With training and rehearsal this skill can and will improve. For this reason, the authors proposed to develop a quick self-evaluation electronic questionnaire that individuals will be able to use. However, in combination with the model, training by the institution can be emphasized on the various techniques used, the psychological vulnerabilities the attacker may elicit, and institutional policy and procedures.

If at any point the mobile user feels emotionally unstable, he/she can choose to terminate the call or be alert on the conversation.

Every vishing attack follows a developed script and this script is meant for gaining trust. The requester will always create a problem and pretend to offer solution. These scripts always trigger our emotional vulnerability. Individuals should be able to listen to the story carefully and question their emotional state at the same time.

Individuals should not feel pressured to act on anything; they should be able to ask for any clarification. Direct question will always disorient the requester as they always act on a given script. If the emotional state is unstable, the script is unclear and requester is unable to clarify, individuals can opt to terminate the phone or be alert.

c) In formation sensitivity

Individual should be knowledgeable, and have absolute clarity, what information is sensitive. Individuals can be trained on this skills, this will allow them to value information they hold. Individual should not give any personal information via the phone, any person requesting such information on a phone should be considered a threat. Any request with words like PIN, Username, Account number or any personal information may be deemed sensitive. At this point if the request is sensitive, the mobile user should terminate the call immediately to escape the attack.

4.5.1 Verification of the model

This section demonstrates the application of the model by use of examples. The data used for verification was collected from experts. The researcher picked two cases that were reported by the IT managers. The first case depicts a request to reward a faithful customer form a bank, however, by a social engineer. The second case the social engineer makes a call to a target whose bank account is registered for mobile banking alleging that his bank account is registered to another person and is currently being swindled. The social engineer takes the customer through a process to offer assistance.

Case one

The first case depicts a call request for a PIN in order to reward the mobile user with cash for being a faithful customer by a social engineer.

Do you recognize the number?

This question makes the mobile user to be alert whenever the phone rings. Most of the social engineers will tend to hide their numbers or masquerade the numbers in order to make it difficult for the investigator to trace them back. The mobile user being alert will pick the phone.

How complex is your phone?

Mobile users should be in a position to understand the complexity of their mobile phone. If the answer to this question is high, the mobile user should be very careful on what request are made by the caller.

Is the script is clear?

The requester usually has a story to tell in order to create trust. The story from a social engineer listened carefully usually has some missing link which creates some discomfort to the target. The story being from a social engineer will create some discomfort that will lead to the next question.

Can the caller clarify?

Asking the caller questions usually disorient them because they normally work on a given script. Their great fear is for them to lose control. However, with various skills and techniques the social engineer possessing and in addition with adequate information he might be possessing about the victim, can convince the mobile user to be a legitimate caller.

If the requester cannot clarify the request and the mobile user feels uncomfortable, he/she can terminate the call. For the purpose of this illustration on how the model can be applied in detection of vishing attack, let us assume that the mobile user continues with the conversation.

How is your emotional state?

The stories focus on triggering particular emotions on the target. When a strong emotion is triggered, such as anger, excitement, fear or anxiety, an individual's cognitive ability may be seriously hampered**.** This may include their ability to make decisions rationally, evaluate the situation, make counterarguments, and reason logically, which is why this is such an effective technique used by social engineers. When the target feels emotionally unstable the reasonable action is to terminate the call. For the purpose of this illustration on how the model can be applied in detection of vishing attack, let us assume that the mobile user continues with the conversation.

Is the request sensitive?

The social request for SIM PIN to reward the mobile phone user is termed to be sensitive. SIM PIN is classified as personal information. At this point, the mobile user will have to terminate the call.

This scenario depicts how a social vishing attack could have been detected.

Case two

In this scenario, the social engineer makes a call to a target whose bank account is registered for mobile banking alleging that their bank account is registered to another person and is currently being swindled. The social engineer takes the customer through a process to offer assistance.

Do you recognize the number?

This question makes the mobile user to be alert whenever the phone rings. Most of the social engineers will tend to hide their numbers or masquerade the numbers in order to make it difficult for the investigator to trace them back. The mobile user being alert will pick the phone.

How complex is your phone?

Mobile users should be in a position to understand the complexity of their mobile phone. If the answer to this question is high, the mobile user should be very careful on what request are made by the caller

Is the script is clear?

The requester usually has a story to tell in order to create trust. The story from a social engineer listened carefully usually has some missing link which creates some discomfort to the target. The story being from a social engineer will create some discomfort that will lead to the next question.

Can the caller clarify?

Asking the caller questions usually disorient them because they normally work on a given script. Their great fear is for them to lose control. However, with various skills and techniques the social engineer possessing and in addition with adequate information he might be possessing about the victim, can convince the mobile user to be a legitimate caller.

If the requester cannot clarify the request and the mobile user feels uncomfortable, he/she can terminate the call. For the purpose of this illustration on how the model can be applied in detection of vishing attacks, attacks let us assume that the mobile user continues with the conversation.

How is your emotional state?

The stories focus on triggering particular emotions on the target. When a strong emotion is triggered, such as anger, excitement, fear or anxiety, an individual’s cognitive ability may be seriously hampered**.** This may include their ability to make decisions rationally, evaluate the situation, make counterarguments, and reason logically, which is why this is such an effective technique used by social engineers. When the target feels emotionally unstable the reasonable action is to terminate the call. For the purpose of this illustration on how the model can be applied in detection of vishing attack, let us assume that the mobile user continues with the conversation.

Is the request sensitive?

At this point, the request will be unusual and sensitive; the social engineer will request the target to look for another phone, which they can use to communicate with the target, as they are being guided on how to adjust their phone setting in order to reclaim back their bank account. In the proses, the target will be requested to enter their bank account and PIN to be assisted. Both of this information is classified as personal and sensitive, at this point the target will have to terminate the call.

4.6 Discussion of results

This academic research study sought to establish factors leading to vishing attacks, to identify mitigation measures of vishing attacks on mobile platform and to develop a model to be used by mobile users to detect vishing attacks. Through qualitative data analysis, this research found that factors contributing to vishing attacks were psychological, technical and information sensitivity. Majority of the respondents agreed that use of psychology factors was one of the key factors facilitating vishing attacks. Where the attacker is able to follow a series of steps such as reading more about their target population, making phone calls and engages the victim into a conversation that triggers their emotional status to create trust. They claim to help the victim to recover their account by helping them successfully navigate through their phone and by so doing they deceptively are able to access the victims account and thus in a position to transfer or withdraw money from the victims account. As it can be noted this are well organized criminals making it had any person without adequate knowledge to be able to detect attack. Findings from this research are inline with

Bezuidenhout *et. al*. (2010) study and other researches, which reveal that social engineers use various psychological vulnerabilities and triggers, to influence the individual's emotional state and cognitive abilities in order to obtain key information from their victims. It is therefore imperative for individuals to have a clear understanding of the psychological triggers used by social engineering attackers in order to recognize each during beforehand.

Technical factors such as mobile complexity expose mobile phone users to vishing attacks in the country. Majority of the respondents 56.3% reported that their phones had some complexity, 25% too much complexity; hence, the complexity on the use of their mobile phone was making them prone to vishing attacks. These findings are similar to Bruce & Schneier (2000) who noted that future of digital systems will be complex, and complexity is the worst enemy of security since the more the complex the system is the harder the user to understand it.

The researcher found that most of the mobile users were vulnerable to vishing attacks because 100% of them were registered to a particular mobile money service. In addition, 87.5% of the respondents believed that human factors to have a potential to cause security incidences and 75 % of the respondents believed to have information security incidents from humans.

Research findings further revealed that most of the mobile users had little knowledge on social engineering attacks which made them to be more vulnerable, 87.5% had little knowledge. None of the respondent had much information on vishing attacks, this shows why the vishing attacks are on the increase in Kenya.

Defence mechanisms: The research found that most of the mobile users lacked proper defence techniques; 93.75% believed that people who wanted to attack them were likely and certain to have knowledge and effective resources to attack them. 87.5% of the respondent felt that they were not protected at all. Findings further revealed that more than half of the respondents did not know how to defend themselves against vishing attacks with less than half the respondents 37.5% having used the black list defence mechanism. There is need for people to people to be taught on the various techniques that exist to help detect and defend an individual from social engineering attacks. Several studies reveal that the most implemented detection technique on vishing is the blacklist technique, which helps the mobile users defend themselves against vishing attacks (Cik *et al.* 2013, Huh and Kim, 2012, Xiang, *et al.*, 2011 and Zhang *et al.,* 2007)

Finally, the analysis of social engineering vulnerability, defence, social engineering attack vectors, education and demographic on mobile users data gathered from the duly filled questionnaires and the identification of various issues that arose from qualitative data helped to inform the model. The researcher therefore, designed and developed a vishing attack detection model for mobile users, which can be used by mobile phone users to detect vishing attacks, which is aimed at helping reduce the incidence of social engineering in Kenya.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATION

5.1 Introduction

In this chapter the researcher makes summary, conclusion and recommendations based on the research findings and analysis done in previous chapter. The conclusion is a summary of the report, including brief explanation on certain observations, while the recommendation will give suggestions and advice based on the research findings.

5.2 Summary and conclusion Key findings

Factors establishing the vishing attacks, human factors were deemed to play a major role in facilitating vishing, this was attested by more than half 50% of the respondents . This was followed by knowledge level among the respondents and majority of the respondents were not aware of the various strategies used by social engineering attackers to get information from people, majority did not even know how to defend themselves from vishing attacks.

The researcher found that SEADM catered only for vishing attacks utilising only psychological and security information sensitivity. Through data analysis on the information gathered from the questionnaires and key informants it come out technical vulnerability is underestimated entity in detection of vishing attacks. This paper proposed a vishing attack detection model, which caters for psychological, information sensitivity and technical vulnerability. The vishing attack detection model has been verified using generalised vishing attacks examples. It has been shown by the use of scenarios that the proposed model is indeed feasible as a preventative measure to social engineering attacks. This model makes a valuable contribution to the field of social engineering, as it aids in the detection of social engineering attacks, by breaking down the decision-making process into manageable components. The mobile users to protect themselves against any form of vishing attacks can use the model as tool.The vishing attack model can be used to detect only vishing attacks, in future a model is needed which can protect the user to all forms of social engineering attacks on a mobile platform.

5.3. Conclusion

Social engineering attacks are on the rise in Kenya due to lack of knowledge on this vice hence making them more vulnerable. There is need for more researches to be conducted in this field that will help in creating awareness about social engineering attacks. Awareness and training have been widely recommended as methods for mitigation of social engineering attacks and both are lacking in Kenya, social engineers take advantage of this. Therefore there is need to raise the knowledge levels of Kenyan citizens on social engineering.

Due to time, the researcher was not able to adequately test and validate the model but used case studies from experts to show the applicability of the model.

5.4 Recommendation

In view of the findings that emerged from this study, the following recommendations, are made with regard to: practice, policy and research

5.4.1 Recommendations for practice

Social engineering attacks continue to escalate and minimal efforts have been done to create awareness on factors that lead to vishing attacks. In order to achieve this, the current study makes the following recommendations

1. Communication Authority should seek to create awareness on the various forms of social engineering attacks that exist through radio and television to increase knowledge level on social engineering.

2. Communication Authority should seek to create training programs on social engineering attacks
3. Kenyan citizens need to be encouraged to report incidences of social engineering attacks as they amount to criminal activities

5.4.2 Recommendations for Policy

The policy framework plays an important role in the creating awareness and providing direction on how to handle and mitigate issues that affect the society.

1. The Ministry of Information and Communication Technology together with other stakeholders should embark on developing a policy on social engineering attack.
2. The Ministry of Internal Security should also develop a policy that seeks to deal with individuals engaging in social engineering attacks as it amounts to criminal activity.

5.4.3 Recommendations for further research

Based on the findings of this research, the following studies are recommended for further research.

1. The researcher used case studies from expert to verify the model; in future, a test must be done using experiments to evaluate the model.

2. More studies to be done on the influence of human factors in the Information and Technology field.

REFERENCES

Alnajim, A. and Munro,M. *"An evaluation of users' tips effectiveness for Phishing websites detection," in Digital Information Management, 2008. ICDIM 2008. Third International Conference on, 2008, pp. 63-68.*

Bezuidenhout, M., Mouton, F., & Venter, H. (August, 2010). "Social Engineering Attack Detection Model:SEADM," in Information Security for South Africa. *IEEE*, (pp. 1-8). Johannesburg, South Africa.

Bhakta, R., & Harris, G. I. (Feb 2015). "Semantic analysis of dialogs to detect social engineering attacks" . *IEEE International Conference on Semantic Computing (ICSC).*

Braisby, N. and Gellatly, A. *(2005) Cognivite Psychology.: Oxford University Press.*

Bottazzi, Giovanni, et al. *"MP-Shield: A Framework for Phishing Detection in Mobile Devices." Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on. IEEE, 2015.*

CAK. (2016). *quarterly sector statistics report fouth quarter for the financial year 2015-2016 (april-june 2016).* nairobi.

Clarke, R.V. and Cornish, D.B. (1985) *Modeling offenders' decisions: A framework for policy and research. In: M. Tonry and N. Morris (eds.) Crime and Justice: An Annual Review of Research. Chicago, IL: University of Chicago Press 6, pp. 147–185*

Devinder Singh, et al., *"Telephony Fraud Prevention," US Patent, 2011.*

Dunham, K. (2009) *"Chapter 6 - Phishing, SMishing, and Vishing," in Mobile Malware Attacks and Defense, D. Ken, Ed., ed Boston: Syngress, 2009, pp. 125-196.*

Gragg, D. (December 2002). *"A multi-level defense against social engineering," SANS Institute, Tech. Rep., .* SANS Institute.

Huh J. A. and Kim H.,*(2012) "Phishing Detection with Popular Search Engines: Simple and Effective Foundations and Practice of Security." vol. 6888, J. Garcia-Alfaro and P. Lafourcade, Eds., ed: Springer Berlin / Heidelberg, 2012, pp. 194-207.*

Jaeseung Song, Hyoungshick Kim, and Athanasios Gkelias, *" iVisher: Real-Time Detection of Caller ID Spoofing" ETRI Journal Vol. 36, No. 5, Oct. 2014, pp. 865-875*

Kigen, P. M., Kimani, C., Mwangi, M., Shiyayo, B., Ndegwa, D., Kaimba, B., & Shitanda, S. (2015). *Kenya Cyber Security Report 2015.* Nairobi.

Kim, S.E. and Yang, Y.J. (2008) *The evolution of tele-financial fraud: An analysis of offender victim interaction structures and respondence to 'voice phishing'. Korean Journal of Public Safety and Criminal Justice 32(1): 103–149.*

Kinuthia, J. N., & Akinnusi, D. M. (2014). Social Engineering Preparedness of Online Banks: An Asia-Pacific Perspective. *Journal of Global Information Technology Management*, 16(4), 21-46.

Longfei Wu, Xiaojiang Du, and Jie Wu, *"MobiFish: A Lightweight Anti-Phishing Scheme for Mobile Phones", in 23rd International Conference on Computer Communication and Networks (ICCCN), 4-7 Aug. 2014, Shanghai.*

Luo, X. R., Brody, R., Seazzu, A., & Burd, S. (2011). Social Engineering: The Neglected Human Factor for Information Security Management. *Information Resources Management Journal*, 24(3), 1-8.

Mahmoud Khonji, Youssef Iraqi, Senior Member, IEEE, and Andrew Jones *(2013). "Phishing Detection: A Literature Survey". IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 4, FOURTH QUARTER 2013.*

Mouten, F., Louise, L., Mercia, M. M., & Venter, H. S. (2014). Towards an Ontological Model Defining the Social Engineering Domain. *11th Human Choice and Computers International Conference* . At Turku, Finland.

Mouton, F., Leenen, L., & Venter, , H. S. (04 Feb. 2016). Social Engineering Attack Detection Model: SEADMv2. *2015 International Conference on Cyberworlds* (p. 223). Pretoria, South Africa: CPS.

Mugenda,O.M. and Mugenda, A.G.(2012). *Research Methods Dictionary. Nairobi: ARTS Press.*

Mulwa, D. K. (2012). *A survey of insider information security threats management in commercial Banks in Kenya.* Nairobi: University of Nairobi.

ProofPoint. (2016). *The human factor report 2016.* https://www.proofpoint.com/us/human-factor-report-2016.

Robson, C. *(2011).Real World Research: A Resource for Users of Social Research Methods in Applied Settings* (3rded.). Padstow, Great Britain: Wiley.

Sawa, Y., Bhakta, R., Harris, I. G., & Hadnagy, C. (2016). "Detection of Social Engineering Attacks Through Natural Language Processing of Conversations". *IEEE Tenth International Conference on Semantic Computing.*

Sheng, Wardman, B., Warner, G., Cranor, L., Hong, J., & Zhang, C, *"An empirical analysis of phishing blacklists," 6th Annual Conference on Email and Anti- Spam (CEAS), Mountain View, CA., 2009.*

Stemberg, R. J. *(2006) Cognitive Psychology, 4th ed.: Thomson Watsworth, 2006.*

Streiner, D. L. & Norman G. R. (1989). From Health Measurement Scales; A Practical Guide to Their Development And Use. NewYork: Oxford University Press. Pg.64-

Xiang, et al., *(2011) "CANTINA+: A Feature-Rich Machine Learning Framework for Detecting Phishing Web Sites," ACM Trans. Inf. Syst. Secur., vol. 14, pp.1-28, 2011.*

Zhang (2007) "*Avoiding Pitfalls in Neural Network Research", ieee transactions on systems, man, and cybernetics—part c: applications and reviews, vol. 37, no. 1, january 2007*

APPENDIX I: Questionnaire

Section A: General Information

1. Gender [ ] Female [ ] Male

2. Age of the respondent (years)

3. Highest level of education attained [ ] Secondary [ ] College [ ] University [ ] Post Graduate [ ] Doctorate

4. Job title or position of the respondent.

5. What type of mobile money services do you use?

Section B: Evaluating Social Engineering Vulnerability

Which of the statements below best describes the complexity of your Mobile phone (e.g. number of different applications, systems and legacy software)?

Very Little complexity	1
Little complexity	2
Some complexity	3
Much complexity	4

To what extent do you consider that human factors may cause information security incidents and problems on your Mobile phone?

Very little	1
Some	2
Potentially significant	3
Potentially critical	4

To what extent do you feel that you have information security incidents and problems from people you trust or criminals on your mobile phone?

Very little	1
Some	2
Potentially significant	3
Potentially critical	4

Which of the statements below best describes your use of the

Internet on you mobile phone?

Internet usage is insignificant (e.g. for information purposes only)	1
Internet usage is useful to my business (e.g. for transactional purposes)	2
Internet usage is important to my business (I can survive without it)	3
Internet usage is business critical (I can't survive without it)	4

To what extent would you say to have used the following Mobile money services? Indicate according to the scale shown below:

1. Not at all

2. To a small extent

3. To a great extent

4. To a very great extent

Mobile money services	**1**	**2**	**3**	**4**
M-pesa				
Airtel Money				
Equity Bank				
Branch				

Any other services not mentioned above				

To what extent are, the following loses experienced because of social engineering attack?

LOSE	1	2	3	4
Lose of data				
Leaking of personal information				
Theft of goods				
Financial lose				

C: Evaluate defence

Do you think that the people who may have the motivation to cause incidents, problems and instabilities, are likely to be knowledgeable and have the resources to attack you?

Unlikely to be knowledgeable and have effective resources	1
May have knowledge and effective resources	2
Likely to have knowledge and effective resources	3
Certain to have knowledge and effective resources	4

To what extent would you say to have used the following detection techniques? Indicate according to the scale shown below:

1. Not at all

2. To a small extent

3. To a great extent

4. To a very great extent

Content based	
Blacklist	
whitelist	
policies	

To what extent do you feel protected against vishing attacks?

To a very great extent	1
To a great extent	2
To a small extent	3
Not at all	4

D: Determine attack vector

To what extent can you say the following attack methods were used to course information system incidences or problems?

1. Not at all

2. To a small extent

3. To a great extent

4. To a very great extent

Attack Vector	1	2	3	4
Bluetooth				
Mobile web/application				
SMSishing				
Vishing				

E: Education

Which of the following statement below describes your knowledge on vishing?

Very little	1
Little	2
Some	3
Much	4