VULNERABILITY ASSESSMENT OF INFORMATION SYSTEMS BASED ON END-USER ACTIONS: A CASE OF UNIVERSITY OF NAMIBIA

A MINI THESIS SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

OF

THE UNIVERSITY OF NAMIBIA

BY

PAULUS S KAUTWIMA

(200841688)

JANUARY 2021

SUPERVISOR: Dr. Valerianus Hashiyana (School of Computing, University of Namibia)

ABSTRACT

Nowadays, data protection is of paramount importance to every institution of higher learning. Unfortunately, most security breaches happen as a result of an end-user error(s). End-user errors are unintentional actions of system end-users. This includes; weak passwords, clicking links from unverified senders, and downloading attachments from unknown senders. Most of the efforts aimed to address cybersecurity issues are either software-centered or hardware-oriented. As a result, user mistakes are overlooked since they are considered infinite, unpredictable, and remain part of human existence. Ignoring end-user error is a gigantic mistake and could result in a higher number of cyber-attack incidents. Therefore, institutions of higher learning where security is a top priority need innovative strategies to deal with end-user errors. Given this, this study aimed to assess different types of end-user errors that could affect the security triad of information systems. The study adopted the mixed-method research approach to collect data from the University of Namibia (UNAM) staff members, who frequently use information systems known as ITS. The quantitative dimension of the study utilized a closed-ended questionnaire to collect data from 310 UNAM staff members, who were randomly selected from the total population. Furthermore, an experimental design was also used to collect data from the staff members. The qualitative dimension utilized an exploratory research design where participants were selected through a purposeful sampling strategy. A semi-structured interview instrument was also applied to collect data from 10 staff UNAM Computer Centre staff members. The findings of the study revealed that end-user error is one of the major threats to information security. End-user errors present several security vulnerabilities and risks to information systems that could subsequently get data exploited by attackers. In addition, the study also established that confidentiality, integrity, and availability of information systems in an institution are also affected by end-user errors. Furthermore, the unprecedented growth of internet interconnectivity has led to an enormous increase in cyber-attacks. Personal security consciousness and security awareness training are some of the most successful measures to mitigate end-user errors. Based on the findings of the study, it is recommended that institutions enforce information security policy and provide security awareness training to staff members to avoid data breaches.

LIST OF PUBLICATIONS

Kautwima, P., Sai, K., Haiduwa, T., Hashiyana, V., & Suresh, N (2021). System End-User Actions as a Threat to Information System Security. *7th International Conference of Networks, Communications, Wireless and Mobile Computing (NCWC 2021).* Australia

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

CSB	Cyber Security Breaches
HEV	Human Error Vulnerability
IDS	Intrusion Detection System
IP	Internet Protocol
IS	Information System
IT	Information Technology
SQL	Structured Query Language
TCP	Transmission Control Protocol
UNAM	University of Namibia
USB	Universal Serial Bus
VA	Vulnerability Assessment
VPN	Virtual Private Network
WAF	Web Application Firewall
XSS	Cross Site Scripting

ACKNOWLEDGMENT

First and foremost, I would like to thank the Almighty God for taking me through this academic milestone which I believe would not have been possible without his grace, power, wisdom, perseverance, and strength. If it wasn't for his wish, the realization of this study would have come to nothing but remained a dream.

Secondly, I want to express my sincere gratitude to my supervisor Dr. Valerianus Hashiyana for his patience, guidance, encouragement, and most of all his unwavering professional support. I treasure all that I have learned from you Dr. Hashiyana.

Furthermore, I want to thank my mentor, Mr. Kundai Sai, for his encouragement and support during the time I almost gave up on this study. Mr. Sai without your encouragement and direction I would not have made it this far. I also want to thank my friend Mr. Titus Haiduwa for his academic support. I also feel indebted to my colleague, Dr. Suresh Nalina for her guidance and contributions.

My sincere gratitude is extended to my family, my fiancée Hileni Kanyanga and my son Petrus Fortune P Kautwima, for their unlimited support via prayers and supplications, love, caring, and encouragement.

Above all, I appreciate the support of everyone who directly or indirectly contributed to the finalization of this study, specifically the reviewers.

.

DEDICATION

This thesis is dedicated to God Almighty, my father Petrus Kandjabanga Kautwima, and my son Petrus Kandjabanga Pomweneipawa Kautwima.

DECLARATION

I, Paulus S Kautwima hereby declare that this study is my work and is a true reflection of my research and that this work or any part thereof has not been submitted for a degree at any other institution.

No part of this thesis/dissertation may be reproduced, stored in any retrieval system, or transmitted in any form, or by means (e.g. electronic, mechanical, photocopying, recording, or otherwise) without the prior permission of the author, or The University of Namibia in that behalf.

I, Paulus Kautwima, grant The University of Namibia the right to reproduce this thesis in whole or in part, in any manner or format, which The University of Namibia may deem fit.

Paulus S Kautwima  17 May 2022

Name of Student **Signature** **Date**

CHAPTER 1 : INTRODUCTION

1.1 Introduction

This chapter presents the introduction of the study. It consists of the background of the study, statement of the problem, research objectives, and significance of the study. The chapter further highlights the limitation of the study, delimitation of the study as well as the outline of the study.

1.2 Background of the Study

The University of Namibia (UNAM) collect different type of data and information from its stakeholders, be it staff members, students, or education partners. The amount of data and information collected therein is a very important resource to the university, hence, safeguarding and protecting it and securing the University's information systems is crucial (Uushona, 2016). The university's information systems here refer to email systems, integrated tertiary system (Self Help enabler), staff computers, and corporate network (internet). In carrying out this mandate, however, the university's responsible division, Computer Centre, need to ensure full implementation of the three-information security requirement: confidentiality, integrity, and availability of the information, also known as the CIA triad. The CIA Triad assures users that information is correct, timely, reliable, and free from modifications, destruction, unauthorized access, misuse, and disclosure (Kizza, 2017).

Information system security has three basic elements for securing information: confidentiality, integrity, and availability (CIA). Confidentiality of information is about protecting system information from unauthorized access (Sheikh, M. et al., 2020). Information is categorized according to its prominence (measured as the impact that information disclosure has on the organization) on several levels that differ from public to top-secret (Sheikh, M. et al., 2020). In this age of ICT, to keep information

secured, there is a use of passwords and encryptions (Zhiying, W. et al., 2020). In order to access such information, individuals are given authorizations and access rights according to the nature of their job, competence, and the level of classification of the data and information they work with (Zhiying, W. et al., 2020). Confidentiality is a legal issue and that is why it is governed by specific laws; it is for this matter that confidentiality contracts are signed.

In the security of information, the integrity of information is key. The integrity of information refers to safeguarding the information from threats that could potentially change data and information (Zhiying, W. et al., 2020). Apart from keeping the information secured by using passwords and encryptions, it is important to keep checking the data to prevent errors from happening, create back-ups, create access control mechanisms, and train employees on issues of data integrity (Sheikh, M. et al., 2020).

Availability, as an element of security of information, refers to assuring access to information for authorized users only at any time (Zhiying, W. et al., 2020). To ensure the availability of information, there is a need for well-functioning hardware equipment, networking systems, and backups (Sheikh, M. et al., 2020). Last but not least is the issue of observance of laws (Kizza, 2017).

Many efforts to improve and address information security have been mainly focused on software and hardware, with little or no efforts directed at addressing the users' aspect of information systems (Sifianu, 2016). According to Neely (2017), the main loose end of information security is the end-users who interact with the information system. Brian and Stalvatore (2014) further argued that an institution might have installed the optimum security technologies in existence and defended its physical

structures, but it is still completely vulnerable to attacks. It is a lack of understanding of security problems that makes people think that technology alone can solve security problems (Hadlington 2018). That is why Burea (2018) argued that technology-focused security alone is insufficient because the users are targeted when the technological attacks do not succeed.

Due to errors that end-users commit, the information security triad is compromised. End-user errors are weaknesses or mistakes and acts performed without intent or malicious purpose by an authorized user of an institution (Sifianu, 2016). The errors could include but are not limited; to using the same credentials on different accounts, not logging out of the system, sharing the password with colleagues, clicking links from an unknown sender, and weak password (Neely,2017). Lack of experience in technology use, improper training, and lack of strong IT security policy are also circumstances that cause compromises to information security (Hadlington, 2018). One of the reasons why such compromised security circumstances happen is because cybersecurity solutions tend to be based on technical solutions and end-user errors remain unaddressed (Sifianu, 2016). Such compromised circumstances create room for attackers to penetrate the information system and get access to sensitive information.

This study aimed at examining how end-user errors impact security systems. It is guided by an assumption that end-user errors are responsible for the ICT systems' threats. The study was conducted at the University of Namibia (UNAM). UNAM as an academic institution widely uses information system technologies in the management and running of the institution. However, according to UNAM Computer Centre Report (2019), over one million spam emails had been detected directed to various user accounts. The report further indicated that spammers used advanced

technics by using compromised accounts of legitimate UNAM users to send out impersonating emails with links to upgrade email accounts or to change their passwords. Although UNAM has technological measures such as firewalls, Intrusion Detection System (IDS), and antivirus to curb loopholes in the network, user accounts are still being compromised resulting in spammers using legitimate UNAM user account to obtain sensitive information from end-users (Shambalula, 2019). Information Systems are exposed to attacks even if optimal technological measures such as firewall, IDS, and antivirus are in place. The reason for attacking is that information security is not limited to the technical part only, but also to the system users. These human-caused threats had been overlooked by several specialists in security studies for decades (Safianu, 2016).

1.3 Statement of the Problem

According to UNAM Computer Centre Report (2019), over one million spam emails were detected to have been directed to various email user accounts. The report further stated that spammers were using advanced technics by using compromised accounts of UNAM legitimate users to send out impersonating emails with links requesting users to upgrade their email accounts or to change their passwords (Computer Centre, 2019). Shambalula (2019) indicated that although UNAM has technological measures such as firewalls, Intrusion Detection Systems (IDS), and antivirus to curb loopholes in the network, user accounts are still being compromised resulting in spammers using legitimate UNAM user account to obtain sensitive information from end-users. Hence, Information Systems could be exposed to attacks even if optimal technological measures are in place (Burea, 2018). This seems to be the case in UNAM corporate network as attacks seem to still happen regardless of the existing technical solutions in place. The reason for the above could be because information security is not limited

to the technical aspects only but goes as far as system users whose actions are hard to manage and unpredictable (University of Hong Kong, 2021). One possible loophole to an institution's IS could be an insider (employees) because they are the ones that could be nearby threat agents to the institutional information (Hadlington, 2018). This could be the case for the University of Namibia issues as enumerated above as its workforces are the ones that utilize the systems to carry out the university's daily operations and consequently make errors, accidentally or intentionally. Hence this could connote a severe threat to the integrity and security of information as paralleled to the threats from strangers. Some of the loopholes associated with the end-user actions could include but are not limited to; not logging out of the systems, leaving valuables items (UNAM laptops) in common areas or vehicles, not adhering to security measures such as clicking on links from unknown senders, ignorance, and sharing of passwords (University of Hong Kong, 2021). It is therefore imperative to scrutinize the system end-user errors as possible threat agents in an Information Technology setting. Although technological solutions have improved over the years, system end-user errors remain a problem that needs to be addressed (Sifianu, 2016). In addition, there is no literature specific to university security or human error as a security challenge and threat to university information systems.

1.4 Objectives of the Study

The overall purpose of this study was to assess the vulnerabilities of information systems with a focus on end-user errors. The research objectives are to:

1. Assess the existing Information Technology security mechanisms and policy at UNAM‟s Computer Centre.

2. Establish and discuss possible end-user errors that could lead to information security threats and system vulnerabilities.
3. Develop a phony phish system to send phishing emails as an attacker to test users' information security awareness.
4. Design and IS security vulnerability conceptual framework and model based on end-user errors, as a counter measure to the end-user errors towards IS.

1.5 Significance of the Study

The findings of this study will enhance an understanding and knowledge concerning IT Security practices in UNAM. It highlights human actions as a threat in terms of protecting and securing information and ensuring information integrity, confidentiality, and availability. The study is also beneficial to university policymakers, IT technicians, network administrators as well as database administrators as it could help them to find an amicable solution for end-users as a threat to information security. Future researchers will pick up where this study ended and help to formulate a better security framework, including human beings. The study guides on how to deal with the complexity of people toward information security.

1.6 Limitation of the Study

The national lockdown which restricted people from moving from one place to another was introduced as a result of the Corona Virus (COVID-19) outbreak. The research could not travel to all distant UNAM satellite campuses. This unfortunate event posed a challenge for data collection and hence, the results of this thesis cannot be generalized to represent all UNAM campuses. As a consequence of the pandemic, this research simply researched only staff members from UNAM Oshakati Campus and Windhoek Main Campus. The challenge of the lockdown was overcome by employing

online data collection tools, whereby some participants were interviewed through zoom and skype and surveyed using Survey Monkey.

1.7 Delimitation of the Study

Delimitations refer to the boundaries of the research study. Therefore, the researcher has set boundaries for the research objectives. The scope of this research is strictly on human-caused threats and prevention measures but not entirely on threats to information security. It touched mostly on human errors rather than all other general causes of threats and vulnerability within IS. Also, the study only used a phony system to implement social engineering as an experiment to test users' information security since social engineering is considered a decent experiment to study human actions towards information security.

1.8 Research Methodology

The study adopted a mixed-methods approach to carry out an in-depth analysis of the behaviors and perceptions of security by UNAM staff members. The quantitative dimension utilized a self-administered survey questionnaire with closed-ended questions on staff's experiences with information security, it was randomly distributed to 310 UNAM staff members to collect data from UNAM staff members who interact with information systems. Simple random sampling was used to select the 310 staff, out of the 1394 employees working for UNAM from the two UNAM campuses, (Oshakati and Main Campus). Data were analyzed using Statistical Program for Social Scientists (SPSS) and Microsoft Excel applications. The results were presented in graphs and tables. The qualitative dimension utilized an unstructured interview to collect information from 10 purposefully selected IT professionals from the UNAM computer center. IT personnel were purposefully selected to provide the right information to technical questions posed during the interview. Data was analyzed

through a thematic approach and themes were generated and aligned to answer the research objectives.

1.9 Outline of the Thesis

The format of this mini-thesis is outlined as follows:

Chapter 1: Introduction; presented the background of the study, statement of a problem, research objectives, significance of the study, limitation of the study, delimitation of the study, research methodology and outline of the study.

Chapter 2: Literature Review; reviewed relevant literature and summarised a number of related works found similar this study. It contains a comprehensive literature review on end user errors, vulnerabilities, information security mechanism and social engineering as technique to harvest user data. The reviews were drawn from several concepts in information systems security and synthesised.

Chapter 3: Research Methodology; discussed the research methodologies used in the study. It discussed the research method, research design, targeted population and sampling technique applied in the study. It further highlighted the research instruments, research procedures and data analysis undertaken in the study. Finally, it discussed ethical considerations, reliability and data validity issues.

Chapter 4: Implementation and Results; described the design and implementation of the phony systems. It further presented the results of the penetration experiment.

Chapter 5: Results and Discussion; this chapter presented results of the data collected through questionnaires and structured interviews and discussed the study results in relation to the research objectives.

Chapter 6: Conclusions and Recommendations; this chapter presented the conclusion of the study and made recommendations from the research findings and suggested for future research.

1.10 Summary

This chapter provided the overview of information security concerning IS security and the need to better understand the security issues that exist within this network. Furthermore, research objectives were identified according to the research problem. The next chapter presents a comprehensive literature review of end user error vulnerabilities, IS security mechanisms and social engineering as a technique for managing end user actions towards securing Information Systems.

CHAPTER 2 : LITERATURE REVIEW

2.1 Introduction

The literature review informs the reader of what is already known about the research topic. It also explains what gaps of knowledge exist and what the study was intended to contribute. Hence, this section presents a review of relevant themes to present the current knowledge in the field that is found relevant to the study objectives outlined in chapter one in order to update readers and establish a gap in the literature. The chapter looked at the end-user error vulnerabilities and the recommended IT security mechanisms that every institution should at least implement to alleviate security breaches. This chapter also discussed an approach employed in this experimental study, which is social engineering and concluded with vulnerability assessment and penetration testing.

The literature review aimed to present a literature review of related work to give a better understanding of end-user error as a threat that contributes to information security vulnerabilities.

Below is the outline of the topics presented in this chapter. Firstly, the researcher presented the overview of information security followed by information security in universities. It later presented a summary of related studies. At last, it discussed end-user errors as a threat to information security. The case of UNAM covered the population, ICT usage, and statistics on devices, infrastructure available, and UNAM ICT policy.

2.2 An Overview of Information Security

Information is interpreted data. People use the information to create wisdom. Nowadays, organizations rely on information for decision-making. Technology such as the internet and mobile devices has made information access much easier. Knowing that information is valuable makes it imperative to protect it at all levels from unauthorized access, disclosure, disruption, modification, destruction and misuse and hence unfortunate that some information systems users do not take appropriate security measures to protect data or information, whether in storage or transit.

Disruption of information systems and misuse of information can have fatal consequences to the entire organization or individuals. In a company where security matters most, information security is the key priority to ensure the confidentiality, integrity, and availability of information. Confidentiality herein refers to information protection from unauthorized access while integrity involves protecting information from any kind of modifications. Availability ensures that access to information is not denied to authorised users whenever needed (William & Tom, 2014; Kantarcioglu, n.d). Confidentiality and availability use various security controls such as management, operation and technical controls to protect an organization's information and information systems. Education on security awareness and the establishment of security policies are also some of the mitigation techniques to eliminate threats to information.

As one of the components of information systems, people are prone to make mistakes. Hence, system users (authorised or unauthorised) remain the biggest threat to information security due to possible errors. The technology at their disposal becomes vulnerable and eventually poses a risk to educational institutions. Threats are possible malicious or accidental events that can put information at risk. An example is a

disgruntled employee, malicious software, hackers, end-user errors or omissions and so on. Vulnerabilities, however, are weaknesses in an information system that could be exploited by a threat.

2.3 Information Security in Universities

Tertiary institutions deal with a large amount of information. It is very imperative for universities to adopt an Information Security Policy as a mechanism to safeguard the confidentiality, integrity and availability (CIA triad) of institutional data as well as any information systems that store, process or transmit institutional data. Institutional data could be defined as any data that is owned or licensed by the university. An information system is defined as any electronic system that stores, processes or transmits information (PWC, 2016).

All institutional data shall be protected in a manner that is considered reasonable and appropriate given the level of sensitivity, value and criticality that the Institutional Data has to the University. Some examples of restricted data include but are not limited to; account passwords, driver's license numbers, and education records of students, financial account information, health information and social security numbers (PWC.2016). Studies have indicated that universities have all technical control installed, however, the existing solution did not address the university users (human security) who interact with the institutional data and IS.

Challenges

Ensuring data protection in institutions of higher learning proved to be a challenge. This difficulty could be attributed to the fact that there is a higher number of users within universities hence a myriad of end user actions. It has been also noted that human errors are infinite and knowing their causes is nearly impossible. Also, people's

behaviour towards security controls differs. This position human security as the major challenge and concern in general. It also, shows a gap in knowledge hence leading to this investigation.

Possible Solutions

Universities need to put in place end-user security assessment strategies to measure and evaluate the level and adherence to rules in place. The university may also use existing solutions such as enforcing ICT policy. Such policy for universities should include Security Awareness and Training of end-user. Appropriate security awareness training for all staff in an institution, along with specific training relating to particular systems and controls, is an essential component in implementing human security controls.

2.4 Related Studies

There are a number of different studies carried on information system security and end-user errors. Researchers have slightly different argumentation, interpretation and perspectives, in their literature reviews. Below is a summary of related work carried out on the topic under discussion. Amongst the reviewed work includes vulnerability assessment of information systems and penetration testing. It focused more on examining possible secuirty threats and the protection mechanism necessary to address threats to information assets. Further, it emphasised the importance of cybersecurity policy. However, end-users are not covered.

For instance, a study by Pill (2019) asserted that information stored in databases is susceptible to a multitude of attacks, however, it is possible to alleviate risks by addressing the most critical threats. Silver (2013), also conducted a study on evaluating technological vulnerabilities and found that to protect against targeted attacks,

institutions could configure a scanner to check web applications for vulnerabilities such as SQL injection, cross-site scripting and forceful browsing. Silver's study recommended the use of a web application firewall to protect against vulnerabilities. Lamar (2012:56) argued that database attacks are prevailing nowadays because of the vulnerabilities in Operating Systems. The study also outlines that database rootkits and services associated with the databases could create a loophole for illegal access which may lead to a Denial of Service (DoS) attack. Kamara et al.,(2010) suggested a taxonomy to comprehend firewall vulnerabilities in the framework of firewall implementations as it is not always practical to analyse and test each firewall for all potential issues. Hence, the study scrutinised firewall features and cross-referenced each firewall operation with the causes and effects of faults in that operation, evaluating twenty recognised flaws with prevailing firewalls.

The work by Kashefi et al. (2013:25),examined vulnerabilities in software and hardware firewalls and discovered that there are four common vulnerabilities in firewalls. (1) Insider attacks, (2) network traffic, (3) tunnelling, and (4) internet threats. Another study by Soomro et al., (2013) established that cryptosystems are even more vulnerable to attack when they are handling little amounts of data. Soomro's study recommended a technique to reduce the inefficiency in the algorithm by introducing XOR operation in the major steps of the symmetric algorithm to alleviate communication overhead in transmitting small amounts of data. According to Kaspersky Lab (2013) report on software vulnerabilities, it was found that software vulnerabilities exist because of improper process, poor design and programming errors. Despite the sophisticated design of modern encryption and cryptosystems, they still exhibit the same flaws that the first systems contained many years ago. According to Hadlington (2018), a lack of understanding of security problems makes people think

that technology alone could solve security problems. Furthermore, Kizza (2017) proffered that technology-focused security alone was insufficient as users were being targeted when the technological attacks did not succeed. Safianu (2016) narrated that even though many institutions made use of an extraordinary number of technical security controls, the non-proportional number of security breaches still prevails.

In summary, all literature stated explores the vulnerability studies in software and hardware aspects of information assets, ignoring end-user actions as a potential threat to information security. For this reason, this study urgently investigated the matter intending to close the gap in knowledge on the topic under discussion. Researchers assume there is a great need to address this problem of end-user error induced vulnerabilities, which had been overlooked by many computer security researchers.

2.5 System End-User Errors as a Threat to IS security

This section highlights weaknesses or mistakes that are done by end-users, without intent or malicious purpose. A study done by Safianu (2016) discovered about 8 common end-user error threats that can make information systems vulnerable to attacks. The said end-user errors include, but are not limited to:

a) Following Links from Unverified Senders

Institutions that use secure communication network protocols such as IP Security, Secure Socket Layer (SSL), Transport Layer Security (TLS), HTTPS, Secure Shell (SSH) and guide employees to follow security procedures and policy tend to have secure hardware and software, hence not vulnerable to vulnerable attacks comparing to those organisations that lack technical and computer security (Zadelhoff, 2016). However, phishing and social engineering are some of the most effective routes to stealing confidential information from organisations. Hence, institutions that use

secure protocols and procedures and have secure hardware and software are equally vulnerable to these attacks as those organisations that lack technical and computer security solutions (Zadelhoff, 2016).

Phishing attacks are growing because are the only available avenue for attackers to steal sensitive data or financial information or extracting trade secrets. Furthermore, by attacking the right users, attackers can gain a grip on the corporate network then use it to exploit sensitive information. Phishing and social engineering attacks are more challenging to manage since they depend on human behaviour and involve taking advantage of vulnerable people. Institutions and individuals today must utilise a combination of technology solutions and user awareness to help protect sensitive information.

This study tested UNAM staff members on the tendency of clicking links from unverified senders by sending emails with links to users. The results of this test are discussed in chapter 4 under results.

b) Deficiency of Strong Password and Inappropriate Password

A password rule is very important. The complexity of passwords is one of the recommended measures in the information security industry. Preferably, a password should be difficult to guess which also implies that it should not be a phrase or word or a number that can be easily remembered such as ID, birth date or telephone number (Neely, 2017). Using a weak password, inappropriate password such as a user using a surname or name as a password, this type of passwords is inappropriate because they could be easily predicted. The sharing of passwords with others and recycling of the same password on different systems are some of the bad practises that could have the potentiality to jeopardise Information System. Passwords are destined to safeguard information from

unauthorised access of individuals both inside and outside of an institution. If the password is compromised, the security of the system is at risk.

Certainly, the complexity of passwords is one of the major issues that is being tackled within the information security industry. Preferably, a password should be difficult to guess which also implies that it should not be a phrase or word or a number such as birth date, surname, name or telephone number that could be associated with the user easily (Neely, 2017). Hence, the password should be generated with phrases or characters the user can easily remember and users must always log off their computers when done using them. Passwords should be short or commonly associated with something the user can recollect.

However, that does not mean that users should have a password which can be predicted easily. Perhaps end-users should embrace a "*passphrase*", which is kindlier. A "*passphrase*" is a line of characters, usually lengthier than a password, from which a virtual password is derived.

A practical example of a typical password could be "Kautwima123" and a typical passphrase could be "MayTheAlmightGodBeWithYouForever," which can also be denoted as "MTGBWYF."

This study tested UNAM staff members for password strength and appropriate password usage and the results for this test is present in chapter four of this study.

c) Reckless Handling of Computers

Threats and vulnerabilities can be avoided if employees respect to log out or lock their devices whenever they leave their desks. Moreover, a session timeout could limit the risk to unattended computers (Kearney, 2010). In many instances, people do leave

their computers idle when leaving the work premises or unattended when attending meetings. Also, some do not log off their computers when visiting the bathroom. These actions such as misconduct of computer-related equipment could jeopardise data security. Insiders' attacks are mostly associated with employees leaving their PCs unattended yet with active sessions running hence threaten the viability of the university in protecting its information. These threats can be avoided if employees are educated to log out or lock their devices when they leave their desks. Moreover, a session timeout could limit the risk to unattended computers (Kearney, 2010). For this study, leaving the computer idle and unattended to tendency was tested on UNAM staff members who frequently utilise the Information system to see if users are taking care of the computers. The finding of this tendency is presented in the result chapter, which is chapter four.

d) Linking to Networks Outside the University Infrastructure

Connecting to a private or a public network other than the institution's network infrastructure can pose a severe threat to information when the device used to connect is compromised. A device that has been compromised could be used as a gateway to an institution infrastructure. Staff members who connect their mobile devices to the home network could expose their devices to attacks, as the devices are outside the perimeter of the more secured institution's network (Lee, 2018).

e) Deficiency of Well Formulated Personal Security Policy

Lack of strong passwords to social media accounts such as Facebook and Twitter could be an entry point for hackers. Workforces are found to be strict on security on one network but are careless about what information they put online. Personal and professional networks where the workers freely and frequently update their status can

offer a chunk of information for attacks. Attackers can gather this information and use it to sketch their victims, with the most popular source for such search is the Internet, especially social networks.

Hadlington (2017) indicated that email is one of the routes attackers use to access a network since breaking the security perimeter is much harder today. When users use the institution network to send and receive emails, jeopardising information. As employees connect to both the institution and public networks, their computers are often less secure and the fact that they run unauthorized applications like emails and outdated software on their computers makes them the perfect targets, allowing the attacker to access their computers and largely the corporate network (Gyunka & Christiana, 2017).

This research investigated whether UNAM employees are cautious on what to post on public network and social media and the results was presented in chapter four of the study.

f) Illegal Application Use

Unauthorised applications used by users in the university network could compromise the security of the university networks. The institution and worker's personal information could be in jeopardy when unofficial applications are used on the institution network (Gyunka & Christiana, 2017). The unauthorised applications are mostly downloaded from malicious websites. This applicant can come along with viruses, Trojan Horses or worms. The study found out that malicious programs could be spread over the university network when files are downloaded from unknown and untrusted web sites. This could cause a serious security breach. These findings concur with the findings of the study conducted by Gyunka & Christiana (2017) which

indicated that unauthorised applications used by users in corporate networks could compromise the security of these networks.

This study tested UNAM end-users on the tendency of downloading attachments from untrusted sites by sending emails with attachments to be downloaded by sending emails with attachments to see if users could download attachments from unknown senders. The result for this test is presented in the result section of this study.

g) Distant Worker Security

As institutions' operations become more and more dispersed and transition online, mobile workers increase the potential threat for data (Hadlington, 2017). Employees tend to move unfinished work to their devices and take it along at home so that they could work on it later. This is quite risky because often personal computers and devices are less secured compared to corporate ones. The study has shown that improper handling of data, such as moving files from an office device to a home computer that does not have proper IT security measures attracts information theft. Hadlington (2017) also indicated that one of the hazardous behaviours of exposing information to attacks is sending them home with an employee. This tendency can turn all of the security measures in an institution into a useless process and could put information at risk of theft and other threats. For this study, the connection to remoted user was investigated to determine the channel security. The findings are given in the finding section of this research.

h) Threats from within the Institution (Inside Attackers)

When workers are discontented with their jobs, peeved with their boss, or sentimental for any reason, they can become insider threats who can purposely damage or leak data (Hadlington, 2017). Hadlington's study further, established that when employees

are unhappy with their jobs, angry with their boss, or sentimental for any reason, they could become insider threats who can purposely damage or leak information. Therefore, users could expose information deliberately to hurt the institution because of some reason as stated above. Hadlington (2017) indicated that sometimes the problem is not that users ignore security threat but the users are the threats themselves they have the potential to deliberately expose information. Hence is crucial to come up with hiring and termination procedures to avoid attack from disgruntled employees. Therefore, the end-user error is an important factor in assessing vulnerabilities in information systems. This research was geared towards evaluating the human errors that contribute to information insecurity. This study investigated threats from within the university that are unintentional such as weak password and ignorance.

Therefore, the end-user error is an important factor in assessing vulnerabilities in information systems. This research is geared towards evaluating the human errors that contribute to information insecurity.

2.6 Possible Causes of System End-User Errors

This section discussed some of the factors but not limited to that could be considered to be the cause of end-user errors. According to Badie and Lashkari (2012), There are five human mistakes that could have a negative repercussion to system end-users' behaviour and are summarised as follow:

Absence of Inspiration

Workforces should be encouraged to embrace safe behaviours and practices. The institution management needs to recognise what encourages the workers. Inspiration transpires when security issues are shared and users are involved in decision making in order to follow security processes (Parsons et al., 2010).

Deficiency of Awareness

The deficiency of awareness is associated with a lack of general knowledge about network attacks. Some common examples that portray the lack of awareness could be the following: System users do not possess abilities on how to recognise a signal of a spyware on the computer and how significant is to create a strong password. Users cannot protect themselves from identity theft, and social engineering and they do not know how to control the access of others to their computer. The lack of education and training on basic information security in institutions are considered the leading cause of end-user mistakes (Kearney, 2010). It is believed that if users are trained and sensitised about security, they are likely not to commit mistakes that could jeopardise the security of IS.

Belief

According to Kearney (2010), the term belief could be defined as the users' belief that is risky to IS. A study undertaken by Metalidoua (2014) revealed the users' opinion on information security and presented several incorrect beliefs that are hazardous to IS. Furthermore, Metalidoua underscored that user usually think that their behaviours are in obedience with the documented system due to the belief that the rules and guidelines are common sense. Some common examples of beliefs that are regarded as risky could be stated as follow: Users believe that the installation of anti-virus software does not make sense for their information, or they are ready to click on any link once they receive an email from unknown persons. Hence, a belief in a user could be dangerous to information protection.

Behaviour

Behaviour in terms of information security could be defined as user's manner that is dangerous to information or IS. Such behaviour could be instigated by several issues. According to Kearney (2010), the best way to mitigate user's risky behaviour is documenting requirements of anticipated information security behaviour could mitigate a little on the effect of user's risky behaviour. It is worth citing the conclusion of Albrechtsen, which stated, ''The users consider a user-involvement approach to be much more effective for influencing user awareness and behaviour''.

Insufficient Usage of Technology

Even the best and well-implemented technological solution cannot completely eradicate information security hitches without the continuous human cooperation and the effective use of this technology (Sadgwick, 2019). Some examples of considered inappropriate uses of technology are the following: making unauthorised reconfiguration of systems, accessing passwords of others, retrieving inappropriate information. Neely (2017) have confidence in that imparting individual's knowledge of IT security basics such as threats, risks, and consequences of their actions to end-users will allow users to gradually acclimatise to constant change and hence allow IT specialists to predict expected behaviour

Therefore, this study identified possible causes of the end-user error and suggested mitigation measures. This study recommended that mitigation measures be users training on the technology use and security awareness.

2.7 Information Systems Security Mechanisms and Policies

According to the study undertaken by Sai et al. (2016) in Zimbabwe, there are eight recommended security mechanisms for a computer network of an institution. These mechanisms as summarised below:

i. Appropriate Installation and Configuration of a Firewall

A firewall is defined as a software or hardware that aids screen out hackers, viruses, and worms that tries to invade the computer over the Internet. Firewalls are the institution's initial line of security and need to be installed regardless of the magnitude of the institution (Microsoft, 2014). A majority of institutions expose their networks to Internet traffic, firewalls are becoming a requirement (Laudon & Laudon, 2014). Intruders in everyday life are undoubtedly probing institutions with a constant Internet connection. Firewalls defend the university network from unauthorised access by filtering out packets from untrusted networks, it is imperative to take cognizance of the fact firewalls cannot safeguard against attacks that pass via authentic communication routes. It is recommended for the university to have hardware and software firewalls installed so that the software firewall could serve as an alternative to back to the hardware firewall. However, it can only operate on the machine on which it is installed, hence the software firewall needs to be installed on all machines for it to provide a good back up for the hardware firewall (Microsoft, 2014).

The results from this study indicated that UNAM has appropriate and well configured firewall, it even proved that the firewall could even block some useful sites. Therefore, firewall as a security mechanism could not be the reason why data breaches is happening.

ii. Updating Software

Updating software is an important part of keeping a computer secured and keeping all software up-to-date will protect a user against the most common security exploits. In the year 2014 attacks increased 2–100,000 times, 60 percent of recorded attacks exploited application weaknesses. Amongst those recorded attacks, 40 percent of the attacks emanated from shortcomings for which a patch had been issued and 20 percent from misconfigured applications (Sai, Gumbo, Mzikamwi, & Ruvinga, 2015).

The patching process is one in which the patch issuer administers a disclosure that details the very nature of the vulnerability that it is about to correct. Because network administrator does not patch quickly enough, it gives hackers the time to exploit that vulnerability and infect systems before the patch is installed (Paul Lin, 2006). This makes it extraordinarily significant to keep all software updated to prevent security incidents. In the case of anti-virus and spyware applications, the program is only as good as the last update (Sai, Manjeese, Mawere, Denhere, & Prosper, 2016). A frequent update software, particularly those that safeguard against malware is very indispensable as it helps to record the names of the up-to-date and leading threats (Helkala & Bakås, 2014).

This study had discovered that UNAM updates software frequently and it is done automatically. This type of security measure is carried out properly in UNAM, hence software update as a security measure could not be the cause of insecurity, since it is done regularly and automatically.

iii. Protection Against Malware

The educational institution should have mechanisms that protect the IS from against malware. The common mechanism to protect the university network from malware is

anti-virus software. Anti-virus software is an application that safeguards a computer from a malicious software called a computer virus. It is recommended that all computer inside the university network should have an anti-virus installed to minimise the network the chances of attacks and security threats (Alkandary & Alhallaq, 2016). Therefore, this study found out that the University of Namibia has recommended antimalware installed in all computers; laboratory and office computers have antimalware installed. This study concluded that antimalware could be the contributing factor to security breaches in UNAM, since antimalware are in place.

iv. Application a Strong Password Policy

Even though these newer technologies are being gradually adopted, the user's name and password authentication method remain the most widely used procedure for protecting information (Sun et al., 2011). Implementing a strong password policy is not all about formulating and enforcing the policy but it also entails educating system end-users on how to protect the passwords. Educational institutions should train employees on the password protection, for instance; not writing down the password, posting a password on social media because these are things that users do (Sai et al., 2016). According to Sun et al. (2011), the level of protection offered by passwords is directly related to their complexity. A strong password is defined as a series of more than 10 characters, at least one change of case, a number that in the middle and a non-alphanumeric character such as hash (#) or ampersand (&) that not appearing at the end of the password (Helkala&Bakås,2014).

For this study, UNAM has good password policy as suggested by the literature; such as expiration of a password after a month, a password with non-alphanumeric and no repetition of a password. The password policy as a security mechanism cannot be

contribute to security gaps since has a strong password to protects the IS from unauthorised access.

v. Putting a Physical Security Mechanism in Place to Protect Computer Resources from Theft and Damage

The basic form of physical security mechanism for the university computers is to put locks on doors of computer laboratories and offices and implementing a Disaster Recovery Plan, whereby a backup is place at different location (Sai, Gumbo, Mzikamwi, & Ruvinga, 2015). Then another ideal strategy towards implementing an enhanced physical security is to record all IT equipment's serial numbers for identification purposes and minimise access to computer laboratories and equipment for instance; servers and switches (Microsoft, 2014). The institution could also secure the computers physically, by using cable ties to tie all cables together and lock them. This make protects computer from physical theft because a computer cannot be easily taken away as opposed to when cables are not secured with cable ties. All laptops should have locks to secure them on the desk when users are leaving them unattended. Areas with sensitive equipment such routers, servers and switches should have access points for identification of employees and could embrace safeguarding entrances and exits. Backup storage area should be protected. Information such as network infrastructure model, indicating the network set up and the devices that protect it should be kept confidential, because information of that nature in the hands of an attacker is tantamount to a route map to the IS' front door.

This study discovered that University of Namibia has physical security in place, such as security officers at the entrance of the computer labs, cable ties and locks for computers physical security. This study concluded that physical security of computer

assets or IS not a challenge, since it is well taken care of in UNAM and hence, cannot be among the factors that contribute to security loopholes.

vi. Implement University Policy and Training

The university employees have a large potentiality to contribute to the attacks of the university Information System because employees interact with IS every day to carry out the university day to day operations, hence it is a sensible idea for an educational institution to adopt employee security awareness and training to mitigate the chances of attacks on the university network (Sai et al., 2016). However, statistically employees training and security awareness are the lowest on the list of top priorities of information security budget at 16 and 13 percent in that order (CSB, 2018).

This study investigated the existing UNAM policy regarding information security to determine what is missing or lacking in the existing information security. The concluded that UNAM doesn't carry out end user train to sensitise user on security issues. This could jeopardise the security of IS.

iiv Connecting to Isolated Users Safely

The remote access technology has advanced corporate productivity, provided online information, facilitated a flexible work schedule and improved business communication (Sai, Gumbo, Mzikamwi, & Ruvinga, 2015). Both public and private networks provide how information can be accessed. Educational institutions have workers who are not fixed at one university branches and need to have access to the university intranet from a distant working site, for instance; home, hotel or guesthouse (Harris & Patten, 2014). Virtual Private Network (VPN) technology is the method that educational institution should adopt to secure the communication channels between the distant employee and the university network. The use of VPNs allows

authentication of users to prevent unauthorised access of the university intranet (Namaya & Mirza, 2018).

This study investigated the weather University of Namibia has remote workers and examined how communications between remote workers are carried out. Securing a remote user is not among the contributing factors to security breaches as demonstrated by this study.

vii. Locking Down Servers

Handling of computers that provides service to other computers is a critical issue nowadays. Controlling what a server can permit and what a server can do is very crucial to information system security. Limiting access to the server is a brilliant idea, just to tighten security. Some network ports that are not necessary for operations could be blocked to ensure limited access to the server. Servers can control personal computer (PC) operation and inhibit users who do not have administrative privileges from downloading unauthorised programs. This is a common mechanism used by institutions to mitigate vulnerability to viruses that attach themselves to programs (Sai et al., 2016)

For this study, the mechanism of locking down servers was investigated in UNAM and it was discovered that, locking down server mechanism is observed by UNAM. Hence it cannot be the reason why security breaches are happening.

viii. Implement Identity Services (Intrusion Detection)

IDSs are intended to discover attacks in the institution network and also to help to trace information about the attacker afterward. The audit trails and logs files logs information regarding attacks for specific IS (Alkandary & Alhallaq, 2016). Usually, an intrusion detection device is a network equipment that is located on a reflected network switch port and reviews network traffic between switches to identify any

possible presence wicked bit patterns. It uses statistical anomaly or pattern matching detection. These systems can also be host-based. It is a virtuous idea to use intrusion detection systems along with access control because access controls alone cannot fully control unauthorised access to the institution network (Jain, et al., 2014). This study investigated whether there is IDS implemented in UNAM. The study established that IDS security mechanism is well implemented by UNAM and under no circumstance shall it contribute to insecurity of IS.

The above work looked only at information security mechanism that is either hardware related or software related while overlooking mechanisms to deal with end user error threats. Therefore, this study addressed user errors that can contribute to information security vulnerabilities and recommend mechanisms to mitigate end user error threats.

2.8 Social Engineering

Social engineering can be defined as, the practise of deceiving someone, either in person, over the phone, or using a computer, to breach some level of security either personal or professional and gain access to an institution's sensitive information (Bansla, et al.,2019). Alternatively, social engineering is a non-technical kind of intrusion relying heavily on human interaction that often involves fooling other people into exposing confidential and sensitive information as well as breaking normal security procedures. The attacker uses social skills and human interaction to obtain information about an organization or their computer systems.

2.8.1 The Life Span of Social Engineering

According to Bansla et al. (2019), every Social Engineering attack is unique, but with the understanding of the situations encountered, social engineering undergoes a rough

cycle of all the activities leading to a successful outcome. The below Figure shows a general representation of the Social Engineering Life Cycle in four main stages:

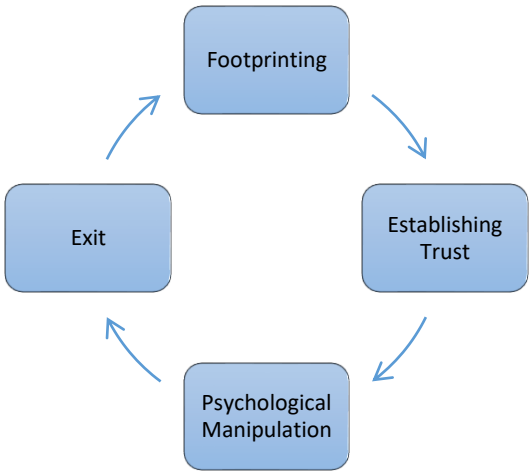

Figure 2.1: Life Span Of Social Engineering

Foot printing: It is the technique of accumulating information regarding the target(s) and the surrounding environment. Foot printing can reveal the individuals related to the target with whom the attacker has to establish a relationship, to improve the chances of a successful attack.

The information collection during the foot printing stage entails but is not limited to; list of employee names and phone numbers, organisational chart, department information and location information. Foot printing usually refers to one of the pre-attack stages; tasks performed before doing the actual social engineering attack. Some of the tools like creepy, SET and Maltego makes Social Engineering engagements easier.

Establishing Trust: As soon as the possible targets have been identified, the attacker then moves on to develop a rapport with the target who is usually an employee or someone working in the business to develop a good connection with them. The trust that the social engineer is gaining will later be used to unveil confidential pieces of information that could cause severe damage to the business.

Psychological Manipulation: In this step, the social engineer employs the trust that gained in the preceding phase to extract as much confidential information or get sensitive operations related to the target system performed by the employee himself to penetrate the system with much ease. Once all the required sensitive information has been collected, the social engineer may move on to the next target or move towards exploiting the actual system under consideration.

The Exit: After all the actual information has been gathered, the Social Engineer has to make a clear exit in such a way so as not to divert any kind of unnecessary suspicion to himself. The hacker ensures not to leave any form of evidence that could lead to a trace-back to hacker's real identity nor link hacker to the unauthorised entry into the target system in the future.

This study used all four stages of the social engineering life cycle to complete the social engineering activities; firstly, the emails of the targeted users were identified and collected and secondly, the rapport was established by sending impersonating emails to end-users, which comes as if it was sent by the UNAM IT technician so that it can entice and persuade the user to respond to the email without reservation. The email intends to manipulate end-users into giving information about their networks such as IP address of the machine, default gateway, hostname and this information could be used by the social engineer to attach the university network.

2.8.2 Social Engineering Attack Methods

Social engineering attacks can be achieved in any place which has human interaction involved as it has different or various forms. According to Bansla et al., (2019), there are five common activities of digital social engineering attacks as discussed below:

Phishing: This is a trick of sending emails and text messages to a system user with aim of promoting a sense of seriousness, necessity, strangeness or panic in the targeted

user. Phishing is a common and prominent attack in social engineering. This type of persuasion prompts users to divulge or releases confidential information by clicking on links leading to malicious websites or downloading attachments that accommodate malware. In the phishing technique, the same message is sent to all users, usually simultaneously (Banu et al, 2013)

Spear Phishing: This type of phishing attack selects specific system users or organisation. Spear phishing technique requires several attempts on the side of the attacker and it may take a considerate amount of time as to pull this scheme off. These schemes are done expertly therefore making them mostly undetectable. In this type of phishing, the attacker modifies the messages established on features, job positions and contact possession of the under-attack person as to make the attack less noticeable or recognizable (Banu et al, 2013).

Baiting: Baiting encompasses a defective promise to stimulate, provoke the under-attack person ‘s material or curiosity. This scheme persuades the users in such a way that they confine them and steal all their vital data or impose malware in their system. Physical Media is the savage form of Baiting which is used to diffuse the malicious malware in the system. The victim clicks the bait because of curiosity and then places it in work or home computer evolving it in the automatic installation of malware. Tempting and attractive advertisements which guide to harmful sites or urges the users to download the malware-infected application are the online form of baiting scheme (Nabie & Schmick, 2016).

Scareware: This attack comprises of the victims who are flooded with flawed panic and fake challenges. Scareware is also mentioned as deceitful software or fraud ware. It is dispersed through spam emails which come out with deceitful threats or create offers for users to buy harmful services. Users are misled to believe that the system is

damaged by the malware, persuading them to install software that has no benefit to the person but the striker or it is a malicious malware itself (Shivam, 2019).

Pretexting: The attack is instigated by an attacker pretending to need crucial information from a victim as to carry out an evaluative task. The attacker obtains information through ingeniously crafted lies. The attacker queries in such a way that person under attack ‘s identity is confirmed and through this critical information could be assembled. The attacker instigates by pretending as a co-worker, police and tax officials who have the authority to know things (Banu et al, 2013).

This study employed a spear-phishing method to attack end users because it gives room for several attempts e to draw the attention of the end-users. A good deceiving email was created and it was presented as if it was from the UNAM IT technician.

2.8.3 Types of Social Engineering Skills

The following are some skills and techniques that could be employed by the social engineer to trick users to get access to confidential information or system. These skills are summarised as follow:

Mimicking a Staff member: This is an art of discovering the situation to convince a target, which can be a person or a computer to release information or perform an action. This is usually conducted via telephone call or sending an email to the targeted person or computer. Most influential and dangerous hoax for the accomplishment of physical access to any system is to pretend to be somebody from inside the institution. Some users may give their password to an unfamiliar person on a phone call, thinking that the person is a member of IT staff. This is specifically true if the caller indicates that their account may be restricted or disabled and might not be able to access important e-mails or access needed network shares if they do not cooperate. It is the most time-

consuming attack as it requires investigation and research to get data and information regarding target to establish the legality in the mind of target (Shivam, 2019).

Threats Tactics: what happens in this particular technique is that the social engineer attempts to pretend as somebody important like a big boss from headquarters, an inspector from the government, a top client of the company, or someone else who can instil fear into the heart of regular employees. The attacker comes storming or raid in, or calls the victim up, already screaming, yelling, angry, irritated or annoyed. The social engineer may also threaten to fire the employee if the required information is not found (Shivam, 2019).

Deception: This is an effort or attempts to trick and pretend the individuals into trusting something false. It also may lead to sudden decisions being taken due to fear of any untoward incident.

Playing on user's sympathy: The social engineer may pretend to be an employee from outside, perhaps from the phone company or from Internet Service Provider (ISP) Company. The employees can be bamboozled to give information over pity and nature of people is to help a person who is in trouble (Bansla et al., 2019).

Creating misunderstanding: Another trick involves first creating a problem and then taking advantage of it. It can be as simple as setting off a fire alarm so that everyone will vacate the area quickly, without locking down his or her computers. Social engineers can then use a logged-on session to attack and eavesdrop on the network (Shivam, 2019)

Reverse social engineering: An even trickier practice of social engineering take place when a social engineer gets and makes others to ask him or her questions instead of questioning them. These social engineers usually have to do a lot of planning,

preparation, scheduling, forecasting, research and investigation to pull it off, placing themselves in a position of seeming authority or expertise (Salahdine & Kaabouch, 2019).

Mail: The use of an interesting subject line triggers and activates an emotion that may lead to accidental participation from the social engineer. There are two common forms. The first involves malicious code; this code is usually hidden within a file attached to an email. The intention is explained in an international journal of computer for improving the Quality of Service (QoS) of routing protocols in Mobile ad hoc networks (Hadlington, 2017).

Dumpster diving: Someone from the company throwing away junk mail or letter of the company without tearing the document. If the mail contained personal information or credit card offers, that dumpster diver could use to carry out identity theft. Dumpster diver also searches for information like company organisation chart, who reports to whom, especially a management-level employee who can be impersonated to hack important detail. Dumpster diving information can be used in the impersonation attack (Salahdine & Kaabouch, 2019).

This study adopted the impersonation technique because the attacker wanted to pretend as the IT personnel, whereby the attacker pretended to be the staff from UNAM computer centre and requested user to click on the link provided in the emails to disinfect their computer.

2.8.4 Social Engineering Mitigation Techniques

Social engineers influence human emotions such as peculiarity or panic to proceed with the schemes and lure the victims in their confines. Hence, always be cautious whenever you sense distress by an email, tempting to an offer which is exhibited on a website or when we come over random digital media lying about. Our attentive

existence can assist us in shielding our self in case of social engineering attacks in the digital world. Subsequent points assist us to enhance our surveillance with social engineering hacks (Mouton et al, 2014).

Do not open emails and attachments from suspicious sources: An attacker could have commenced the email addresses are scammed all the time, an email supposedly approaching from a reliable source. Never reply an email whose sender you don ‘t knows and if you are acquainted but are doubtful about their messages, verify and authenticate the news from other sources like telephones or service provider ‘s (ISP) website (Hadlington, 2018).

Use multifactor authentication: One of the possessions attackers pursues issuer’s credentials. Therefore, use multiple verifications which guarantee the account ‘s insurance in the case of system compromise.

Beware of tempting offers: when the user receives an offer which is too tempting or attractive, the user needs to think prudently before accepting it. To validate whether the user is dealing with a valid or credible offer or a deception, just google it, it could assist.

Keep an antivirus or antimalware software updated: Institution should ensure that automatic updating is active or make sure to download the updated signatures first every day. Regular verification should be checked to ensure the application updates are performed then scan to find the possible infections (Namaya et al, 2018).

Anti-phishing tools: The use of this tool is attached to a database of blacklisted phishing websites and helps to suggest them. These tools are unable to give full security as the phishing sites are cheap, simple to construct and lifetime is of few days.

The examples are: Web sense, McAfee ‘s anti-phishing filter, Netcraft anti-phishing system and Microsoft Phishing Filter.

Strong passwords: Individuals system users themselves should ensure sustaining a strong password and changing occasionally. Same passwords for all accounts are not recommended at all as the security is in jeopardy. Some people should make sure they have passwords in them keep some crucial data in phones safe. Obedience on office network should be assured by the institution (Sun et al., 2011).

Education and training: This includes progressing security awareness and training programs to develop employees in approaches to resist social engineering. It should involve periodic prompting about the essentials of security consciousness (Keller et al., 2005).

2.9 Vulnerability Assessment and Penetration Testing (End User Security Assessment Strategies)

The vulnerability assessments (VA) are very crucial in information security and requires to be performed on regular basis; monthly, bi-weekly if not daily. VA assessments are cheap methods to detect and report on security problems that could be prevailing in the website, applications, software and devices could be exposed to exploitations. This allows the network administrators and database administrators to close loopholes in the institution network. There an English proverb which says ‘’prevention is better than cure’’, therefore it is sensible idea to anticipate attacks by performing vulnerability assessment on the institution network, be proactive.

There are tools that could be used to perform VA on the institution network, one of the common tools used to carry out vulnerability assessment is penetration testing. Network administrators use penetration testing to determine how weak or robust the

network is in terms of information protection. This section discussed vulnerability and penetration testing as a method of mitigating security issues.

2.9.1 Vulnerability Assessment

What is a Vulnerability Assessment?

First and foremost, one needs to comprehend what is meant by a vulnerability, a vulnerability is a weakness in the application, website, software and network which could be an implementation bug or a design error that allows an attacker to invade the user of the application and get extra privilege and eventually modify information (Doshi & Trivedi, 2015). Vulnerabilities are the possible threat for the IS. Hackers make use of vulnerabilities to exploit the system and get unauthorised access to information or IS**.**

According to Doshi and Trivedi (2015), **a vulnerability assessment** is the method of noticing, recording, and enumerating the existing security vulnerabilities within the network setting. A vulnerability assessment is intended to be a comprehensive evaluation of the security of a vital structure, endpoints, and IT assets. It gives insight into system weaknesses and recommends the appropriate remediation procedures to either eliminate the issue or reduce the weakness to a tolerable level of risk.

Vulnerability assessments typically follows an organised method, which should entail the following:

- Identification and cataloguing of assets; systems, infrastructure and resources in an environment
- Detection and prioritisation of the security vulnerabilities or possible threats to each asset.

- Reporting on the recommended remediation or mitigation of vulnerabilities to reach an acceptable risk level.

The Goal of Vulnerability Assessment

The main objective of a vulnerability assessment is to detect, catalogue and prioritise the group of vulnerabilities existing within the network environment. The intention is to remediate the identified issues to a tolerable risk level (Zeeshan et al., 2017). The objective of a vulnerability assessment emphases on generating a list of identified vulnerabilities and establishing a plan to remediate vulnerabilities. Generally, the focus of the assessment is about breadth, rather than depth, identifying issues across the environment and prioritizing them for remediation based on multiple risk factors.

An institution may identify issues within its environment but is in need of outside technical expertise to diagnose and address the weaknesses. A vulnerability assessment can aid institution to comprehend the problem and establish a plan to remediate the identified vulnerabilities.

In this study vulnerability assessment concentrated on system end-users and social engineering penetration test was used as a tool to assess vulnerabilities on UNAM network based on employees' behaviours towards protecting the university's IS.

2.9.2 Penetration Testing

What is a Penetration Testing?

A penetration test attempts to simulate the activities of outside or interior invaders trying to crack the information security of an institution, it can be an educational institution or health institution or any association (Firmansya et al., 2018). The tester carrying out the test utilises a variety of tools and methods and tries to bypass the prevailing security mechanism of the intended institution. The aim is to gain access to

sensitive systems and confidential information. The procedures that guide the penetration testers is integrally less structured to allow for speedy amendment while testing the network environment. Nevertheless, majority of penetration methodologies stereotypically follow stages:

- Determination of the scope and testing objectives;
- Targeted information gathering and reconnaissance;
- Identification and exploitation of weakness to gain and increase access;
- Demonstrate completion of the testing objective;
- Clean up and reporting.

The Goal of Penetration Testing

The principal aim of a penetration test can be modified depending on the institution and environment undergoing the test. A penetration test usually requires achieving some level of insider access in order to demonstrate control of a key system or asset on the inside network. Penetration tests are robust as they simulate the activities of a real attacker and test an institution's current maturity levels within their security monitoring, network detection, access controls, and security response procedures (Firmansya et al., 2018). Generally, the focus of a penetration test is to demonstrate success against the testing objective. The testing objective could be breaching an organization's border security controls, gaining administrative rights to a key system, or even remaining active on the network for a period of time without detection by the organization's security team.

Penetration testing can provide an institution with a significant value as it relates to understanding the current state of its security operations. However, penetration tests require a higher level of security maturity to realize their full value. As a result,

penetration testing should be conducted by an organization with at least a moderate level of maturity in its security operations.

A moderate level of security encompasses investment in security tools and processes and a team to manage its security operations. This level of maturity allows the institution to test not only the technical security of its environment, but its people, and the incident response procedures that support security operations. As part of an institution's overall Threat and Vulnerability Management Plan, both vulnerability assessments and penetration testing should be performed periodically to ensure the state of operations within an institution is constantly refining.

In study social penetration testing was used to assess UNAM staff members on information security, whereby an impersonating email was sent to specific user to see whether staff members are reacting to the email. The email appeared as if it was sent from UNAM Computer Centre.

2.9.3 Social Engineering Penetration Test

This is one of the penetration testings conducted on the network to mitigate vulnerabilities that could be contained within the network environment. This test is usually performed to test the risky behaviours of system end-users. In a social engineering penetration test, the institution requests the pen tester to attack the users. This is where the use of speared phishing attacks occurs and browser exploits to trick users to malicious activities which could jeopardise the security of information or IS.

Social engineering penetration testing effective techniques

1. Phishing: This is all about sending emails to system users to persuade the users to carry out a certain activity. The objective of most phishing emails in a pen testing task is basically to induce the system user to click on some icons or links and then record

that activity, or to actually install a program as part of a larger penetration testing effort (Ackroyd, 214). Eventually, exploits could be tailor-made to client-side software known to have problems, such as browsers and dynamic content or media plug-ins and software. The fundamental to a fruitful phishing campaign is personalisation.

According to Ackroyd (214), creating the email to the targeted system user, such as by sending it from a trusted or perceived-to-be-trusted source, increases the probability of the user to read the email or follow some manipulations in the email. An experienced pen tester will always remember to check spelling and grammar; a well written email, even a short one, will be much more believable. Perhaps the best acknowledged tool for creating phishing attacks is the open-source Social Engineering Toolkit (SET). With its menu driven email and attack-creation system, it's one of the easiest ways to get started with phishing. Commercial tools like PhishMe Inc.'s PhishMe and Wombat Security's Phish Gurucan also be useful

2. Pretexting: Entails telephoning the targeted users and trying to solicit information from them, usually by playing to be someone that needs assistance from the user or institution. This particular method can function effectively in a penetration testing scheme by targeting non-technical users who can provide useful information (Dimkov et al., 2015).

The good plan is to commence with trivial requests and drop names of real people in the institution who could be expecting for something from somewhere. In the pretexting conversation, the pen tester expounds the need for the targeted user and the target's help. Majority of users are willing to do trivial tasks that aren't perceived as suspicious requests. Once relationship has been established, the pen tester can ask for something more considerable with more success.

3. Media dropping: Media drops usually encompass a USB flash drive left somewhere noticeable, like a parking lot or building entrance arena. The social engineer places an interesting-sounding file on the flash drive that launches some sort of client-side attack when opened. One free tool for creating these files is Metasploit, with its built-in malicious payload generators. The "Infectious Media Generator" option in SET also utilizes Metasploit, but helps automate the process. SET can create a "legitimate" executable that executes automatically when Autorun is enabled on a target's PC. Using automatic execution techniques and interesting-sounding files together can increase the chances of success (Ackroyd, 214).

4. Tailgating: Tailgating is the process of entering into a physical facility by forcing or fooling staff there, or just walking in. Generally, the focus of these tests is to demonstrate that the pen tester can bypass physical security. Pen testers should plan to procure sensitive data or install a device quickly to prove they were successful, as they may have only a short window of time before needing to leave the facility. The pen tester can take pictures of exposed documents left on printers or desks, or install a pen testing drop box device to provide Wi-Fi or 3G network access back to the environment later (Banu et al, 2013).

Through using these four social engineering techniques, the pen tester could expose an educational institution's vulnerabilities and then recommend security controls and education techniques that could mitigate the probabilities of an institution falling prey to malicious social engineering attacks.

This study used social engineering penetration test to gain a better understanding of end user behaviours as a threat that contributes to information security vulnerabilities.

The phishing technique was used in this study to phish emails to target UNAM staff members.

2.9.4 Requirements of a Social Engineering Penetration Test

Like any other penetration test, there are some requirements that an ethical social engineer has to conform to, these could comprise legal and contractual issues that specify liabilities and accountability (Xynos et al., 2010). There could also be a requirement to inform specific individuals that the test is taking place; for example, in relation to health and safety issues where the target is a critical safety system. These requirements can differ across the world, depending on legal structures in the host country and this could lead to a challenge for institution which span international boundaries (Xynos et al., 2010).

Furthermore, the social engineer is contractually and ethically bound to abide by the institutions' requirements but should ensure the penetration test is performed properly and does not lead to a false or misleading sense of security. Even though a code of conduct and best practice is put down out by several professional bodies, in real exercise, the individual is often required to make an informed decision given a particular situation. Therefore, the individual should possess the necessary procedural, ethical permission and technical training.

For this study, the researcher obtained permission from UNAM Computer Centre which is responsible with the management of the university network. The requirements of the penetration test have been met; hence, the social engineering test proceeded.

2.9.5 Advantage of Social Engineering Penetration Test

A social engineering pen test helps exposes various user related vulnerably that could be contained within the network environment. These could include absence of

recommended security policies in place, the lack of security training to end-users or deficiency of strong and appropriate password. A social engineering pen test offers the simulated experience of dealing with a security breach caused by users. It is similar to a fire drill, during which employees are trained to be aware of the possibility of security attacks and threats (Goel & Mehtre, 2015). Penetration testing has an array of benefits and helps identify any potential vulnerabilities, nevertheless, pen test unaided cannot stop information breaches. As a matter of fact, even the most prudently tested and analysed technology or applications could fall prey to attacks.

2.9.6 Social Engineering Penetration Testing Tools

There are numerously automated, free and open-source tools that can be employed to perform social engineering penetration testing; such tools could include.

Table 2.1: Penetration Testing Tools adopted from (Bacudio, et al. 2011)

Social Engineering Tools
• Social Engineering Toolkit (SET): Available for free • Metasploit: Available for free • Infectious Media Generator: Available for free • PhishMe: Commercial • PhishGurucan: Commercial

Social Engineering Toolkit was used because it is the simplest way to embark up a phishing attack and it is for free, which is under Kali Linux tool set which also include a gathering of multiple testing tools used for security tasks as Penetration Testing, Vulnerability Assessment, Information Gathering, Password Cracking or Reverse Engineering. Furthermore, Kali Linux includes more than 600 penetration tools and it

is a very specific list which is used for most common security checks (Hasani & Dode, 2016). This study has used the Social Engineering Toolkit (SET), a tool under Kali Linux tools which has demonstrated efficiency in assessing and identifying human error vulnerabilities.

2.10 The Knowledge Gap

Several studies have discovered areas of vulnerabilities in information systems of individuals and institutions which is either software-oriented or hardware-oriented. Lamar (2012) claimed that databases (information systems) are being attacked today because of the vulnerabilities which are discussed below: (1) Vulnerabilities in Operating Systems like Windows, UNIX and Linux and their services associated with the databases could breed a loophole for illegitimate access which could result into a DoS attack. (2) Database rootkits: A database rootkit is a software package or a procedure that is hidden inside the database and that provides the database administrator with extraordinary privileges to be able to access data in the database. Sometimes the rootkits could turn off alerts prompted by Intrusion Prevention Systems (IPS) and this could be hazardous as information could be accessed by the hackers without being noticed. (3) Weak authentication: Authentication models that are not strong e.g using your name as a password could permit invaders to use schemes like social engineering and brute force to obtain database login credentials of end users. (4) Pathetic audit trails: A weak audit logging method in a database server is hazardous to an institution mostly in retail, financial, healthcare, and other businesses with strict regulatory compliance. PCI, SOX, and HIPAA rules that require extensive logging off actions and also generate events when something went wrong. Lamar (2012) concluded that to mitigate database vulnerabilities, logging to critical transactions in a database must be done in an automated way. Audit trails work as the last line of database defense and can sense any

violation. Audit trails can help trace back the violation to a particular period and a particular user. Lamar (2012) further indicated that audit trails could help in assessing for any database vulnerabilities, identifying compromised endpoints and classifying sensitive data. Managing user access rights and removing excessive privileges and dormant users could also assist in mitigating database vulnerabilities. Monitoring all database access activity and usage patterns in real-time to detect data leakage, unauthorized SQL, big data transactions, protocol and system attacks. Blocking malicious web requests from the network could alleviate database vulnerabilities. Automating auditing with a database auditing and protection platform could be helpful in mitigating some prevalent vulnerabilities. Archiving external data and encrypting databases.

Silver (2013) investigated vulnerabilities with application security and found that to protect against targeted attacks, institutions could organise a scanner to check web applications for vulnerabilities such as SQL injection, cross-site scripting (XSS), and forceful browsing; or they can use a web application firewall (WAF) to protect against these vulnerabilities.

One study by Kashefi (2013) examined vulnerabilities in software and hardware firewalls and discovered that there are four common vulnerabilities in software and hardware firewalls, they are discussed as follow: (1) Insider attacks: firewalls do not protect from insider threats. It is accepted that insiders impose threats to security when they have unlimited access to information, knowledge and valuable assets of their intuitions. End users are granted access legally and this could endanger the security of an institution. Firewalls sniff the packets in the boundaries of the networks and do nothing for the domestic traffic flow. Hence, it is not applied for the intrusions that come from inside the network. (2) Network traffic that doesn't go via firewall: There

are ways to route the prohibited traffic through an unpermitted path that does not pass through the firewall and this is a challenge in safeguarding information. (3) Tunnelling; this is a common way applied to bypass the firewall; one can envelop message for a protocol inside some other message format. (4) Internet threats like virus attack or password cracking: Firewalls do not carry out deep exploration to detect malicious codes in the packets; in this way, they are likely to ignore some threats of this kind. However, as indicated in the prevailing literature synopsis, security studies concentrated more on software or hardware aspects of the information assets while the user aspect remains a virgin land or undressed. The majority of the previous security studies they did not talk about user's weaknesses that expose an institution to risks (human error vulnerabilities). For this reason, this area specifically in the Namibian context, remain not researched. Therefore, this study seeks to unravel this gap by exposing the different types of user errors shortcomings in the world of information security.

In this study social engineering experiment was employed to assess and identify the human errors that contribute to information insecurity. The literature discussed social engineering as the best penetration tool to address user errors in any given network. Hence in order to test behaviours and attitudes of users, social engineering is always a solution. This study is different from the works in the literature review because it is a special endeavour to address the user mistakes towards information system security. It directed on how to deal with the complexity of people towards information security. The user errors vis-à-vis Information Technology (IT) had raised interest from the IT fraternity. Lee (2018) concurred those new solutions to deal with information insecurity had focused on technology alone while a solution to combat human errors had been limited. Frequently, institutions ignore the human errors that are significant

in the security structure. Technology is frequently seen as an immediate solution to information security problems.

Shannon (2019) indicated that even though various institutions make use of a high number of technical security controls, they still show a non-proportional number of security breaches, this happens because Information Security is primarily a human error problem that remains unaddressed. As long as it is people who use technology it is equally important to invest in the people. Related studies reviewed in the literature did not talk about human weaknesses that expose an institution to risks, such as social interaction, customer interaction, discussing work in public locations, taking data out of the office, paper, mobile phones, laptops, emailing documents and data, mailing and faxing documents, installing unauthorised software, removing or disabling security tools, allowing unauthorised persons into the office, opening spam emails, connecting personal devices to company networks, writing down passwords and sensitive data, losing security devices such as id cards, lack of information security awareness, and key data. Furthermore, previous security studies ignored human errors such as, file sharing, storing data on mobile devices such as mobile phones and universal serial bus (USB). The literature also concentrated more on information security mechanisms but did not look at sensitising and training users on basic information security.

Regardless of the robust nature of a security system, it will have to depend on people. The increasing dependence on technical solutions alone cannot handle end users. Kizza (2017) argued that it is a lack of understanding of security problems to think that technology alone can solve security problems. Lee (2018) indicated technological security insufficient and further argued that users are targeted when the technological attacks fail. Therefore, the end user error is an important factor in assessing vulnerabilities in information assets. This study was aimed towards identifying end

user errors that contribute to information insecurity at university specifically in a Namibian context and address them. It guides on dealing with the complexity of people towards information security.

2.11 Chapter Summary

This chapter presented related work to the study, an overview of information security, Information security in tertiary institution and system end user errors as a threat to IS security. The discussed possible causes of system end user errors, information systems security mechanisms and policies in UNAM. The study also deliberated on end user error assessment strategies (social engineering and penetration testing). In summary all literature stated explores the vulnerability studies in software and hardware aspects of information assets, ignoring end-user actions as a potential threat to information security. For this reason, this study investigated the matter intending to close the gap in knowledge on the topic under discussion. The researcher assumes there is a great need to address this problem of end-user error induced vulnerabilities, which had been overlooked by many computer security researchers.

The following end user error has been identified and discussed. This include: following links from unverified senders, chapter 4 under results, deficiency of strong password and inappropriate password, reckless handling of computers, linking to networks outside the university infrastructure ,lack of well formulated personal security policy, use of illegal application, distant worker security, inside attacks, causes of system end-user errors included Absence of Inspiration, lack of awareness and limited competency, wrong believes, behaviours and habits, lack of technology and ICT policy. Threats presented by such errors involve data theft, and system breaches. It is recommended to have assessment strategies and end user security solutions such as

continuous training and education. Critical analysis of human usage of equipment and the systems must be implemented.

CHAPTER 3：METHODOLOGY

3.1 Introduction

This chapter highlights the research methods used for the study. In particular, it presents the research population and sample size, design, research tools, procedures or ethical considerations and an overview of data analysis.

The section discussed; the methodology employed in the study. Research philosophy, research strategies and reasons for choosing a specific strategy were discussed. The target population, sample size and sampling strategies used, were also described. The chapter further discusses the research instrument applied; how it was administration to collect data and also how its validity and reliability were ensured before the data collection. Methods used to analyse the data, limitations of the study and ethical considerations are also described in this chapter.

3.2 Research Method and Design

The study adopted the mixed-method approach to carry out an in-depth analysis of the end user (UNAM staff members) behaviours and perception towards information system vulnerabilities. The mixed method approach endeavours to integrate the two approaches of quantitative and qualitative, seeking the results of both by using both in a research study (Creswell, 2012). This study adopted the convergent parallel design since both the qualitative and quantitative data were collected, analysed and findings compared simultaneously. The quantitative dimension employed a survey questionnaire design to gather information that reflects system user's attitudes, behaviours, opinions and beliefs that cannot be observed directly and exploratory design. An exploratory design was utilised in qualitative dimension of this study because this problem of human error vulnerabilities has not been investigated clearly

and there is no much information available on it and the purpose of conducting exploratory research is to develop more understanding about this problem of end-user's behaviours towards information systems (Avedian, 2014). The study also adopted an experimental research design to collect data from the staff members for the UNAM.

3.3 Population

Population is an entire collection of people, firms, states or objects, that the researcher is interested in, which the researcher would like to describe, explain or predict (Avedian, 2014). The population for this study from which the sample was drawn comprises of 1394 employees working for the UNAM from two campuses, Oshakati and Windhoek main campus. Such population composition included people with different portfolios such as lecturers, directors, IT technicians, network & database administrators, System Analyst and Programmers.

3.4 Sample

This study employed a mixture of both simple random sampling and purposive sampling techniques to select the sample from the targeted population. The qualitative dimension purposefully selected ten (10) out of twenty (20) IT professionals who were selected through the non-probability purposeful sampling from Computer Centre. Ten (10) technicians were taken due to reaching the point of saturation. This sampling strategy was suitable for the current study because the IT professionals are the ones who are at the forefront of mitigating on the victims of information attacks and theft at the UNAM.

The quantitative dimension used a questionnaire with closed questions on staff's experiences with information security and simple random sampling was used to select 310 staff out the 1394 employees working for the UNAM from two campuses

(Oshakati and main Campus), Yamane (1967) formula was used to select 310 participants and is given by:

$$n = \frac{\mathrm{N}}{1+e^2\mathrm{N}} = \frac{1394}{1+0.05^{2*}1394} =$$

310…… (1)

This was suitable in the face of this study since the researcher wanted to find out the experiences of the university staff members on the issue of information attacks and theft.

3.5 Research Instruments

3.5.1 Semi-Structured Interview

Ten (10) IT professionals from UNAM computer Centre were interviewed. The IT professionals work in various roles in the Computer Centre. Their views were solicited on the practices and behaviours (human errors) that employees portray that can make data and information vulnerable to attacks and theft. The interview was unstructured which allowed open responses. The interviews were recorded and the responses were transcribed and analysed. The interview was validated by pilot test, whereby one IT personnel from Oshakati Campus was interviewed for testing.

3.5.2 Closed Ended Questionnaire

A self-administered survey questionnaire with closed-ended questions was distributed to 310 UNAM staff members from Oshakati Campus and Windhoek Main Campus. A questionnaire was chosen because it offers the participant a greater sense of anonymity since participants' name is not written in the questionnaire. The questionnaire was developed under the guidance of the supervisor and piloted. A smoke-screen approach was used in the survey as it was more effective to capture participants' security awareness if they are not aware of their awareness being

assessed. This was because the participants might act differently if they knew that their awareness was being assessed. Therefore, the survey was entitled “Effectiveness in staff-Management relationship”. The title was chosen so that the participants could not realize that the survey was about information security.

The survey comprised of seven scenarios. Two of the scenarios had general attributes that were used as deviation from the hidden subject. The other five questions had the real purpose of assessing participants’ tendency to:

- Access a link from unknown sender
- Respond to requests to install programs form unverified person
- Share keys to wireless network to visitors
- Share username and password with colleagues
- Use weak or strong password

3.5.3 Experimental

An experimental study (Penetration Testing) was undertaken using social engineering, penetration attempts were performed on employees to find out if they follow security standards and policies. The attack was conducted by developing a phony phish system. The goal of the phony phish system was to send phishing emails that can be used to measure the accuracy of the research. The pilot test was done on the phony system, whereby the email was sent to a known person and confirmed its success.

Experimental Setup of a Phony Phish System

- Hypertext Mark-up Language (HTML) Form: This module collects data of the victim who have the tendency to respond to phishing attacks.
- Hypertext Pre-processor (PHP) script: This logs victims’ data to the log file.

- Simple Mail Transfer Protocol (SMTP) server: The SMTP server sends a phony email to each victim. Every email is outfitted with a unique link to the HTTP server.
- Hypertext Transfer Protocol (HTTP) server (Apache): The HTTP server logs victims' information through PHP script

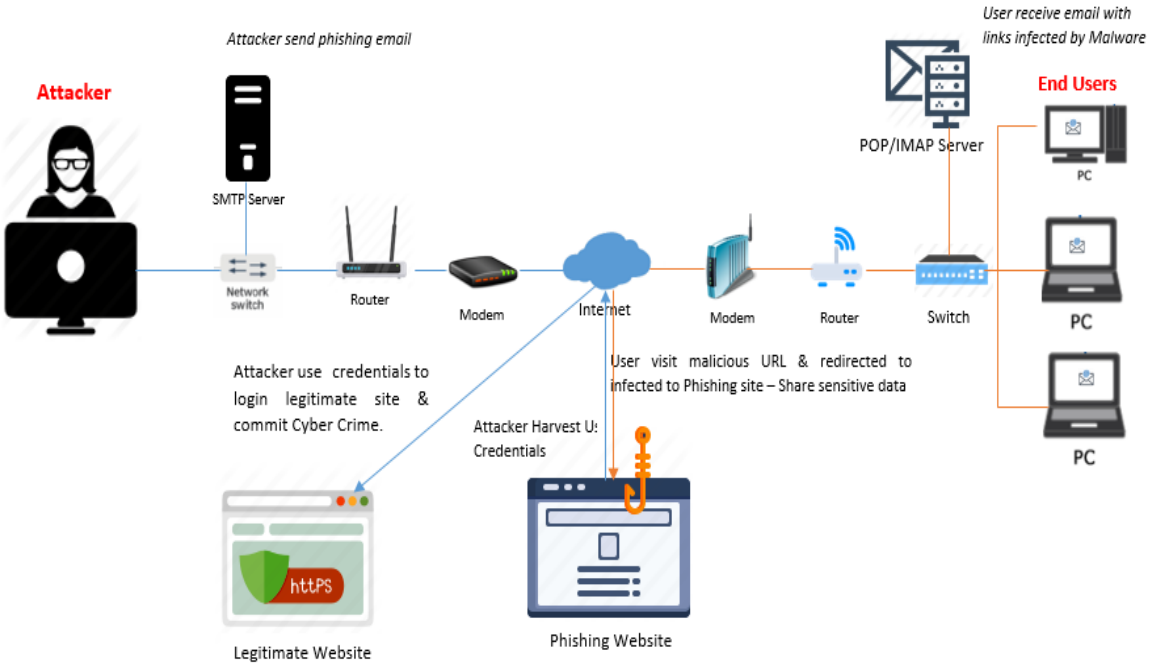

Figure 3.1 : Phony Phish System Architecture and Design

Figure 3.1 indicates the social engineering penetration system which was used to attack UNAM employees in order to find out whether they follow security standards and policies. The attack system sends phish emails and the capture the information of the specific user under attack. To measure the accuracy of the survey, phishing attack was used as a tool in the investigation of information security, whereby persuading phishing email attacks were sent to UNAM network users. The attack requested participants to visit a page which then asked them to input given data to continue. The email was formulated as follows:

Dear UNAM Network User;

Your computer has been infected with a virus and to remove the virus downloads and installs the tool from this link herein https://leancoding.co/70TIYR with the institution's authorized PC cleaner to eliminate the virus from your computer.

Have a nice day.

Kind regards;

IT Technician

UNAM Computer Centre

The raw data gathered from the social engineering attack is tabulated in table 3.1. Fifty (50) emails were sent to the participants, this is the number of staff who frequently use information systems. The email was delivered to 40 employees out of 50, as 10 recipient email addresses were unreachable. Out of the 40 only 30 responded and visited phishing web site.

Table 3.1: Emails sent in social engineering attacks

No. of emails sent	50	
Reachable	Responded	No-Response
	30	10
Non-Reachable	10	

It should be understood that, unlike real phishing attacks, that actual information was only collected for the purpose of the study to prove that user indulge themselves in unbecoming behaviours that could put information at risk, no software was installed on their systems, and the security of their systems was in no way compromised in this experiment.

3.5.4 Configurations and Experiment Protocols

Mail Phishing and Spoofing Experiment

E-mail phishing and spoofing was performed on some selected email addresses using the latest Kali Linux social engineering toolkit. Credential harvester attack method was used to collect information of the victim's (user) computer.

Majority of people who have interest in IT security are curious to know a method to send spoofed emails to friends, colleagues and family for entertaining. But in term of information security, this could be hazardous if users are not educated on such mechanisms that security experts are aware of. However, spoofed emails in spite of the advanced spam filtering technology adopted by email service providers are still possible. This can be done either by using your normal Gmail accounts or Relay servers. A relay server is an SMTP Server that is trusted by major companies as an authorised sender of the email.

KALI LINUX Social Engineering Toolkit (SET) is the standard for social engineering testing among security professionals. Basically, it implements a computer-based social engineering attack. The diagram below shows a representation of a mass mailer which is commonly used to send a phishing page link to the e-mail addresses of the targeted Kali Linux victim as a starting point.

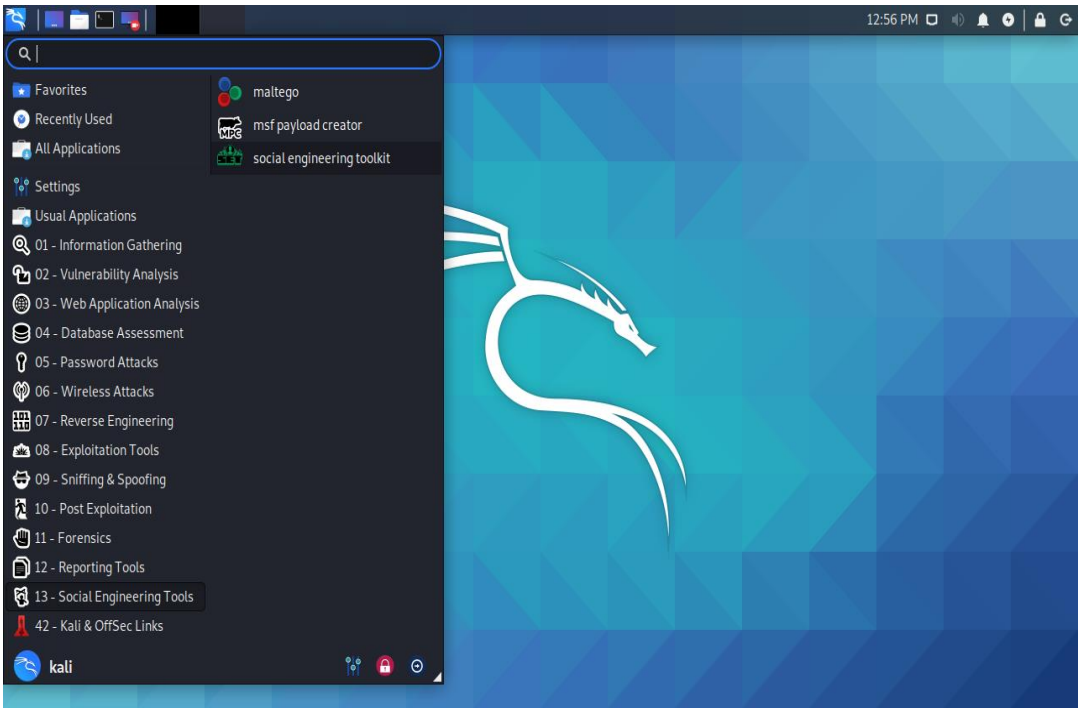

Figure 3.2 A Mass Mailer Which Is Commonly Used to Send a Phishing Page Link To The E-Mail Addresses.

Adopted from (Kali Linux tools, 2020).

Figure 3.2 indicates where to find a mass mailer that is commonly used to send a phishing page link to the e-mail addresses of the targeted Kali Linux victim as a starting point.

In another diagrammatic representation below is an output from the undertake experiment showing the types attack to be conducted.

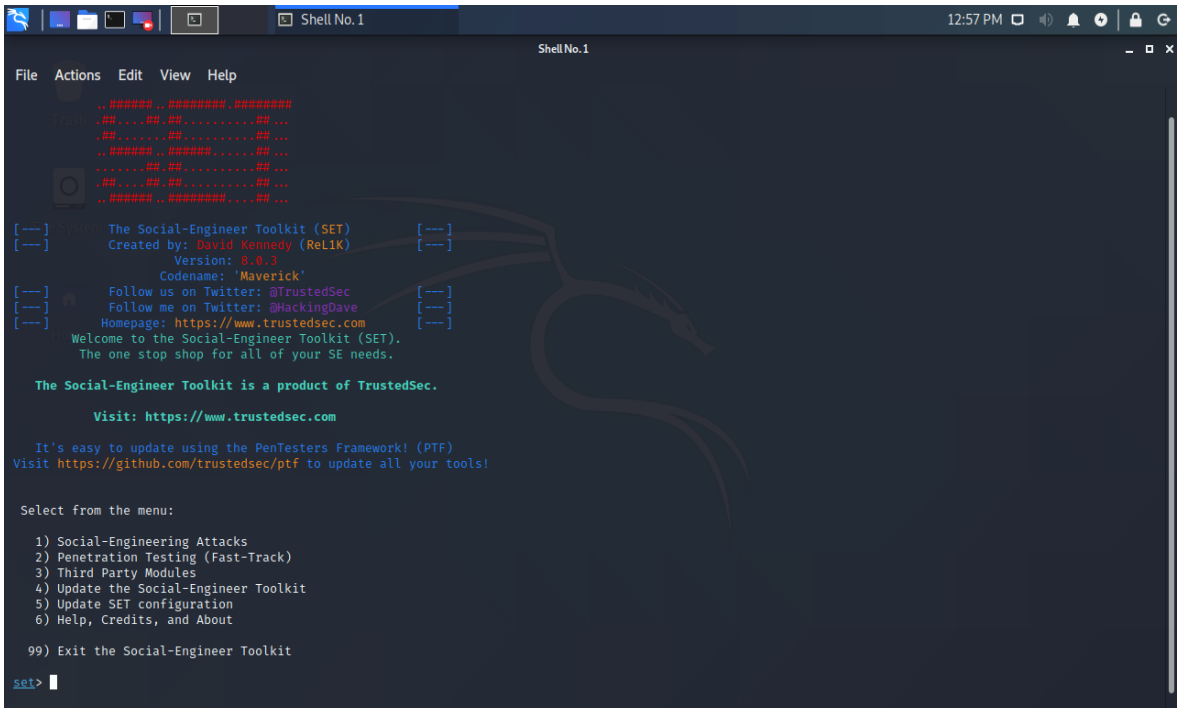

Figure 3.3 Types of Attack to Be Conducted

The Figure 3.3 indicates the types attack to be conducted. Here social engineering which is in option 1 had to be selected from the attacks menu since email phishing falls under that.

The Figure 3.4 shows social engineering attacks types whereby mass mail attack option was selected.

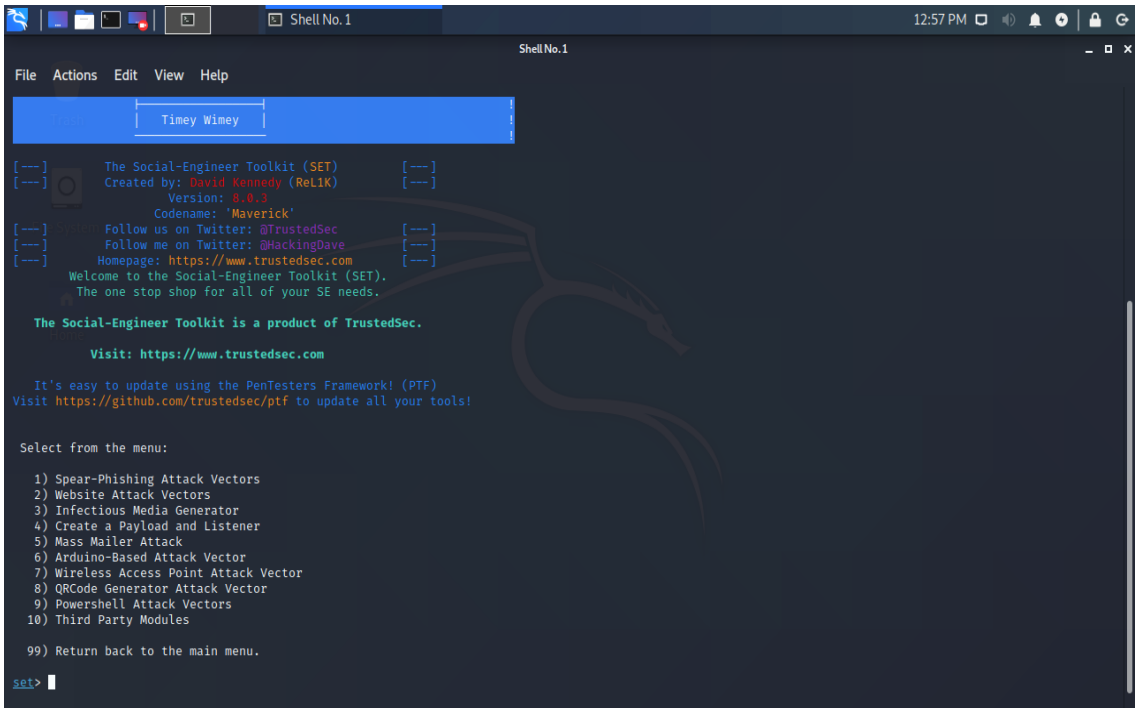

Figure 3.4 Social Engineering Attacks Types

The Figure 3.4 indicates social engineering attacks types. Here email phishing is being experimented and, hence mass mail attack option was selected.

In another diagrammatic representation below shows options on how emails will be sent to victims are shown.

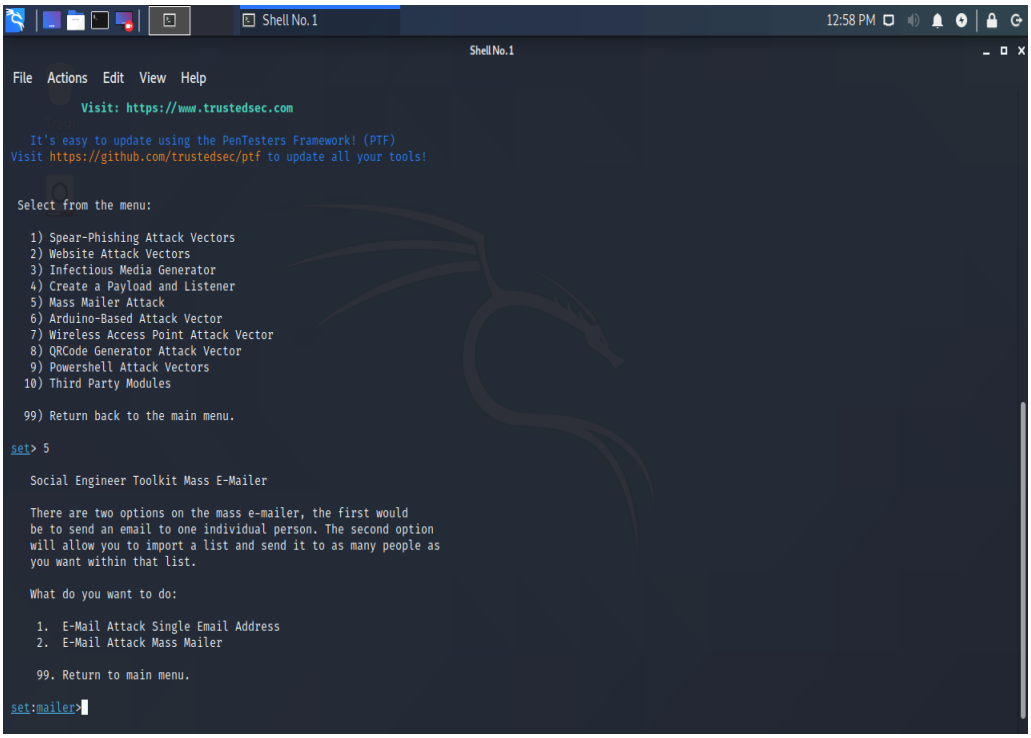

Figure 3.5 Options On How Emails will be Sent to Victims

Figure 3.5 indicates options on how emails will be sent to victims. Whether the attack will be performed on a single email address or mass emails. In this case mass mailer attack option was chosen.

The diagrammatic representation below shows indicates the options of email address to be used to perform an attack.

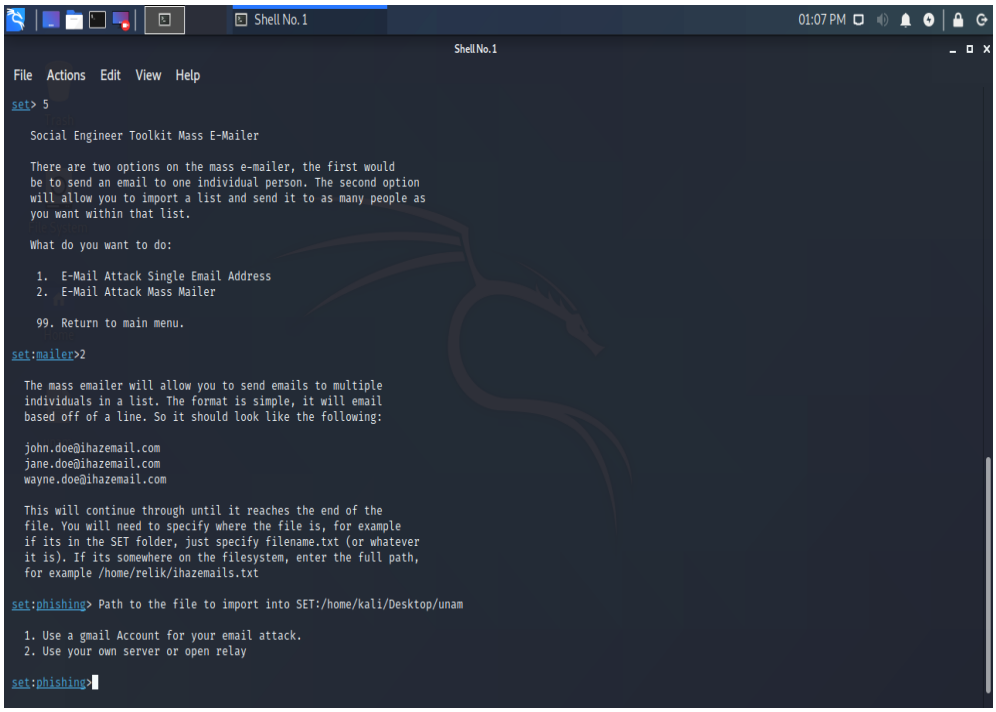

Figure 3.6 Options of email address to be used to perform the attack

Figure 3.6 indicates the options of email address to be used to perform the attack, whether is Gmail email or other mail server. In this experiment Gmail account was used hence, option 1 was selected.

The diagram 4.22 indicates the prompting for Gmail account to be used

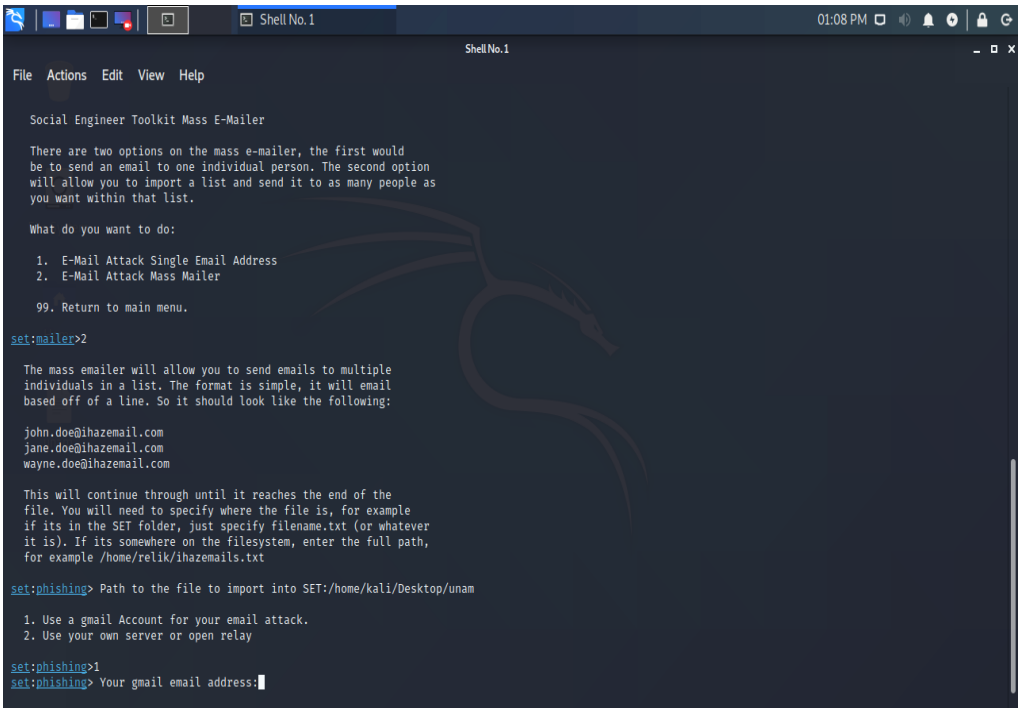

Figure 3.7 Prompting for Gmail account to be used

The Figure 3.7 is prompting for Gmail account to be used.

The Figure 3.8 shows flagging the email as high priority

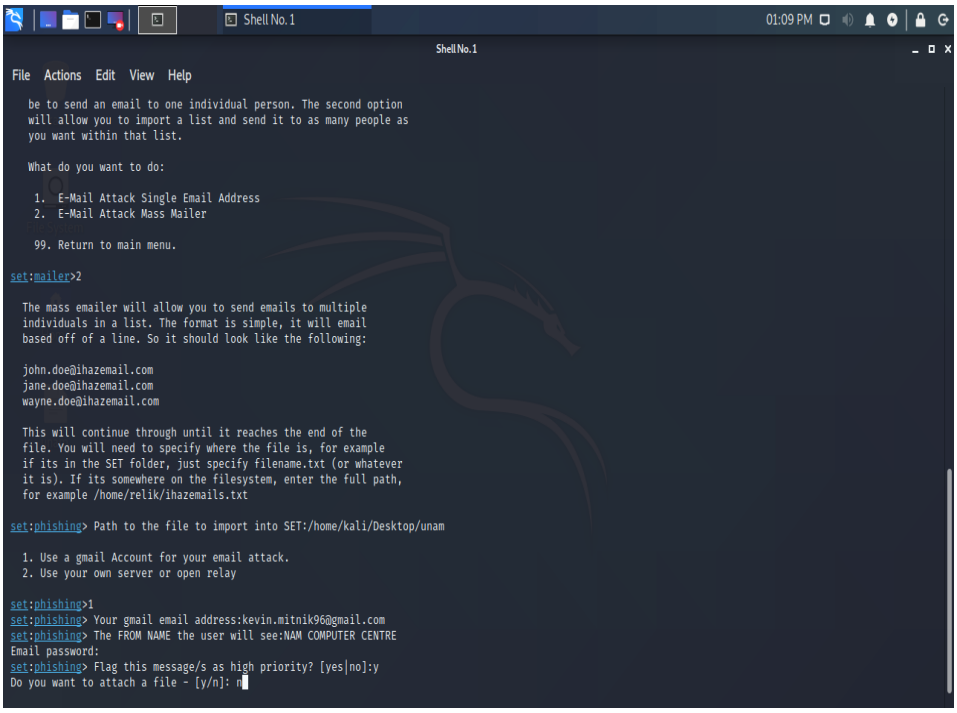

Figure 3.8 Flagging the email as high priority

Figure 3.8 indicates flagging the email as high priority. This prevents the message to go into the spam box at the recipient side instead of going into the inbox. When flagged as high priority, then it will not go in the spam box.

The Figure 3.9 shows the body of the message to be received by the target

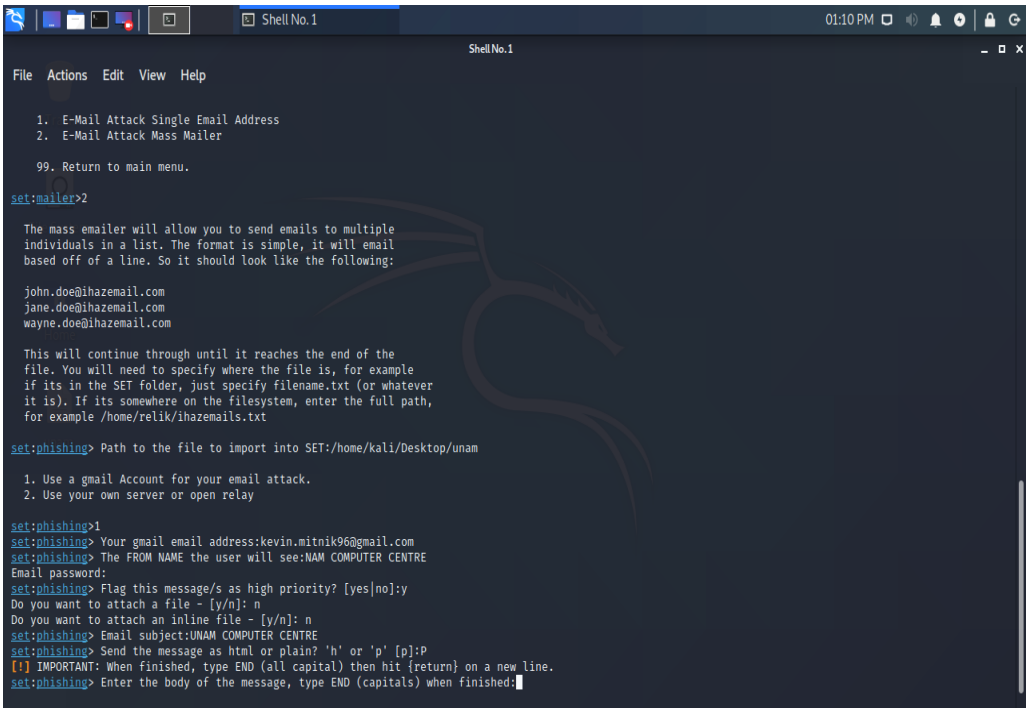

Figure 3.9 Body of the Message to be Received by the Target

The Figure 3.9 shows the body of the message to be received by the target. The message should look attractive and not so open for the user to detect.

The Figure 3.10 shows turning off the less secure settings in google so that it does not regards or sees our tool, kali Linux as a harmful or untrusted app or system.

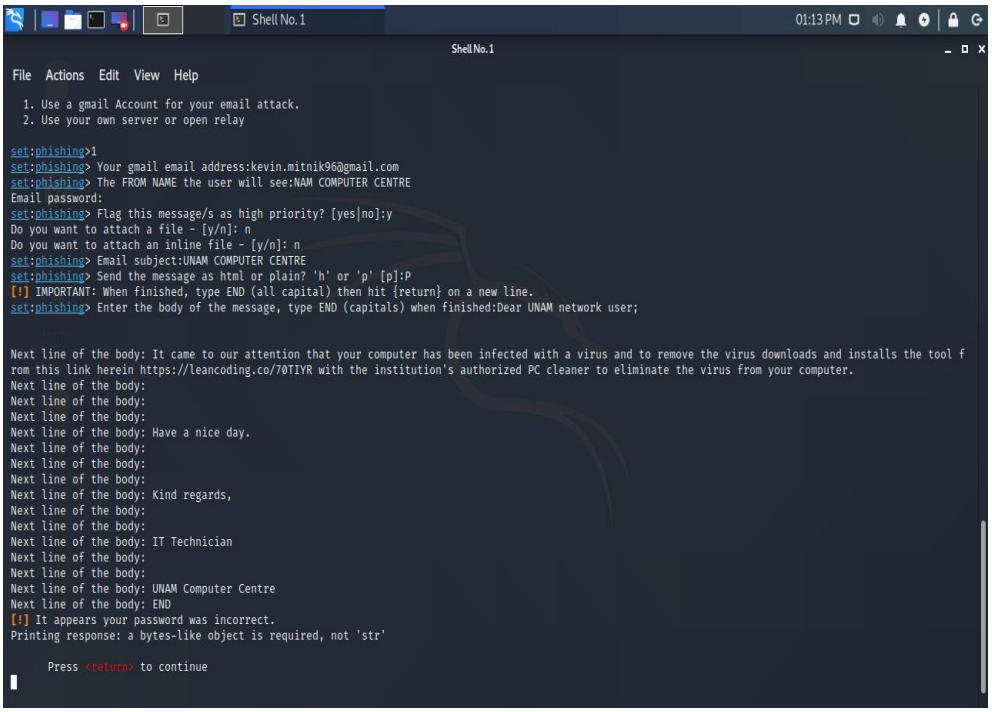

Figure 3.10 Turning Off the Less Secure Settings in Google

Here it can be seen that the emails were not sent to target emails. The reason is that, since the researcher was using Gmail email address to do this experiment and Gmail is very secure, the researcher need to turn off the less secure settings in google so that it does not regards or sees the tool, kali Linux as a harmful or untrusted app or system. So, it was turned off in google and in the next Figure the emails started going through as anticipated.

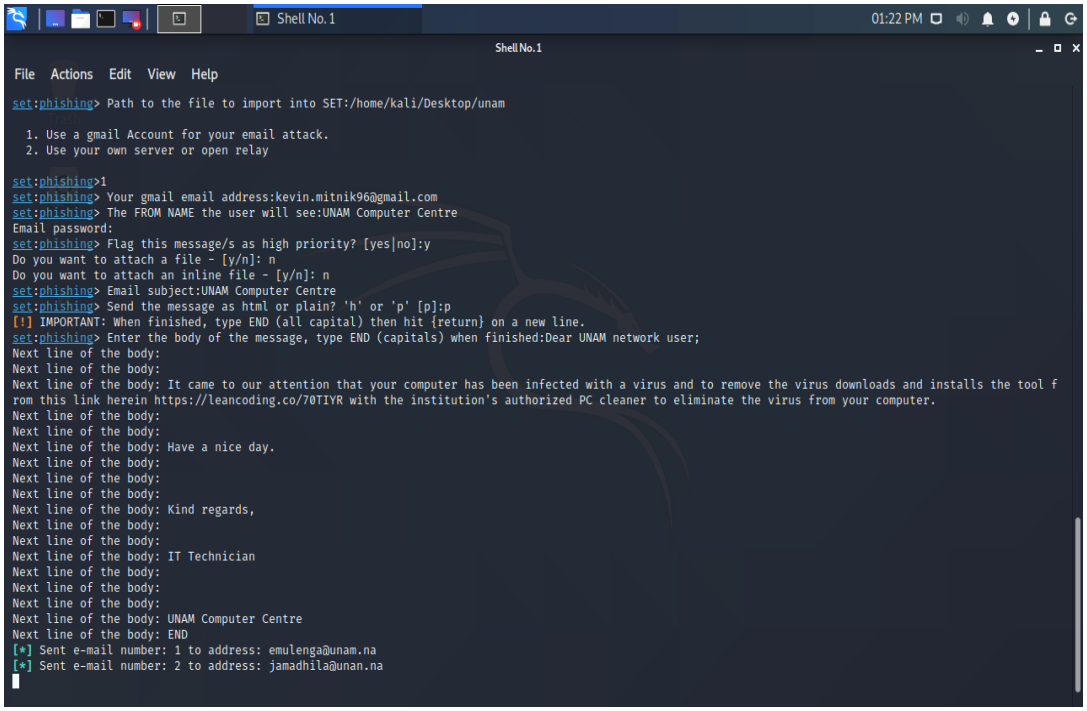

Figure 3.11 E-mail Going Through to Target Email Addresses

The Figure 3.11 shows an e-mail going through to target email addresses

The Figure 3.12 shows a complete screen when all the emails successfully went through

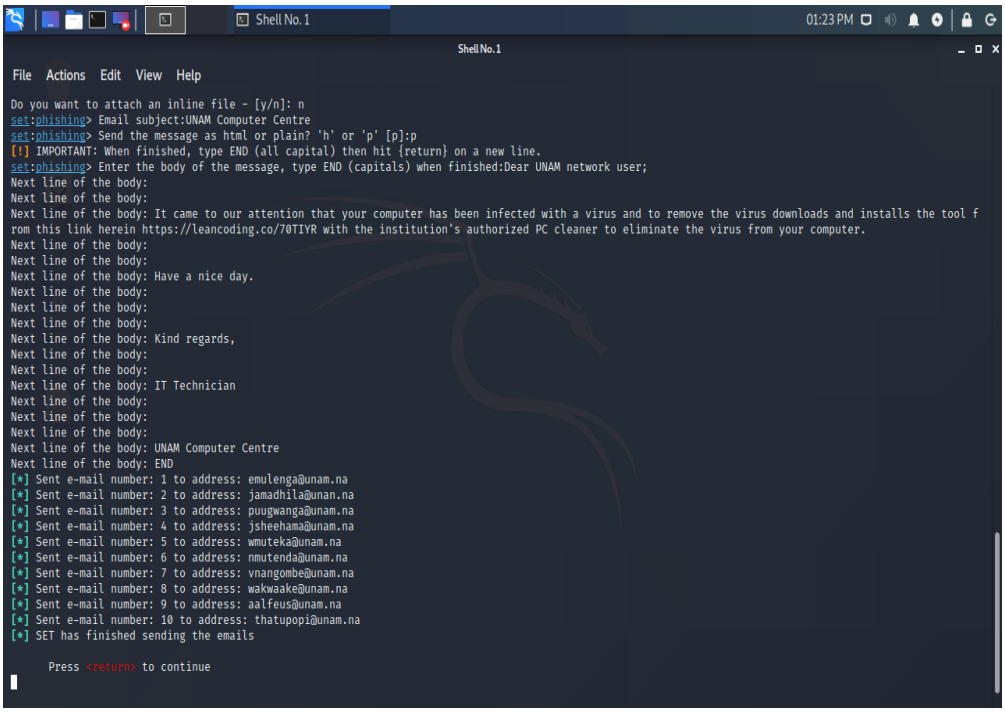

Figure 3.12 : A complete screen when all the emails successfully went through

Figure 3.12 is a complete screen when all the emails successfully went through. Meaning the emails were successfully sent to the targets and just waiting for any possible reply from one or more. One reply can compromise the whole network since the users share the same network and not every user is technically active or security wise.

The spear-phishing attack vectors

The Spear-phishing module allows us to specially craft email messages and send them to our targeted victims with attached So, payloads for example, sending malicious PDF document which if the victim opens it, and it will compromise the system. There are three options for the spear phishing attack:

- Perform a Mass Email Attack
- Create a File Format Payload
- Create a Social-Engineering Template

To track the results from targets, another tool called IP Logger is used. Results can be Geo-logged from IP Logger as a location tracker to track the exact GPS-based location of the clicked or open the e-mail. IP Logger URL shortened provides the most advanced and detailed statistical data for all clicks on links or views of images. Information about user's IP address, country, city, and type of device, browser and other useful information can be accessed through IP Logger.

3.6 Procedure

For objective (1), professional and technical inputs were solicited from IT professionals through interviews. The data for the second objective (2) was collected using a survey questionnaire that was distributed to employees who frequently utilise information systems. For objective (3) social engineering experiment was conducted to test the accuracy of the survey and to aggregate data for specific identified variables. A phony phish system was developed to test user's information security. The goal of the phony phish system aimed at send phishing emails that can be used to measure the accuracy of the survey.

3.7 Data Analysis

Quantitative data from the questionnaires for this study were analysed using MS Excel and the SPSS software version 26 to answer Objective (2). This part of the study was descriptive; hence, tables and graphs were used. The qualitative data from interviews and the phony phish system was analysed using content analysis to generate themes to answer Objective (1). The researcher transcribed the data and followed the eight steps for data analysis as proposed by Creswell, 2014). The researcher gets a sense of the whole by reading all the transcripts carefully, jotting down along the margin some ideas as they come to mind in connection with each topic. Choosing the transcript on top of the pile of the transcribed interviews, the researcher reads through the transcript,

asking himself what it is that he is reading. This step involved thinking about the underlying meaning, rather than the "substance" of information. This process was repeated until a list of all the themes were generated.

The themes were then clustered together into baskets that could be labelled as "major themes", "unique themes" and "left-overs". With the list at hand, the data is revisited. An abbreviation for each of the topics was made in the form of codes and the codes were written next to the appropriate segments of the texts. This preliminary organizing scheme was used to see if new categories and codes emerge. The researcher found the most descriptive wording for the topics and turns them into categories. Efforts were made to reduce the total list of categories by grouping together topics that related to one another. Lines were drawn between categories to show interrelationships. The researcher then made a final decision on the abbreviation for each category and alphabetises the codes (Antwi & Hamza, 2015).

3.8 Reliability and Validity

The research instruments were tested for content validity. Taherdoos and Lumpur (2016) defined content validity as to measure or quantify what is intended to be measured. In view of this, the content validity was ensured in the study through literature review and was determined by experts like supervisors and mentors' opinion in the development of the questionnaire. Furthermore, Suresh (2016) stated that test-retest reliability could be utilised to determine the magnitude to which the test scores were reliable. In addition, Taherdoos and Lumpur (2016) stated that the reliability of numerical experiment data could be strengthened by increasing the data collection process and by maintaining consistency of the output. The questionnaire was developed under the guidance of the supervisor and piloted. The degree of agreement between the supervisor and the mentor determined the reliability of the questionnaire.

After the piloting phase, the problem questions were adjusted for some slight ambiguities and other related issues in order to enhance the reliability and validity of the instrument. Suresh (2016) indicated that if the research findings could be repeated, it is reliable and further described reliability as the extent to which a measuring instrument is repeatable and consistent.

Hereafter, the inter-rated reliability is used to rate uniformity of the questionnaire. The self-administered survey questionnaire is structured in such a way that only valid responses were captured from the participant. Social engineering experiment was carried out to ensure the reliability and accuracy of data collected from the survey. Filtering is used to enhance valid responses for some particular questions that needed particular information. Before data analysis was done, data cleaning and consistency checks in the captured information were done through the use of cross-tabulations and frequency tables. Values that were inconsistent with what was expected for particular questions were dealt with accordingly, that is, either removed or corrected.

3.9 Data Verification

Mugo (2017) presents the model of ensuring the trustworthiness of qualitative data was applied. The four characteristics to ensure trustworthiness are truth-value, applicability, consistency and neutrality.

3.9.1 Truth-Value

Truth-value asked how confident the researcher is with the truth of the findings based on the research design, informants and the context in which the study was undertaken. It is concerned with whether the findings of the study are a true reflection of the experiences of the study participants (Antwi et al., 2015). Truth-value is established by the strategy of credibility and, for the purpose of this research, the researcher used the following criteria: Interviewing techniques. The researcher made use of various

interviewing techniques during the interview, for example probing, verbal and non-verbal expressions, restating and summarising in order to enhance the credibility of the study.

3.9.2 Applicability

Almalki (2016) defines applicability as the degree to which the findings can be applied to other contexts and settings or to other groups. Applicability is established through the strategy of transferability. In order to achieve transferability, the researcher provided a dense description of the research methodology employed in the current study.

3.9.3 Consistency

Consistency of data refers to "whether the findings would be consistent if the enquiry were replicated with the same subjects or in a similar context" (Mugo, 2017:34). Consistency is established through the strategy of dependability and it was achieved by using an independent coder.

3.9.4 Neutrality

The fourth criterion is neutrality. It refers to the extent to which the study findings are free from bias. Antwi et al.(2015) proposed that neutrality in qualitative research should consider the impartiality of the data rather than that of the researcher, which suggests conformability as the strategy to achieve neutrality. The researcher tried to maintain neutrality by not giving his own opinions during the interviewing process.

3.10 Ethical Considerations

Ethics should be applied at all stages of research, whether it is planning, data collection, evaluation and reporting of the research findings. The four basic ethical

principles are autonomy, beneficence, non-maleficence, and justice. Some of the facets of ethical researching which was applied by the researcher are as follows:

3.10.1 Informed Consent

A written consent was sought from all participants after an explanation on the purpose of the study has been given by the researcher prior to participation. This was a sign of respecting their autonomy. The informed consent form used by the researcher in the study is attached as Appendix D.

3.10.2 Confidentiality

The researcher observed privacy and confidentiality at all times by protecting the identity of all the participants. Raw data was filed and kept safe where access to it was restricted. Interview proceedings did not contain the names of the participants.

3.10.3 Non-Maleficence

Ethics refers to the part of human philosophy concerned with appropriate conduct and virtuous living (Avedian, 2014). Ethics involves the entire research process from the nature of the problem under investigation, reporting the theoretical framework underpinning the study, the research context, and data collection instruments and methods being utilised, the research participants involved and the procedures used to analyse the data (Creswell, 2014). This study involves human subjects and as such, special precautions will be taken to protect the rights of these human beings. Researcher ensured that no harm would place to the participants because of the research. This should be ensured before, during and after the research. Data was collected through an in-depth face to face interview which was filed and kept safe therefore the researcher does not foresee any harm.

To uphold the principle of beneficence or “doing what is good”, Blaikie (2014.p12) suggest that the main aim of the researcher should be to produce results which will be

beneficiary to the individuals and the entire society at large. Apart from that, consideration for the potential for harm among the participants will also be observed. The study involved human participants therefore clear and careful elucidation of the risks and benefits of the study should be made clear to the participants prior to the study. A clear measure of whether the risks involved would outweigh the benefits had been made. The researcher obtained a written approval clearance from the University of Namibia Ethical Clearance Committee, Appendix E.

The principle of respect for human dignity affirms the rights of students to self-determination, and the right to decide on whether to participate in the study or not, after full disclosure of the aim and purpose of the study (Blaikie, 2014). Full disclosure in this respect means that prospective participants should be informed of the identity of the researcher, the purpose and nature of the study, the right to participate and the right to withdraw anytime they wish to without any penalty, the responsibility of the researcher, and possible benefits of the study, measures to ensure privacy, anonymity and confidentiality.

The principle of justice includes the participant's right to fair treatment and privacy (Akaranga & Makau, 2016). This fair treatment should prevail before, during and after their participation in the research study. Furthermore, participants should be treated with respect and dignity and should always be free to ask the researcher for clarity on where they did not understand; and should they wish to withdraw from the study there should be non-prejudicial treatment.

A formal application to the University of Namibia Ethical Clearance Committee for clearance was made seven months before the study was undertaken. In making the application, a clear and detailed research proposal together with all the research

instruments was submitted for ethical clearance. An informed consent form explaining the nature and purpose of the study was completed and enclosed in the application.

With regard to withdrawals, participants were told that they are free to withdraw from the study should they feel they do not want to continue participating in the study. The participants were then then requested to sign consent forms before taking part in this study. Data was captured on a personal computer which was password protected. Pseudonyms were used for the research participants and they were assured of anonymity and confidentiality at all times.

3.10.4 Voluntary Participation

All participants in this study were voluntarily participating. No force, coercion or bribery was used on participants to take part in the study. Those who refuse to take part in the study was not penalised in any way.

3.10.5 Permission to Carry Out the Study

A formal request to carry out the study was made to the UNAM before data was collected. The researcher only collected data after full permission to undertake the management the University of Namibia granted this study. A pilot testing and the questionnaire has been used.

3.11 Chapter Summary

Research methodology forms the heart and integral part for any research study. This chapter presented the research methods that were used in the study. In this study, the mixture of both quantitative and qualitative research methods was used and well expounded. Additionally, the chapter also presented the research sample that was used in the study. This chapter also presented issues of data analysis, instrument used and the data collection procedures.

CHAPTER 4：DATA ANALYSIS

4.1 Introduction

The chapter presents results of the data analysis for both the qualitative and quantitative data. The results of the study are reflected by way of tables, charts, graphs and statistical data and discussed in relation to the research objectives.

The data was collected and then processed in response to the problems posed in the introductory chapter of this study. The research objectives necessitated the collection of data and hence data analysis and interpretation. The study focused on assessing and identify the human errors that contribute to information insecurity.

The primary data analysis dealt with a detailed statistical analysis of the data followed by the presentation of results and findings. Data from interviews were analysed using thematic analysis. Data from the questionnaires was first coded and then entered into SPSS. In SPSS, descriptive statistics such as frequencies were used to establish the data structure. Then pie charts, bar graphs and histograms were generated in Microsoft Excel to present the data.

4.2 Questionnaire Analysis

In this study a survey questionnaire was distributed to 310 UNAM staff members who frequently use information systems, who were randomly selected from the two campuses (Oshakati and Main Campus). Probability sampling techniques were used through simple random sampling strategy. Out of all the distributed questionnaires, 300 questionnaires were received back and ten (10) staff members could not return the questionnaires. The response rate of the staff members was 80% and it was representative of the sample and hence could validate results. The survey investigated the user's tendency to:

- Access a link from unknown sender
- Respond to requests to install programs from unverified person
- Share keys to wireless network to visitors
- Share username and password with colleagues
- Use weak or strong password

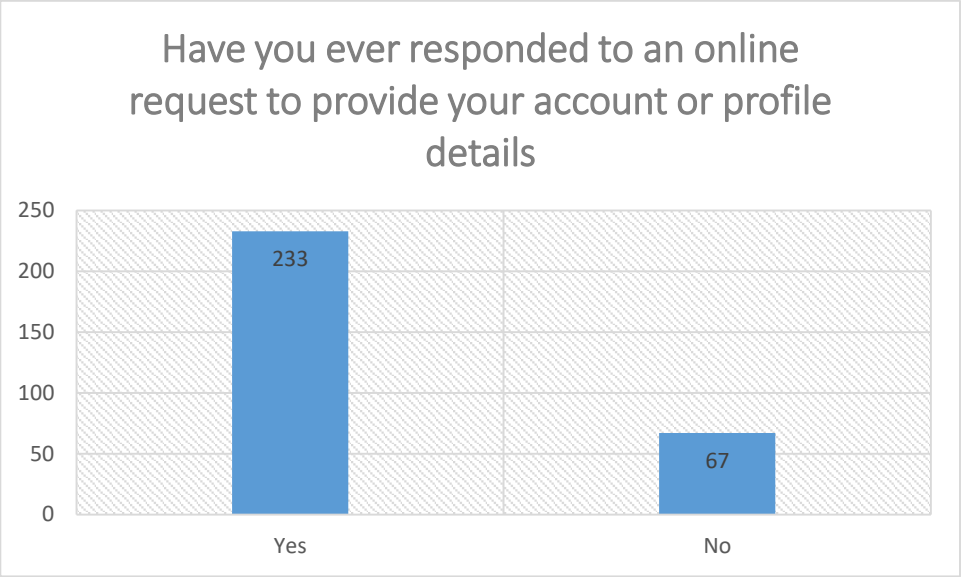

Figure 4.1: Response to an online request

Figure 4.1 shows that is indicating users who respond to online request to provide their account or profile details, 233(77.7%) said yes, while 67(22.3%) said no. The finding from the Figure 4.1 is in line with Osmar (2016) that majority of system users respond to online requests providing their credentials, these users have the potential to become victims of hacking.

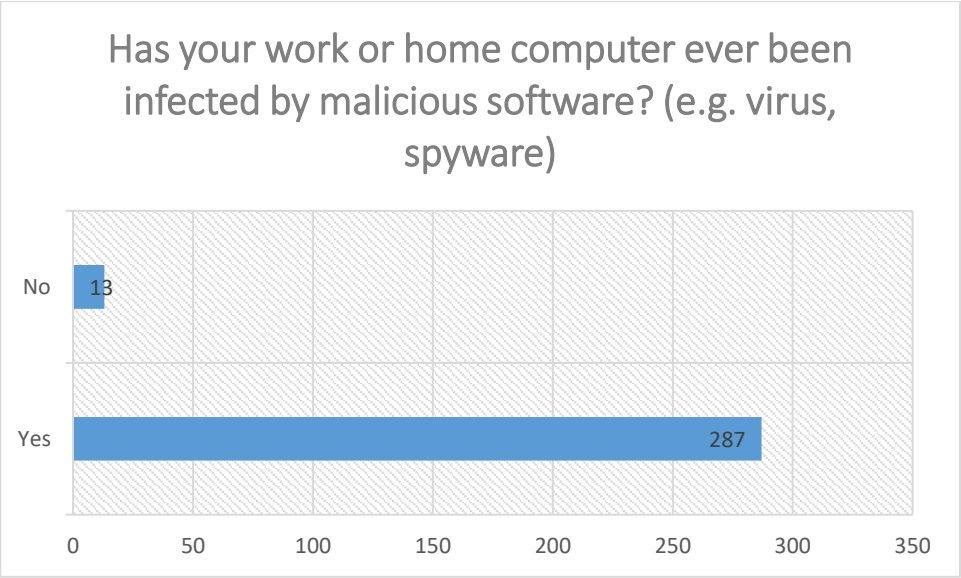

Figure 4.2: Infection of a computer by malicious software

The Figure 4.2 is indicating the infection of user's computer by malicious software. 287(95.7%) users indicated Yes and 13(4.3%) indicated No. Furthermore, it is indicating that majority of participants computers do get infected by malicious software. This attitude of users can put data and information at risk, that hackers can use this vulnerability to retrieve sensitive information from them.

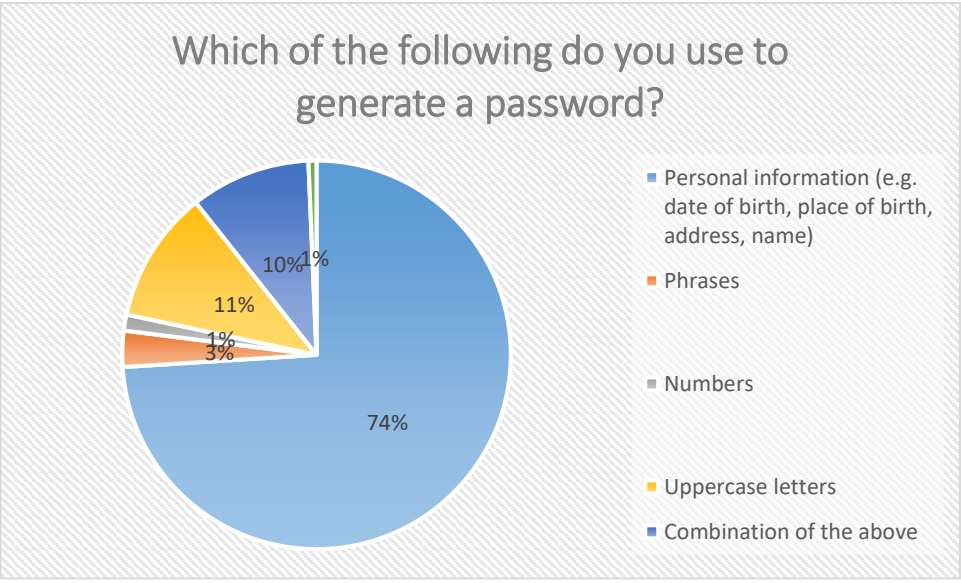

Figure 4.3: Generation of a password

The Figure 4.3 show the characters used by the participant to generate the password. As indicated by the Figure 4.3, 222 (74%) of the participants indicated that they use personal information such as name, date of birth, place of birth etc. to generate

password, 9(3%) of users use phrase, 4(1.3%) use numbers, 33(11%) use uppercase letter 32 (10.75%) use the combination. Having a strong password is one of the ways to protect information. As indicated by the Figure 4.3, users use guessable data (personal information) to formulate their passwords. Their password can be described as weak. The reason why this a problem is that their passwords can be guessed and their account can be broken into easily using brute force techniques thus putting data at risk.

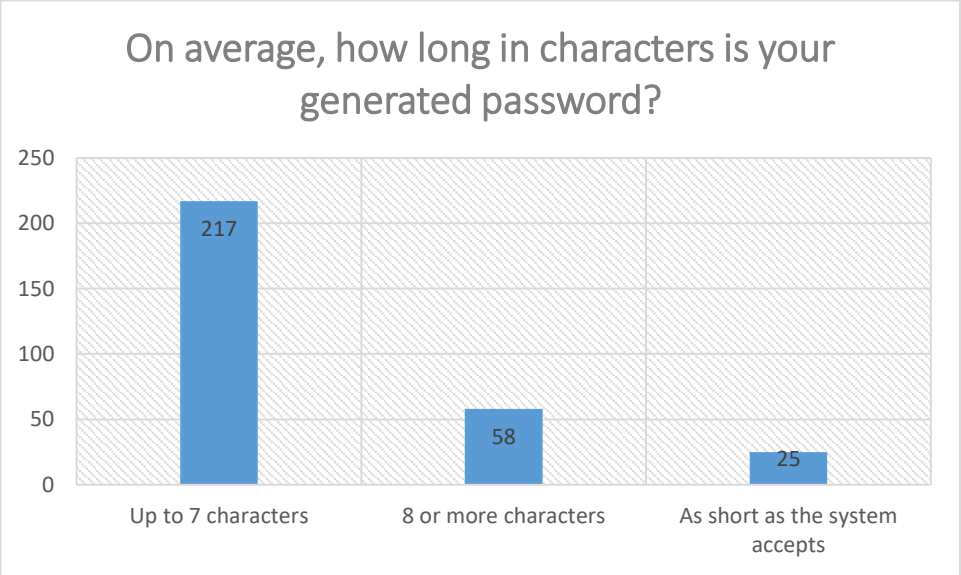

Figure 4.4: Password length

Figure 4.4 indicates that 217 (72.3%) of the participants use up to 7 characters to generate their password. 58 (19.3%) use 8 characters while 25 (8.3%) indicated that their password is short as the system accept.

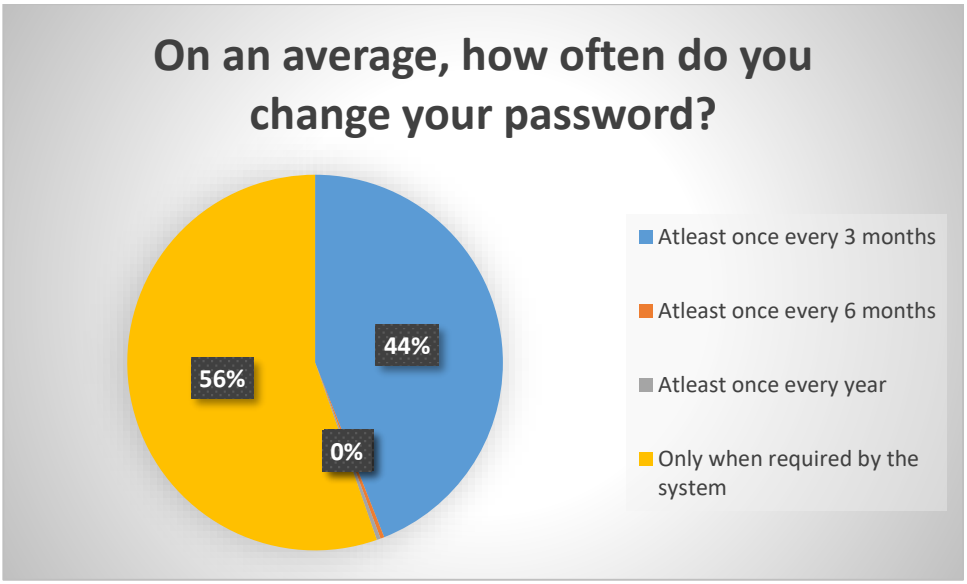

Figure 4.5: Changing of a password

Figure 4.5 indicates that 166 (55.3%) of the participants only change their password when required by the system. 132 (44%) of the participants indicated that they only change their password once every 3 months. One (1) of the participants said change the password at least once every 6 month and one at least every year.

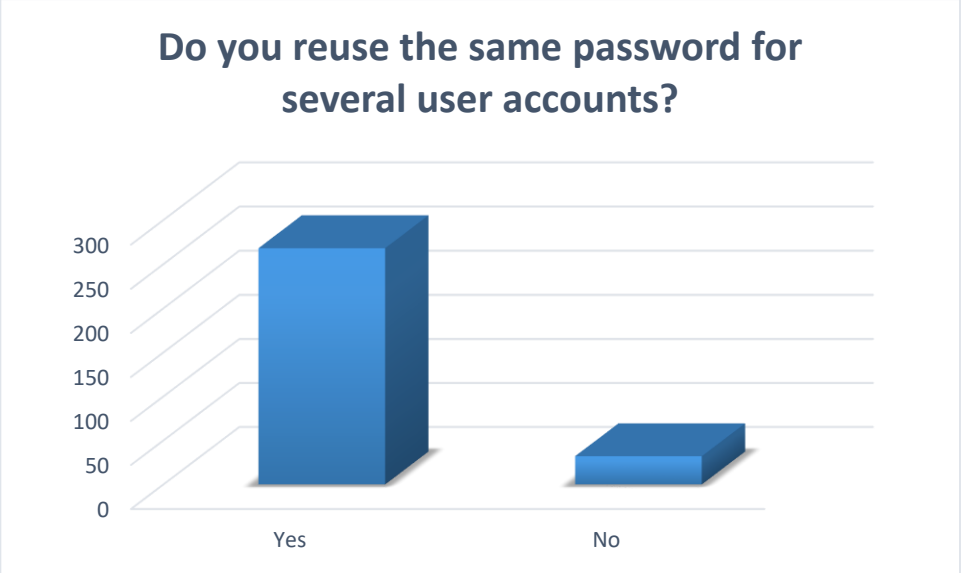

Figure 4.6: Reusing of the same password on several user accounts

The Figure 4.6 indicates that 268 of the participants reuse the same password on several user accounts, for example the same password of the work account is the same

for google account. While 32 of the participants indicated that they do not reuse the same password on several user accounts.

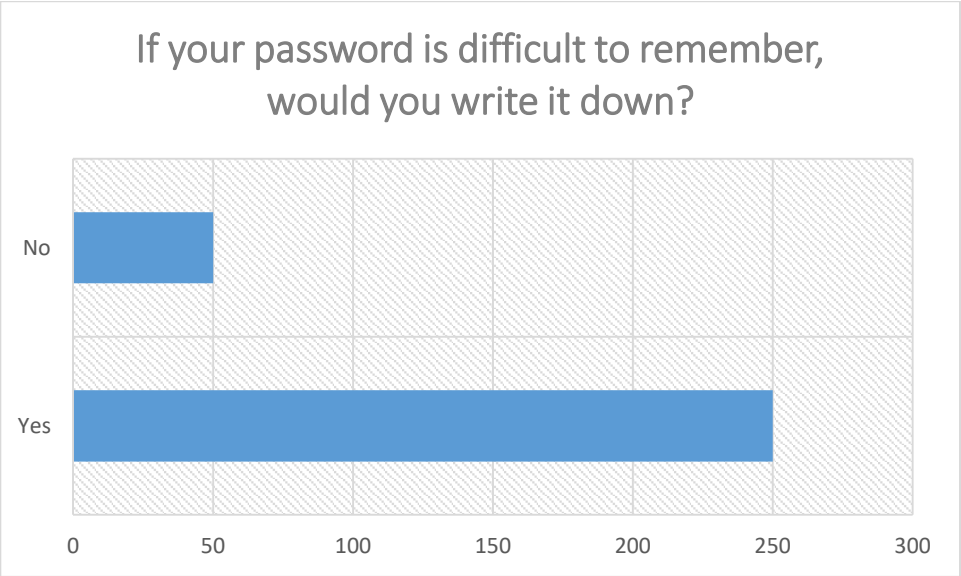

Figure 4.7: Writing down the password

Figure 4.7 is indicating that 250 of the participants do write down their password if they are difficult to remember, and 50 indicated that they do not write down their passwords.

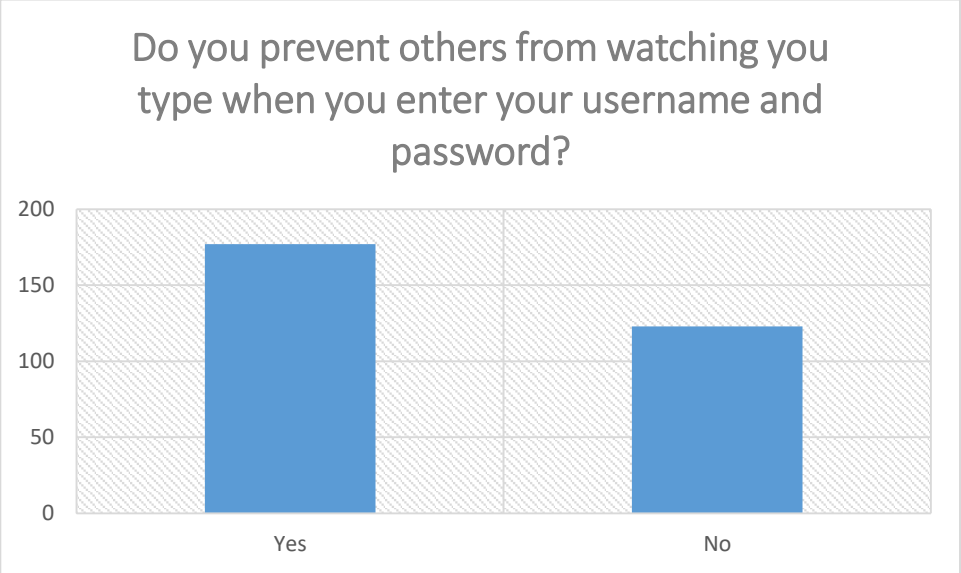

Figure 4.8: Preventing others from watching when tying the password

The Figure 4.8 indicates that 177 of the system users prevent others from watching them when they typing username & password, while 123 of the participants indicated that they do not prevent others when typing a password.

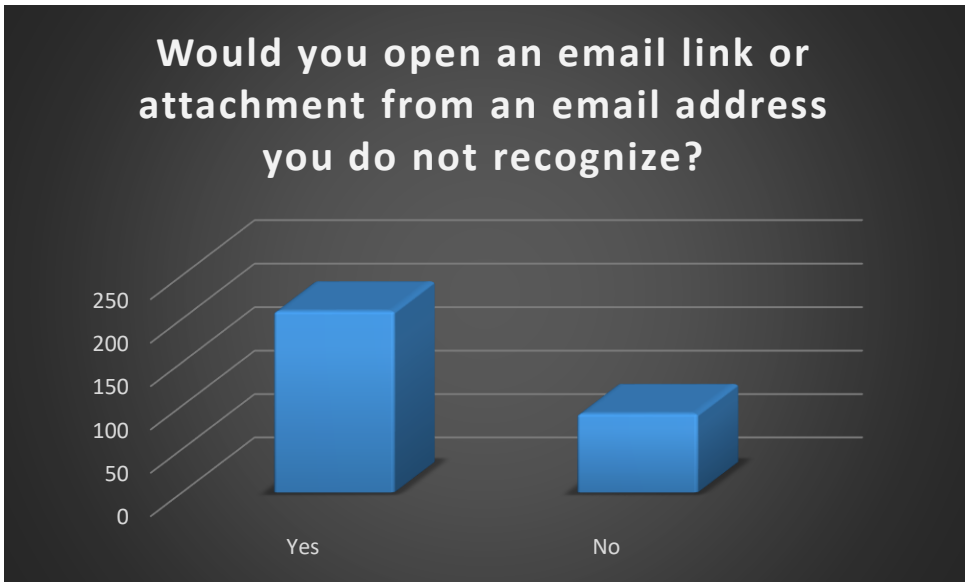

Figure 4.9: Opening an email link from or attachment from an unknown email

The Figure 4.9 indicates that 209 participants open email links or attachments from an address they don't recognise. While 91 participants indicated that they could open email from unrecognised address. This tendency of users can allow hackers to have access to their credentials and eventually access to sensitive information such as the salary of the employees or some file with sensitive information like student marks and salary information.

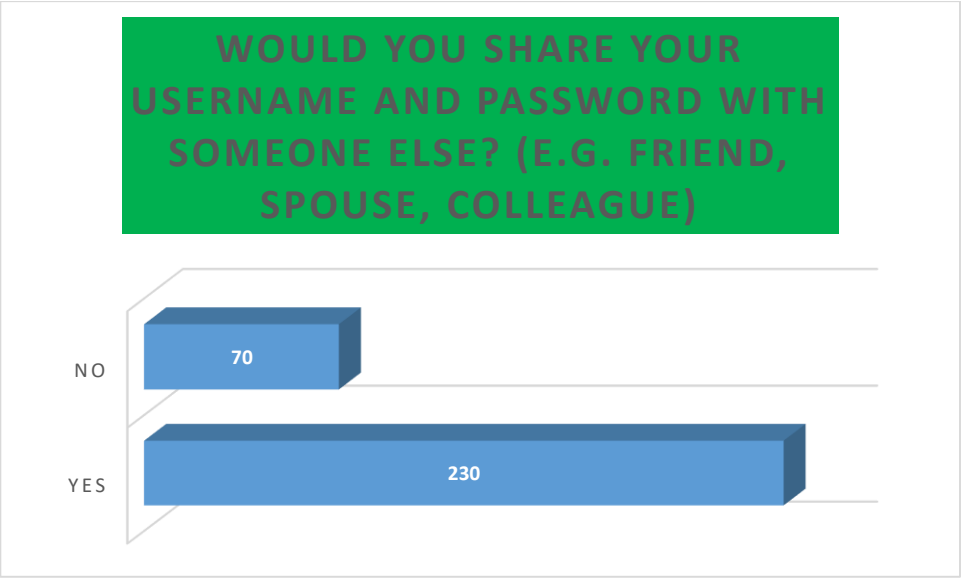

Figure 4.10: Sharing of password with someone (friend, spouse, and colleague)

Figure 4.10 shows that 230 of the participants share their passwords with either their colleagues, spouse or friends, while 70 of the participants indicated that they do not share their passwords with anybody.

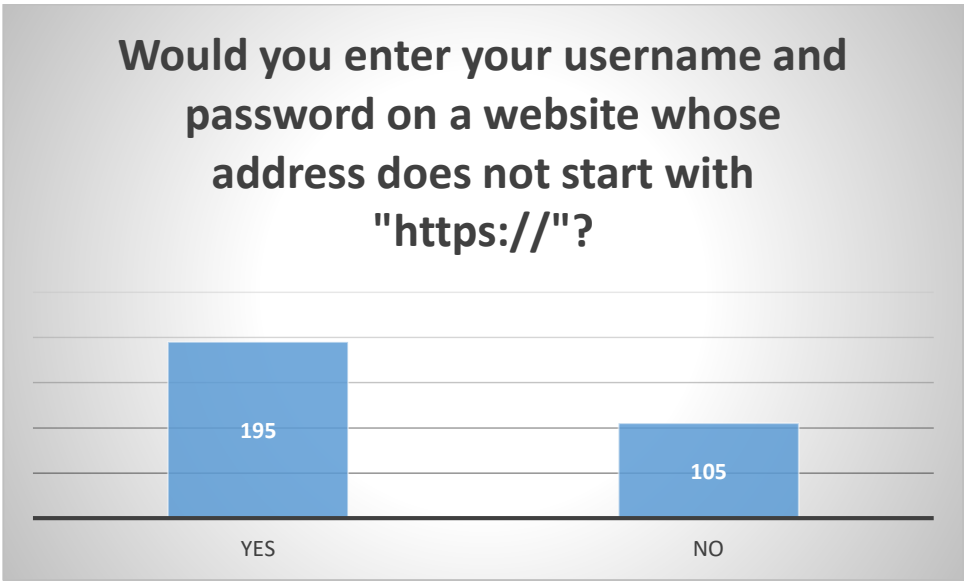

Figure 4.11: Entering username and password on a website whose address does not start with "https://

Figure 4.11 indicates that 195 of the UNAM system users enters their username and password on a website whose address does not begin with https._While 105 indicated that they do not enter their credentials on insecure address. The implication with this

attitude of UNAM staff members is that a third person can have access to their log in credentials.

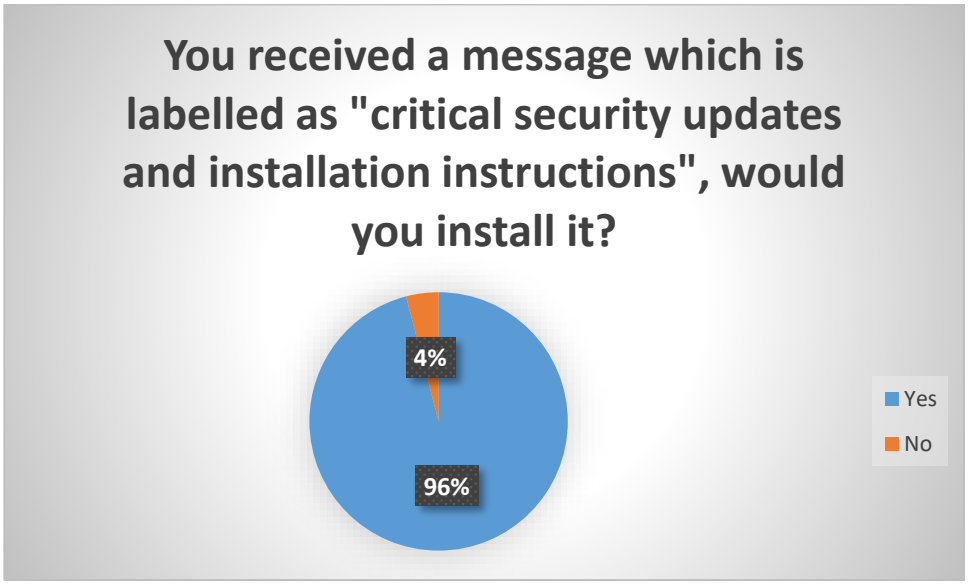

Figure 4.12: Installing Updates

The Figure 4.12 shows that 260 participants install updates and 11 indicated that they don't install updates.

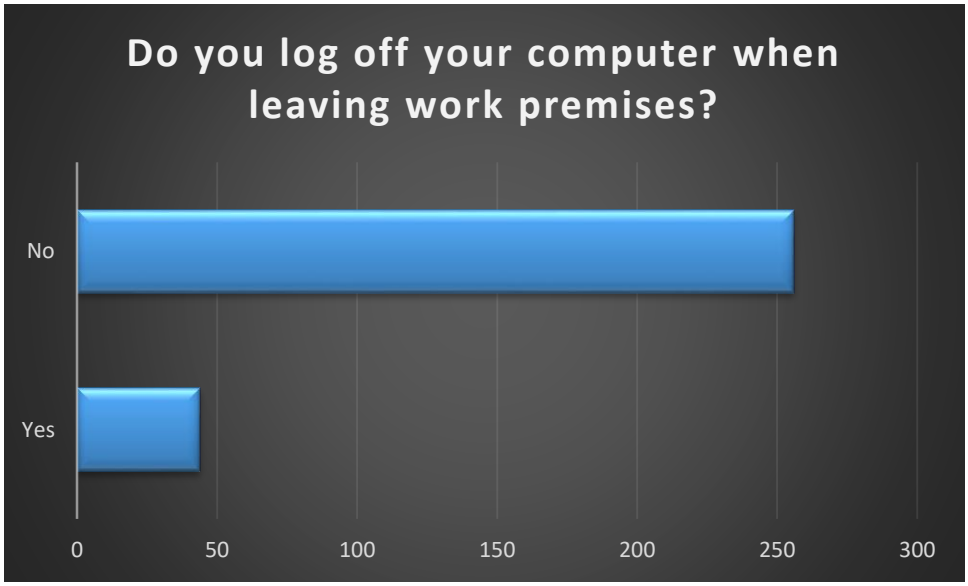

Figure 4.13: Logging off a computer when leaving work premises

Figure 4.13 indicates that 256 of UNAM employees who participated in the study do not log off their computers when leaving work premises and only 44 of the participants indicated that they log off their computer even when their work place.

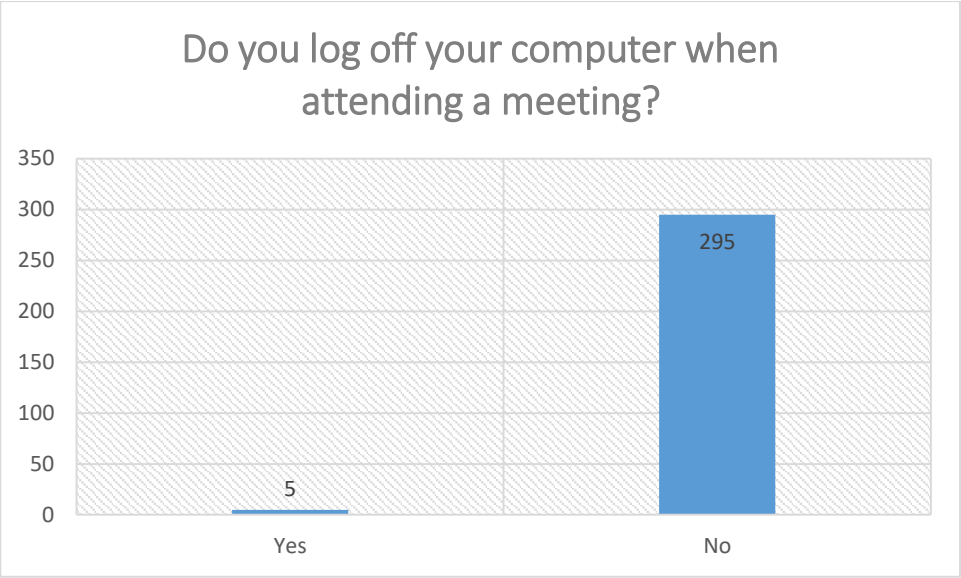

Figure 4.14: Logging off a computer when attending a meeting

Figure 4.14 indicates that 295 of UNAM employees who participated in the study do not log off their computers when attending a meeting and only 5 of the participants indicated that they log off their computer even when attending a meeting. One of the actions that can put information at risk is not logging off unattended computers. The negative repercussion of this attitude is that it can result into an unauthorised person having access to computers and the data and information contained in the computers can be exploited or exposed at the detriment of the main user.

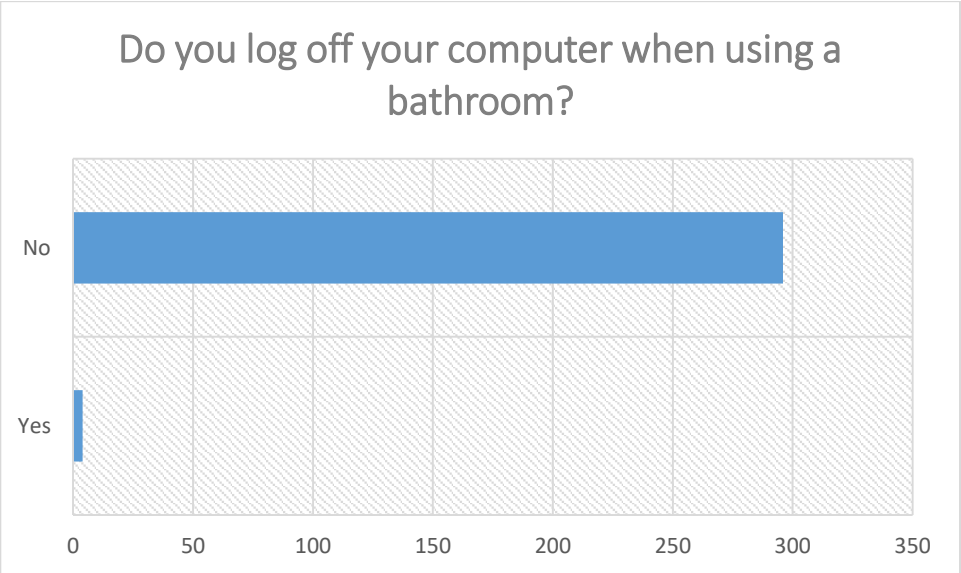

Figure 4.15: Logging off a computer when using a bathroom

Figure 4.15 indicates that 296 of UNAM employees who participated in the study do not log off their computers when visiting a bathroom and only 4 of the participants indicated that they log off their computer even when using a bathroom.

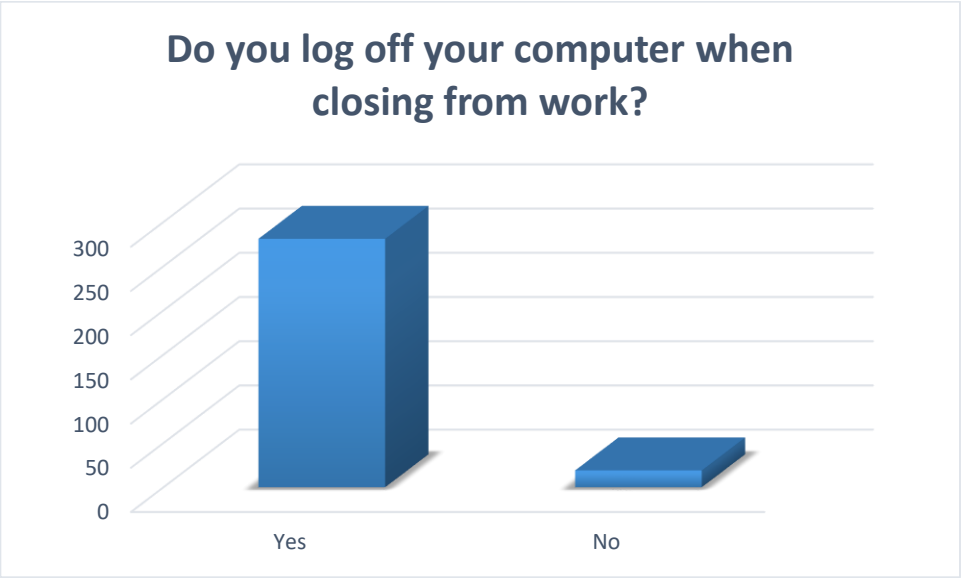

Figure 4.16: Logging off a computer when closing from work

Figure 4.16 indicates that 281 of UNAM employees who participated in the study do log off their computers when closing from work and 19 of the participants indicated that they do not log off their computer when closing from work.

4.3 Demographic details of each participant who took part in the in depth face to face interview .

Table 4.1: Demographic information of each participant

Participant	Gender	Educational level	Age
1	Male	Diploma	29
2	Female	Honours Degree	26
3	Male	Bachelor Degree	37
4	Female	Diploma	28

5	Male	Honours Degree	42
6	Male	Honour's Degree	45
7	Female	Bachelor's Degree	45
8	Female	Bachelor's Degree	29
9	Male	Honours Degree	49
10	Male	Honours Degree	30

This subdivision presents the demographic information of the participants to offer the reader a better understanding of the study participants as reflected in Table 4.1 above. The participants were UNAM employees from Computer Centre. Six of the participants were male, while four were female.

The table 4.1 shows that five (5) participants were employees from UNAM Computer Centre holding honour's degrees. Three (3) participants were bachelor's degree holders and two (2) diploma holders. These findings show that the study participants are fully qualified employees who are in a good position to proffer meaningful solutions to the issue under investigation.

4.4 Qualitative Analysis

This section presents the findings from the various themes that emerged from the study. Data presentation includes the description of the collected data into some form of explanation, understanding or elucidation of the people and situations under study. This involves turning and exhibiting the data from the interviews into findings that provide useful information, suggesting conclusions, and supporting decision-making (Marx & Gardner, 2010). Since the section was following a qualitative approach, the data was

analysed thematically and presented in themes and sub-themes that were aligned to answer the research questions of the study.

The data collected during the individual in-depth face to face interview was transcribed and then analysed according to the framework of data analysis for qualitative research (Blaikie, 2014). Thematic analysis is performed through the process of coding in six phases to create established, meaningful patterns (Braun & Clarke, 2017). The researcher's explanations and analysis are integrated with the literature, which serve as substantiation of the themes and sub-themes (Almalki, 2016). The themes were recognised and acknowledged through sequential phases which are data familiarization, data coding, searching for themes and theme development, reviewing themes, defining and naming themes and finally writing up the themes. The data was then presented in themes with transcribed quotations of the respondents being included to support the findings. The themes and sub-themes that emerged from the analysed, transcribed collected data are tabulated in Table 4.2

Table 4.2: Main Theme and sub-themes

MAIN THEME	SUB-THEMES
Existing IT security mechanisms and established policy in the University of Namibia	**Sub-theme 1.1**: Install and properly configure a firewall
	Sub-theme 1.2: Updating Software
	Sub-theme 1.3: Protection against malware
	Sub-theme 1.4: Implement a strong password policy
	Sub-theme 1.5: Implement Physical Security Measures to Protect Computer Assets
	Sub-theme 1.6: Connect Remote Users Securely
	Sub-theme 1.7: Lock down servers
	Sub-theme 1.8: Implement Identity Services (Intrusion Detection)

4.4.1 Sub-Theme 1.1: Install and Properly Configure a Firewall

Firewalls are systems which protect networks or network devices, such as institution PCs, control systems, cameras and routers from unauthorized access by preventing network traffic to or from these systems. Ten participants, representing 100% of the participants, indicated UNAM has firewalls installed. One (1) participant, indicated that they had firewalls which had not been properly configured because it blocks some useful sites, while 9 respondents indicated that UNAM had properly configured firewalls. The citations below from the participants supports and upholds these claims:

> *"UNAM have firewall installed and this really save the university from attacks by blocking traffic from untrusted sources and protects information from being disclosed to intruders"* (Participant 1) This was further supported by Participant 2 who sated that, *"The university network has firewall installed which filter out network traffic from unverified or suspicious sites or sources, UNAM firewall can even block useful sites and hence the installed firewall does not allow any traffic untrusted sites.* This issue was further strengthened by Participant 5 who said that, "*UNAM has properly configured firewall which filter out network traffic from suspicious sources. Firewalls had been a first line of defence in UNAM network security for over 25 years."*

In terms of the frequency of reconfiguration, participant 4 indicated, "*Our university firewall is usually reconfigured once a yea*r" This issue was further strengthened by participant 8 who said that, "*reconfigurations UNAM firewall is adhoc basis*"

These findings above support the findings of Microsoft (2014) who stated that firewalls are institution's first line of security and need to be installed regardless of the size and magnitude of an institution. The findings validate the earlier findings by Laudon & Laudon (2014) who indicated that as majority of institutions expose their networks to internet traffic, firewalls are becoming a requirement for every institution.

4.4.2 Sub-Theme 1.2: Updating Software

Updating software is an essential part of keeping a computer secure, and keeping all software up-to-date will protect a user or institution against the most common security exploits. If software's are not up to date, this could lead to unauthorised access computer systems which has the potential to expose sensitive information such as student marks, salary details of employees and so on. (Helkala & Bakås, 2014). The participants in the study indicated that their computers have recent software's which are regularly updated. The citations below from the participants supports this claim:

> *"UNAM computers have an up-to-date software and are updated 3 or more times a year this is securing UNAM computers from malicious software infections." (Participant 7).* This was further supported by Participant 9 who stated that *"Software update automatically depending on their requirements and this could safeguard computers from malwares"*

These findings concur with the findings of Wash et al., (2014) who indicated that, updating software is an essential part of keeping a computer secure, and keeping all software up to date could protect a system user against most common security exploits. If software is not up to date it gives a hacker carte blanche to exploit vulnerabilities

and infect the system, hence it is extraordinarily imperative to keep all software updated to prevent security incidents.

4.4.3 Sub-Theme 1.3: Protection Against Malware

Protection against malware attempts to identify, prevent and eliminate computer viruses and other malicious software. Ten participants, representing 100% of the research sample, indicated that they had antivirus software installed and the antivirus updates automatically as new updates occur. The citations below from the participants harmonises this claim:

> "*The University has antivirus software installed which updates automatically as new updates occur*" (participant 10). On this issue participant 9 had this to say, *"UNAM has Kaspersky antivirus installed from prevent computers from malwares*"

These findings are in agreement with the findings of Alkandary & Alhallaq (2016) who stated that an antivirus software should be installed on all computers to protect against security threats. Having anti-malware installed provides a multiplicity of security protection, as well as a monitoring of spams, viruses and spyware.

4.4.4 Sub-Theme 1.4: Implement A Strong Password Policy

Implementing a strong password policy important as it includes not only developing and enforcing the policy, but also educating employees about how they should be protecting their passwords. Thorough control of passwords is an easy and an effective first step in sustaining information security (Keller, et al., 2005). Ten IT professionals, representing 100% of the research sample, showed that they had a password policy in UNAM, such as non-repetition of a password, password expiration, prohibition of username as a password. Regarding the password length 1 of the respondents,

indicated that they had 6 or more-character password length while 9 IT professionals, indicated that their password ranged between 7 or more characters in length. In relation to the characters that constitute a password 10 of the respondents, representing 100% of the research sample, indicated that their password consisted of numbers, upper and lowercase, symbols and special characters. The citations below from the participants upholds these claims:

> *"UNAM has a password in place such as non-repetition of a password, which implies that a user cannot reuse the same password after it expires, the system always prompts for a never used password"* (Participant 1). This issue was further strengthened by participant 3 who indicated that, "*Our university has a password which expires after one month, which means we have password expiration as an additional measure to our password policy*" Participant 4 had this to say on the issue "*UNAM system prohibits the use of username as a password and the password length is 6 or more characters, all these are measures in the password policy*"

These findings harmonies with Sun et al (2011) who stated that implementing a strong password policy educates employees about how they should be protecting their passwords. A strong password should have more than 8 characters, at least one change of case, a number that is not at the end, and non-alphanumeric character such as & or * that is also not at the end of the password.

4.4.5 Sub-Theme 1.5: Implement Physical Security Measures to Protect Computer Assets

Physical security measures can be as simple as putting locks on doors and adopting a Disaster Recovery Plan (Sai, Gumbo, Mzikamwi, & Ruvinga, 2015).When a question

was presented to the IT professionals in order to investigate if they had implemented security measures to protect their computer assets, 10 IT professional said that they had implemented physical security measures to protect their computer assets. Laptops are locked to desks and physical access is highly restricted to staff members. The citations below from the participants endorses these claims:

"UNAM has physical security measures in place as our computers have locks and cable ties as a physical security measure to protect computers from theft as threat to information" (Participant 7). This was further supported by participant 5 who said that "*UNAM has disaster recovery plan, which means we can back up our data even if computers in the university are destroyed by disasters such as fire or theft"*

These findings concur with Sai (2015) who indicated that physical security measures could be simple as putting locks on doors and adopting a disaster recovery plan. Sensitive areas should have access point for identification of workers and could include safeguarding entrances and exits.

4.4.6 Sub-Theme 1.6: Connect Remote Users Securely

The remote access technology has advanced institutions output, catered for online information, simplified flexible work schedule, and enhanced business communication (Sai, Gumbo, Mzikamwi, & Ruvinga, 2015). Both public and private networks provide the means by which information can be accessed. All the participants (100%) indicated that they do have remote users and they connect to remote users securely using VPN communication which can never be intercepted. The citations below from the participants validates these claims:

"We have remote users and we connect to remote users securely using VPN communication which can never be intercepted" (participant 1) This was further supported by participant 2 who indicated that "UNAM *connects to its remote employees securely with the help of VPN, which contain encrypted data in its channel making it difficult for information to be compromised"*

These findings support the findings of Sai (2015) who stated that VPN technology had been the tool to achieve a secure communication between mobile employees who need to access the institution's network from a remote location. VPN channels is secure as it contains encrypted data. On this note, it is concluded that UNAM connects securely to remote users.

4.4.7 Sub-Theme 1.7: Lock Down Servers

Management of servers is very important in today's world of information security. Limiting what a server can do and what it can allow is an effective way to protect this vital network components. All 10 participants, representing 100% of the research sample, indicated that they had secured server rooms, as server rooms are locked and had biometric authentication. The citations below from the participants corroborates these claims:

"*Our server rooms have locks to prevent unauthorised access or entry*" (Participant 8). This issue was further validated by participant 9 who indicated that "*Our server rooms are always locked have authentication as a security to avoid unauthorised entry"*

These findings concur with Sai, et al (2016) who indicated that limiting exposure to servers is always a good idea. Scanning open ports and block ports that are not needed for operation also limit exposure of servers and reduce attacks.

4.4.8 Sub-Theme 1.8: Implement Identity Services (Intrusion Detection)

IDSs are crucial in network security because they detect network attacks in progress and assist in post-attack forensics, while audit trails and logs serve a similar function for individual systems (Alkandary & Alhallaq, 2016).When the questions were presented to the respondents in order to investigate if the institution had a properly configured intrusion detection system, all (100%) participant said that they had intrusion detection system which send alerts to admin in case of paranoid or suspicious activity. The citations below from the participants substantiates these claims:

> Regarding the configuration frequency, 9 participants said "*our IDS is configured once every year"* This was further strengthened by participant 10 narrated that, "*We have intrusion detection system which send alerts to administrator in case of suspicious activity".*

These findings harmonies with Alkandary & Alhallaq (2016), who indicated that, it is a good idea to use IDS along with access control because access control alone can fool controls.

4.5 Results from The Experiment

To validate the accuracy of the survey a phony phishing system was developed to test user's information security. Two of the survey variables were experimented and these were:

- Participants' tendency to install programs requested by an unknown person

- Participants' tendency to give away username and password

Details Collected During the Practical Experiment:

The phishing email was created and sent to targeted users using the social engineering tool kit and credential harvester method attack. The email which was used for attack is displayed below, the email looks legitimate and authentic.

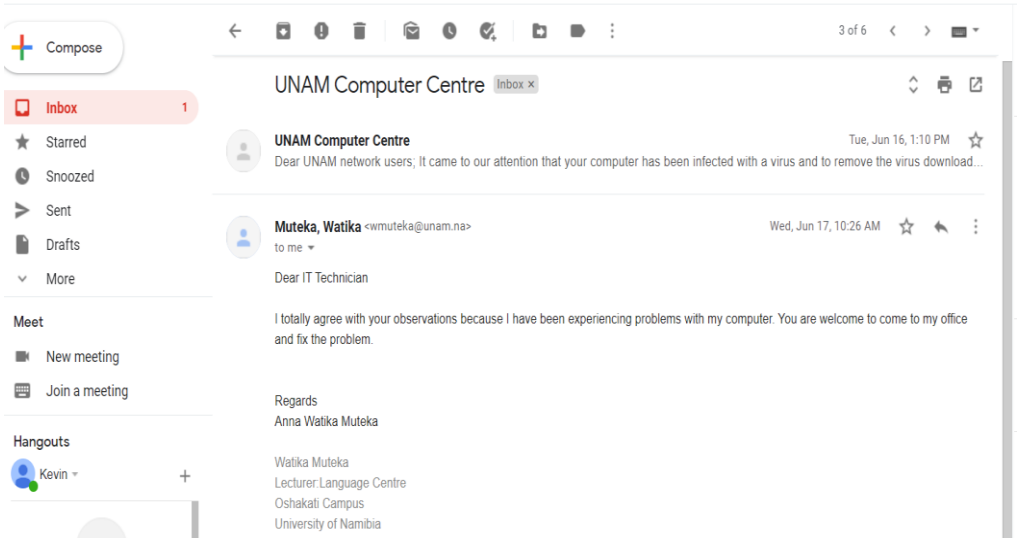

Figure 4.17 Phishing email used to attack the users

Figure 4.17 demonstrates that the user was tricked by the phishing e-mail send, and user even replied to the phishing email. In this case, an attacker can go further too even ask for other credentials and do whatever harm they indent to do.

Date/Time	IP Address	Country	User Agent	Referring URL	Host Name	ISP	More
2020-06-16 08:38:23	64.26.151.55	Canada, Ottawa	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:69.0) Gecko/20100101 Firefox/69.0	no referrer	64.26.151.55	ROGERS-COMMUNICATIONS	More Info
2020-06-16 08:55:17	197.188.33.40	Namibia, Oshakati	Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0	no referrer	197.188.33.40	TELECOM-NAMIBIA	More Info
2020-06-17 01:20:13	197.188.220.36	Namibia, Windhoek	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.97 Safari/537.36	no referrer	197.188.220.36	TELECOM-NAMIBIA	More Info
2020-06-17 01:28:49	197.188.220.36	Namibia, Windhoek	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.97 Safari/537.36	no referrer	197.188.220.36	TELECOM-NAMIBIA	More Info
2020-06-17 20:25:30	197.188.220.36	Namibia, Windhoek	Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko	no referrer	197.188.220.36	TELECOM-NAMIBIA	More Info
2020-06-26 05:24:54	64.26.151.55	Canada, Ottawa	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:69.0) Gecko/20100101 Firefox/69.0	no referrer	64.26.151.55	ROGERS-COMMUNICATIONS	More Info
2020-11-11 07:04:50	197.233.196.185	Namibia, Swakopmund	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36	no referrer	197.233.196.185	TELECOM-NAMIBIA	More Info
2020-11-11 07:15:17	197.233.196.185	Namibia, Swakopmund	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)	no referrer	197.233.196.185	TELECOM-NAMIBIA	More Info

Figure 4.18 The alerts listed in order of engagements

In this Figure 4.18, this is where we are checking if the user has clicked on the link attached to the email. The moment the user clicks on the link, the IP Logger will alert the attacker through the e-mail. The alerts are listed in order of engagements.

The Figure 4.19 shows the advanced log such as the IP address, location, Operating system used and who their ISP is

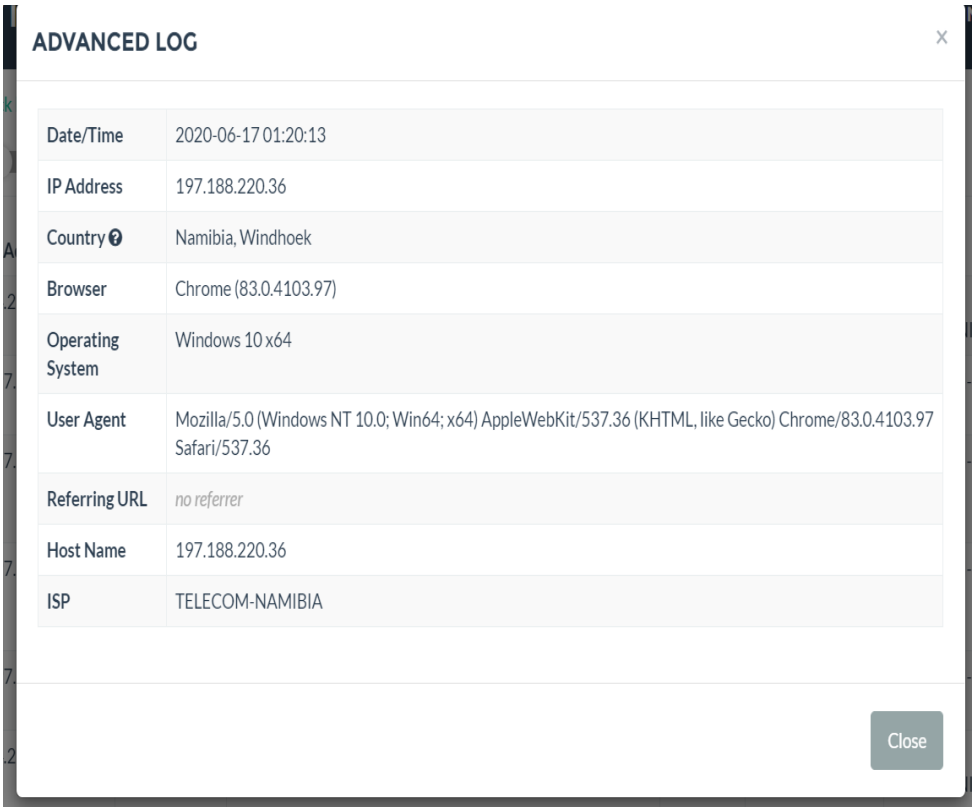

Figure 4.19 Advanced Log

In this Figure 4.19, this is where we are checking if the user has clicked on the link attached to the email. The moment the user clicks on the link, the IP Logger will alert us through the e-mail and here we are able to see some other information linked to the user such as the IP address, location, Operating system used and who is their ISP.

4.6 Counter Measures

The main objective of this study was to identify end-user errors that could lead to information security vulnerabilities and threats in UNAM and to assess the existing IT security mechanisms and policy at the University of Namibia.

In order to achieve this objective, a survey was conducted on users who frequently use information systems, and social engineering penetration testing was adopted, and it revealed a number of vulnerabilities (threats) as discussed in chapter 5. The protection of the network against attacks is unavoidable, however, attacks can be

mitigated. Suggested mitigating strategies to countermeasure vulnerabilities identified are outlined below:

4.6.1 Security Awareness

Security awareness and training are some of the most fruitful measures to mitigate the end user error (actions) threats to information security. The institution needs to provide basic security awareness training to all users of information systems within the institution to sensitise them on the key role they can play in ensuring that they are the first line of defence against any information disclosure or security breaches. Employees needs to be sensitised about phishing, spamming and anything that can contribute to security breaches. In this regard, any information security plan should include needs assessment that entails collecting information on the existing processes, the knowledge that is required of employees, and the flaws in the existing information security.

4.6.2 Endpoint Security

A number of information system in institutions is not centralised. Where there are no centralized systems, information is often shared among employees and replicated to different devices and a result of not having centralised data, most of the time employees bring in storage devices from other places without scanning them for viruses. Endpoint security is the concept that each device in an institution needs to be secured. It is recommended that sensitive information on portable devices like laptops and tablets should be encrypted. Moreover, removable storage such as DVD drives and USB ports could be blocked if they are considered to be a major threat path for malware infections or data leakage. To secure endpoints, a wide-ranging planning is needed, like applying policies that state that only certain computers like laptops can

connect to particular networks. Usage of wireless (Wi-Fi) access points should also be restricted.

4.6.3 A Strong Password should be Enforced or Implemented

It is suggested that functionality that rejects users from registering passwords that do not meet certain conditions should be used to ensure that only strong passwords are registered. A strong password should therefore have the following qualities:

- Be at least 12 characters in length
- Contain both upper and lowercase alphabetic characters (e.g., A-Z, a-z)
- Have at least one numerical character (e.g., 0-9)
- Have at least one special character (e.g., ~! @#$%^&*()_-+=)
- Employees should also:
  - Not share their password with anyone at the work place
  - Change their password regularly
  - Password should not be written down or stored in an insecure manner
  - Reusing of password should be avoided
  - Usage of the same password for multiple accounts should also be discouraged.
- The university should use "timeouts" for all PCs to ensure that users are automatically logged out or that PCs are locked, to minimize the risk of insider attacks.
- Institutions should include information security policies in their standard codes for conducting business. These policies need to be understood and implemented. Workers must realize that they play a critical role in sustaining the university security and are responsible and accountable for security

breaches. Quality and security assurance should not be sacrificed for anything. Every employee should:

- Refer to the company's code, mainly those relating to information security, on daily basis to conduct business.
- In every business transaction they make they must be conscientious about security be it in the office or at home.

4.6.4 Suggested Practices for Working with Portable and Smart Devices:

- Devices should be chosen carefully: All device have different security levels. For instance, iPads are built for general consumers and not as concerned by security and is therefore less innately secure than a BlackBerry device designed for business users.
- Turn on encryption: Once a device with stronger security controls has been chosen, the controls must be used.
- Require Authentication: it is essential that employees be required to turn authentication features on their devices so that lost devices cannot be easily broken into.
- Utilize Remote Wipe Capabilities: Employees should give IT administrators the capacity to remotely access and disable their devices in the event of loss or theft. This could be very handy in a situation where, say, an employee loses his or her device with sensitive data stored within.
- Third-Party Apps should be controlled: Smart devices are basically small computing devices that can accept any third-party applications and are therefore risky. It is recommended that unknown third-party applications should be limited to prevent people from seizing control of the devices.

- Set Unique Firewall Policies: people should set up unique firewall policies specifically for traffic coming from smart and portable devices. Smart device users don't necessarily need access to every bit of data on the network, so it makes sense to limit exposure by only offering access to the types of data they need.
- Disable Bluetooth when not in use: Bluetooth capabilities on smart devices which can make it possible to talk on a hands-free headset can also be target for hackers who can utilise its 'always-on, always discoverable' default settings to launch attacks. In order to limit exposure, it is recommended that users deactivate Bluetooth when it is not actively transmitting information

CHAPTER 5：RESULTS AND DISCUSSIONS

5.1 Introduction

The Discussion of the results of the study about the research objectives to answer research objectives by critical interpretation of the results obtained during the research is presented in this chapter. A model has been proposed aiming to address end user error issue as well as a recommended inclusive information security framework are discussed. The study firstly investigated whether there are recommended IT security mechanisms and policies in UNAM and the finding is discussed by 5.2

5.2 Objective (1): Information Security Mechanisms and ICT Policy in Practices at UNAM

The purpose of this study was to assess and identify the end user errors vulnerabilities that contribute to information insecurity within UNAM network. In order to determine that is users (humans) that contributes to information insecurity, the study discussed the security mechanisms implemented in UNAM. The study had discovered that the university had implemented all the recommended technical security mechanisms but user education and training on basic information security is ignored, for instance a training on how to identify phishing. Hence the study concluded that information breaches are happening because of users' actions but not necessarily because of technical issues. The following security mechanisms are in place in UNAM;

Establishment of an Acceptable ICT Policy

This policy serves as a guideline for compliance for all UNAM employees and students using its network (internet), e-mail systems, computers, and other ITS services such as Finance iEnabler, Personnel iEnabler, Lecturer iEnabler, and UNAM Portal.

Software patches and regular updates of system software and applications

When questions were presented to the participants in order to investigate if software updates were carried out and the frequency of the updates was posed, 10 participants, representing 100% of the research sample, indicated that they do carry out software updates. Responding to the frequency of updates question, 10 of the participants, indicated that software updates are carried out three or more times a year.

This finding is in agreement with the two researchers, Helkala and Bakås (2014) who claimed that a frequent update of software, particularly those that safeguard against malware is very indispensable as it helps to record the names of the up-to-date and leading threats.

Malware Protection

Protection against malware is also instrumental in protecting corporate information. This is accomplished through the installation and configuration of anti-malware programs. The educational institution should have mechanisms that protect the IS from malware. The common mechanism to protect the university network from malware is anti-virus software. Anti-virus software is an application that safeguards a computer from malicious software called a computer virus. It is recommended that all computers inside the university network should have an anti-virus installed to minimize the chances of attacks and security threats on the network (Helkala & Bakås, 2014). Therefore, this study found out that the University of Namibia has recommended anti-malware be installed in all computers stationed in laboratories and offices. Even though these newer technologies are being gradually adopted, the user's name and password authentication method remain the most widely used procedure for protecting information (Keller, et al., 2005).

Implementing a strong password policy is not all about formulating and enforcing the policy, but it also entails educating system end-users on how to treat and protect the passwords. Educational institutions should train employees on password protection dos and don'ts, such as not writing down the password or using the same password for both work and social media because these are things that users do (San et al., 2011). According to San et al. (2011), the level of protection offered by passwords is directly related to their complexity. A strong password is defined as a series of more than ten characters, at least one change of case, a number in the middle, and a non-alphanumeric character such as hash (#) or ampersand (&) that does not appear at the end of the password (Helkala & Bakås, 2014). At UNAM, the application of a strong password policy is embraced. The technical team continuously encourages by introducing measures such as the expiration of a password after a month, a password with non-alphanumeric, and no repetition of a password.

Physical Access Control

Putting a physical security mechanism to protect computer resources from theft and damage is done in the basic form of locks on doors of computer laboratories and offices (Sai et al., 2016). Another ideal strategy towards implementing enhanced physical security is to record all IT equipment's serial numbers for identification purposes and minimize access to computer laboratories and equipment, for instance, servers and switches (CSB, 2018).

The institution could also secure the computers physically by using cable ties to tie all cables together and lock them. This protects the computer from physical theft because a computer cannot be easily taken away as opposed to when cables are not secured with cable ties. All laptops should have locks to secure them on the desk when users are leaving

them unattended. Areas with sensitive equipment such as routers, servers, and switches should have access points for employee identification and could embrace safeguarding entrances and exits. The backup storage area should be protected as part of the Disaster Recovery Plan. Information such as the network infrastructure model, indicating the network set up and the devices that protect it should be kept confidential because information of that nature in the hands of an attacker is equivalent to a route map to the front door. This study discovered that the University of Namibia has physical security in place, such as security officers at the entrance of the computer labs, cable ties, and locks for computers' physical security.

Cybersecurity Training and Awareness

On the other hand, training university employees on cybersecurity attacks have become a priority of the computer centre team. Ignoring this exercise has a large potentiality to contribute to the attacks of the University Information System because employees interact with IS every day to carry out the university day to day operations; hence it is a sensible idea for an educational institution to adopt employee security awareness and training to mitigate the chances of attacks on the university network (CSB, 2018). However, statistically, employee training and security awareness are the lowest on the list of top priorities of the information security budget at 16 and 13 percent, respectively. The existing UNAM policy regarding information security was analysed to determine what is missing or lacking in the current information security.

Identifying and Authenticating Users

Students and staff members are identified facial and authenticated on the synchronized ITS system. In this case, they are required to present what they know, such as their username and passwords.

Secure Remote Access

The remote access technology has advanced corporate productivity, provided online information, facilitated a flexible work schedule, and improved business communication (CSB, 2018). Both public and private networks provide a channel through which the information can be accessed. Educational institutions have workers who are not fixed at one university campus and need access to the university intranet from a remote site, such as home, hotel, or guesthouse (Sai et al., 2015). Hence, virtual private network (VPN) technology virtual private network (VPN) technology is used to safely connect isolated users to the firm's network. VPN technology is the method that an educational institution should adopt to secure the communication channels between the distant employee and the university network. VPNs allow users to authenticate data from end to end and prevent unauthorized access to the university intranet (Helkala & Bakås, 2014).

Hardware Security

Handling of computers that provides service to other computers such as servers is a critical issue nowadays. Controlling what a server can permit and what a server can do is very crucial to information system security. Limiting access to the server is a brilliant idea, just to tighten security. Some network ports that are not necessary for operations could be blocked to ensure limited access to the server. Servers can control personal computer (PC) operations and inhibit users without administrative privileges from downloading unauthorized programs. This is a common mechanism used by institutions to mitigate vulnerability to viruses that attach themselves to programs [12]. For this study, the mechanism of locking down servers was investigated in UNAM.

It has been determined that severs and lab computers with Linux and Windows systems were given vulnerability protection utilizing a firewall to prevent access from hostile IP addresses. A firewall can be software or hardware that aids to filter out available attackers and malware that attempt to invade the devices over the Internet. Firewalls are the institution's first line of security and need to be installed regardless of the magnitude of the institution (Microsoft, 2014). As most institutions expose their networks to Internet traffic, firewalls are becoming a requirement (Sai et al., 2015). Intruders in everyday life are undoubtedly probing institutions with a constant Internet connection. Firewalls defend the university network from unauthorized access by filtering out packets from untrusted networks; it is imperative to take cognizance that firewalls cannot safeguard against attacks that pass via authentic communication routes. It is recommended for the university to have hardware and software firewalls installed so that the software firewall could serve as an alternative to back to the hardware firewall. However, it can only operate on the machine on which it is installed; hence the software firewall needs to be installed on all devices to provide a good backup for the hardware firewall (Microsoft, 2014). The results from this study indicated that UNAM appropriate and well-configured firewall; however, the results also revealed that the firewall could inadvertently block access to some useful sites.

Intrusion Detection and Prevention

Intrusion Detection System (IDS) also used as anomaly-defence systems which detect network intrusion, threats (i.e., data breach, misuse of information systems or manipulation of information and corruption of data), and attacks (i.e., unauthorized access, identity theft, denial of service, and man in the middle attack) in the institution systems and also to help to trace information about the attacker afterward. The audit trails and logs file logs information regarding attacks for specific IS (Sai et al., 2015).

Usually, an intrusion detection device is network equipment located on a reflected network switch port and reviews network traffic between switches to identify any possible presence of wicked bit patterns. It uses statistical anomaly or pattern matching detection. These systems can also be host-based. It is a virtuous idea to use intrusion detection systems along with access control because access controls alone cannot fully control unauthorized access to the institution network (Sai et al., 2015).

Encryption

To encrypt content in transit via the Unam website, the institution has a secure certificate that uses communication such as protocols Secure Sockets Layer (SSL) and Transport Layer Security (TLS).

5.3 Objective (2): End-Users Errors That Could Lead to Information Security Vulnerabilities and Threat

The end-user errors that emerged during the survey, interview and social engineering experiment on threats that could leads to information security vulnerabilities include acts performed without intent or malicious purpose by an authorised user. The interaction of users with information systems, sometimes could results in some harmful actions could leads to information security vulnerabilities. These harmful user actions were identified and they are listed and discussed below:

I. Following Links from Unverified Senders

The study indicated that a big portion of the participants (77.7%) followed a link that requested them to change their credentials while 22.3% of the UNAM staff members who participated in the study followed a link that requested them to download updates. This is amazing to discover that majority of the respondents (195) said they would enter their login details on a website whose address does not start with “https”. This

tendency of system users can give hacker and social engineer a leeway to steal sensitive information.

Phishing and social engineering are one of the most common ways to stealing confidential information from educational institution such as UNAM. These attacks are a growing threat because attackers' primary motivation is stealing sensitive data such as employee's salary or financial information or extracting trade secrets. Moreover, by attacking the right people, attackers can gain a grip in the university network, then use it to exploit sensitive information. Phishing and social engineering attacks are more challenging to manage since they depend on human behaviour and involve taking advantage of vulnerable people. Educational institutions and individuals today must adopt a combination of technology solutions and user awareness to help protect sensitive information.

The findings above confirms the findings of Van-Zedlhoff (2016) that clicking on links from unconfirmed sources can lead to security breaches. This is one of the techniques phishing attackers and social engineers employ to persuade victims to give them the information that they want and hence clicking on links from unverified sender should be avoided at all cost.

ii. Deficiency of strong password and inappropriate password

The study discovered that majority of the participants engage in practices that could compromise their passwords. The study further established that 55.3 % of the participants change their passwords only when the system requires them to do so and 44 % indicated that they change their password after 3 months.

On password strength, the study indicated that 72.3 % of the participants use up to 7 characters to generate their password. And 8.3 % said their passwords are as short as

the system allows. Furthermore, 74 % of the participants indicated that they use personal information such as name, date of birth, place of birth, address, etc. to generate their password while 11 % use only upper letters. Moreover, 83.3 % of participants indicated that they do write their password down when it is difficult to remember.

The study discovered that UNAM staff members are indulging themselves in practices that could compromise their passwords such as, the usage of a weak password, writing down and sharing of passwords with others, and reusing the same password on different systems are some of the bad practices that could put data to risks. Passwords are to protect data from access from unauthorised individuals both internally (other employees) and externally (hackers). If the password is compromised, the security of the system is at stake.

The findings above supports the findings of Neely (2017), who cited that using a weak password, writing down and sharing of passwords with others, and reusing the same password on different systems are some of the bad practices that has the potential to put information at risks. Therefore, users must create strong passwords and log out properly on any system they are interacting with.

iii. Reckless handling of computers

The study indicated that majority of the participants 85.3% do leave their computers idle when leaving the work premises. Furthermore, majority of the participants (98.3%) do leave their computers unattended to when attending meetings and 98.7% do not log off their computers when visiting the washroom. These actions put data at risk especially the risks of insider attacks associated with employees leaving their PCs unattended with active sessions running. A substantial number of unauthorised access

events may occur when someone sits down at another user's computer. Threats to unattended computers can be in forms like illegal access to employee's data like salary information; unlawful access to sensitive business information to the level of changing that information. This could be in a form of camouflaging up a fraud or increasing bonuses or commissions by changing sales numbers. Another threat is the tendency to circumvent approval processes and access levels by accessing a superior's computer. Institutions are protecting their systems and workers against physical security threats, but ignoring the very real threat that exists from something as basic as an unattended PC. Sending emails in another person's name could have huge consequences. A simple thing like that could lead to security breach like access to customer information. This threat can be avoided if employees are educated to log out or lock their devices when they leave their desks. Moreover, a session timeout could limit the risk to unattended computers. Computers which had been left idle and unattended to can pose a threat to data as do other threats. This gives room to unauthorised accesses which can facilitate access to sensitive data and email messages.

These findings concur with the earlier findings by Evans et al (2016) who indicated that computers that are left idle and unattended to may pose a threat to information. This tendency of leaving computers unattended to gives an opportunity to unauthorised accesses that can facilitate access to sensitive information and email messages. Evans et al (2016) futher stated threats to unattended computers can be in ways like illegal access to employee's information like salary information, illegitimate access to sensitive institution information such as student marks to the extent of altering that information. This could be in a form of covering up a fraud or increasing bonuses or commissions by changing sales numbers. Hence employees should not leave their computers unattended this could put information at risk of being exposed and altered.

Iv. Linking to Networks Outside the University Infrastructure

The study indicated that some employees connect to the outside networks. Connecting to a private or a public network other than the university network infrastructure can pose a serious threat to data when the device used to connect is compromised. A device which has been compromised could be used as a gate way to an institution infrastructure. Employees who connect their mobile devices to the home network could expose their devices to attacks, as the devices are outside the perimeter of the more secured university network. Four of the IT personnel interviewed indicated that attackers could launch a silent attack against any device connected outside a university network when it is inactive pending the device to connect back to the corporate network.

The findings above supports and upholds the findings by Kearney (2010) who indicated that connecting to a private or a public network other than the institution network infrastructure has the potential to impose a severe threat to information when the device used to connect is compromised. According to National Security Agency (2015), a device that has been compromised could be used as a gateway to an institution's network infrastructure and this could allow the attacker to gain access to the network from the inside because the network will consider the devices as trusted ones as they are already used within the institution network.

v. Deficiency of Well Formulated Personal Security Policy

The lack of consistence in privacy settings gives attackers room to operate. End users are strict on security on one network but are inconsiderate on what information they post online. Two of the IT professionals interviewed indicated that on this attitude, especially the behaviours of system administrators. Hackers can gather this

information and use it to plan their victims, with the most popular source for such search being the Internet, especially the social networks.

The study discovered that email is one of the routes attackers use to access a network since breaking the security perimeter is easy nowadays. When users use the institution network to send and receive emails, they are putting the network and information in jeopardy. As employees connect to both the private (corporate) and public (internet) networks, their computers are often less secure and the fact that they run unauthorized applications like emails and outdated software on their computers makes them the perfect targets, allowing the attacker to access their computers and the entire institution network at large.

The study further discovered that some UNAM staff members are irresponsible when using the institution's computers. They often leave their computers unattended and without proper password. All these behaviours make data and information vulnerable to attacks.

The findings above substantiate with the findings of Gyunka & Christiana (2017) who indicated that the lack of consistence in privacy settings gives attackers room to operate and phish information to attack the network. End users are established to be strict on security on one network but are careless on what information they post online and social media. Personal and professional networks where the employees liberally and frequently update their status can offer a large piece of information for attacks. Therefore, employees need to vigilant of what they post online and social media.

vi. Illegal Application Use

Unauthorised applications used by users in the university network can compromise security of the network. The unauthorised applications are mostly downloaded from

malicious websites. Employees abuse the opportunity given to them for internet access by downloading from untrusted sites which jeopardise security of information. The study found out that malicious programs could be spread over university network when files are downloaded from unknown and untrusted web sites. This could cause serious security breach. University and employee's personal information can be at risk when unofficial applications are used on institution network. The study had discovered that frequently used unauthorised applications are email and social networks such as Facebook or Twitter. Employees could lose sensitive data through negligence and hackers could steal data through these applications.

These findings concur with the findings of Gyunka & Christiana (2017) which indicated that unauthorised applications used by users in corporate networks can compromise security of these networks. Hacker steals sensitive information that process of using and installing unauthorised applications.

vii. Distant Worker Security

One of the dangerous ways of exposing data to attacks is by sending them to home. This activity can turn all of the security measures in an institution into a completely useless process. Employees have the tendency to move a non-finished work to their devices and personal computers at home so that they could work on it later at home. This is quite risky because often personal computers and devices are less secured compared to the corporate ones. While business operations become more and more dispersed and online, mobile workers increase the potential threat for data. The study shown that improper handling of data such as moving files from an office device to a home computer that does not have proper IT security measures attracts information theft. These findings concur with the findings of Hadlington (2017) who indicated that one of the hazardous behaviours of exposing information to attacks is sending them to

home with an employee. This tendency can turn all of the security measures in an institution into a useless process and could put information at risk of theft and other treats

viii. Threats from Within the Institution

The study established that when employees are unhappy with their jobs, angry with their boss, or sentimental for any reason, they could become insider threats who can purposely damage or leak information. Therefore, users could expose information deliberately in order to hurt the institution because some reason as stated above. The findings above correspond with the findings of Hadlington (2017) who indicated that sometimes the problem is not that users ignore security threat but the users are the threats themselves they have the potential to deliberately expose information

5.4 Objective (4): Design an Information System Security Vulnerability Conceptual Framework and Model Based on End-User Errors, As a Counter Measure to the End-User Errors Towards IS.

One of the objectives of this study was to design and propose a model to better comprehend the end user errors as a connection between attacker and technological components of an information system. Furthermore, it intended to propose an inclusive conceptual framework for information security management in tertiary institutions. In response to objective 4, this subheading presents a proposed end user error model as well as a conceptual framework for information security which includes end user errors management.

5.4.1 A Proposed Information System Security Vulnerability Conceptual Framework

The figure 5.1 below presents a proposed conceptual framework that can be considered in any institution of higher education as it is deemed effective at ensuring information

security requirements. The proposed conceptual framework aims to bridge the conceptual divide between information security technical countermeasures and soft countermeasures such as human errors. This gap can be closed by analysing end-user errors for possible causing security breaches and by studying conflicting attitudes of employees on security in the organization. Study results demonstrated that the divide could be bridged by effective communication, training, and education.

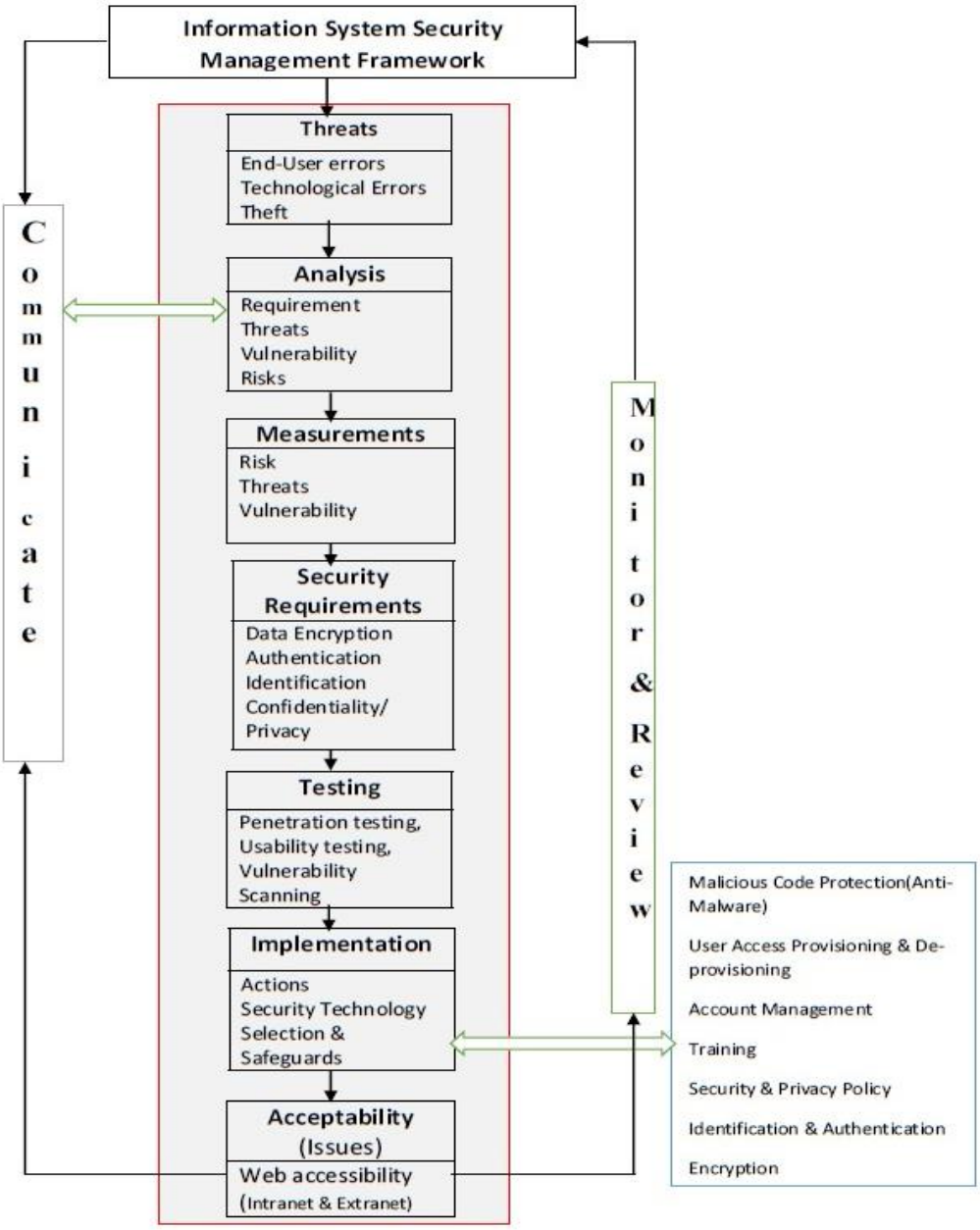

Figure 5.1 Conceptual Framework for Managing Information System Security in Institutions of Higher Education (IHE)

The conceptual framework in Figure 5.1 is intended to help universities meet obligation needed compliance with the data protection act, reassure security and reduce fraudulent use of personal and confidential data stored on the systems. Also, it can help staff members to acquaint themselves with knowledge on different type of threats (human-caused, technical and environmental threats) and be able to effectively implement preventive measures in their operating environment. This framework consists of controls for people (system end users), application, and systems. The study discovered that UNAM has technical solutions to defend its information from attacks and exposure, however users training and education on basic information security is ignored.

5.4.2 Proposed End User Error Model

The proposed model might help shape or improve policies towards protecting sensitive information and the systems in general. The proposed model was designed based on Human Oriented Criteria and not technological criteria. Irrespective of the technical measures put in place, information systems can be vulnerable to attacks if systems users are not incorporated in the security framework, hence the proposed model is deemed necessary to improve policies towards information protection. The proposed model, represented in Figure 5.2 could be used to mitigate end user error related information system vulnerabilities in tertiary institutions.

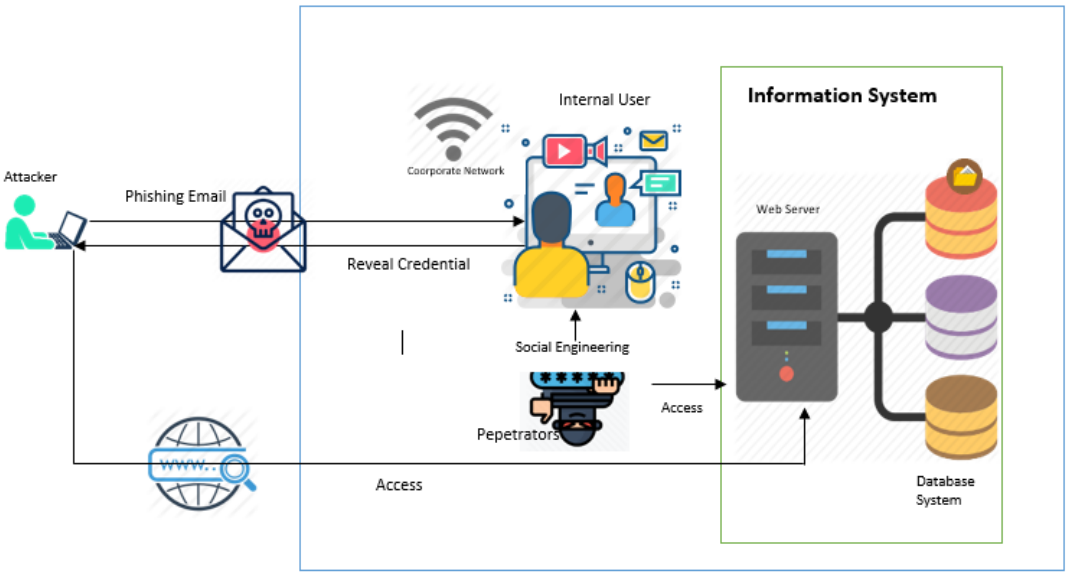

Figure 5.2 The proposed end user error model of security vulnerabilities

The proposed model in Figure 5.2 shows the system users including their interaction with computers could be one of the major loopholes in information systems security. Social engineer (hacker) from external network sending emails to deceive a user inside the university network, a user responds (human error) to emails and act on them. The attacker could capture the credentials of a user and details of the computer the user is using. This may result in the loophole or breaches in the network. IS can being vulnerable to attack even if the best technical security measures such as firewall, IDS and antivirus are in place. The reason is that information security is not limited to technological aspect but must include the system users. Institutions must therefore include system users when designing policies for information security. Confidentiality, Integrity, and Availability (CIA) is compromised when users who interact with the system are not adhering to the security policies. By chance sensitive information can be accessed by intruders because of errors that users could commit and this information can be exposed to unauthorised access, this information could be

altered or made unavailable and as a result the CIA triad model of information security is compromised.

The study discovered that UNAM has technical solutions to defend its information from attacks and exposure, however users trading and education on basic information security is ignored. This is a clear manifestation that the attacks the university is experiencing is coming as a result of user's bevors that are dangerous to information security. Therefore, users need to be trained on what to do and on what not to do within the university settings.

The proposed model end user errors model might help shape or improve the existing security framework which only emphasised on the technical aspect of security. The following suggested conceptual framework in Figure 5.2 resulted from the end user model proposed. This conceptual framework could be helpful to mitigate all security vulnerabilities including end user errors (actions) vulnerabilities.

CHAPTER 6：CONCLUSION AND RECOMMENDATION

6.1 Introduction

This chapter presents the conclusions and recommendations drawn from the findings of the study. The section also provided recommendations on how to reduce some of the shortcomings discovered during the study. Finally, it served as a guide for further research directions that could be explored in the near future.

6.2 Recommendations

Based on the findings of the study, the following prevention measures are recommended to the university. Although human-caused threats are unpredictable, they could be generally eliminated through effective end-user training as is widely believed that the first step in systems protection is knowing the threats. Hence, education is the key to avoid security threats emanating from system end-users. Since, end users' errors can be accidental or intentional, in case it happens all levels of the university network must remain protected in order to ensure the best security for the institution. Also, when selling or donating computers or disposing hardware particularly the hard drives, it must be properly sanitized, wiped or completely destroyed as data be recovered from old devices by experts although seems deleted. In addition, to protect the resources of the university, physical access control must be taken into account. This require a maximum restriction access to areas in which sensitive data are stored by controlling entry and creating physical barrier such as locking data centre or server rooms, using tracking devices on movable devices, RFID badge and/or using biometric systems with Iris and retinal recognition rather than the

ordinary fingerprint scanning that can be copied. This measure ensures that laptops and other portable devices and hardware are not stolen by an insider and outsiders and deter unauthorized access to data by anybody including hackers who may otherwise exploit the information system.

Lastly, it was also further recommended the adoption of the proposed security framework as discussed in chapter 5 (*see* Figure 5.1). The university could outsource IT expertise for the development of strong IT policy. The institution should formalize security awareness and training include professional IS security tutors/trainers.

6.3 Future Research

The experimental work done in this study and its findings served as the starting point of future work. It was evident that this study was very limited in terms of accessibility, tools and infrastructure. However, it has reached its objectives.

The future direction of this study is to consider the application of other penetration tests such as brute force attack, SQL injection and integrate them with social engineering test to test the protection of data at the University of Namibia.

6.4 Conclusions

The study concluded that even though technology indispensable in the information security structure, technology alone is insufficient to safeguard the university's IS from data breaches. The study also discovered that the university had implemented all the recommended technical security mechanisms but user education and training on basic information security is ignored, for instance a training on how to identify phishing emails and spams. Hence the study concluded that information breaches are happening because of users' actions but not necessarily because of technical issues. End-users need to be incorporated into an information security model to make the security framework complete. It is not a sensible idea to think that the role of people is to run

applications only but people must be considered in terms of IS security of an Institution. System end-users can either be the weakest or the strongest aspect in the security framework and therefore should alleviate the deficiencies in the prevailing security technology. For that reason, the study concluded that there is a need for an Institution to integrate IT and human as a security to defend the university IS under a true information security management system.

Therefore, information security is not about a technical or technological problem; rather, people and universities need to comprehend system end-user errors, which need plentiful consideration in order to accomplish an effective information security management system practice in the university setting.

Refining security using technical means is important for an institution conducting business online as well as for institutions that are at the same time seeking to realize their missions and objectives. However, implementing technical measures alone does not guarantee a more secure environment. All kinds of end user errors could adversely affect the management of security in personal and institution settings. Thus, security is not solely a technical or technological problem; rather, people and institutions need to understand system end user errors, which need abundant considerations in order to accomplish an effective information security management system practice.

.

7. REFERENCES

Goel, J. N., & Mehtre, B. M. (2015). Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology. *Procedia Computer Science*, 57, 710–715.

Akaranga, S., & Makau, B. (2016). Ethical Considerations and their Applications to Research: a Case of the University of Nairobi. *Journal of Educational Policy and Entrepreneurial Research, 3*(12), 6.

Ali, S., & Heriyanto, T. (2011). *BackTrack 4: Assuring Security by Penetration Testing.* Packt Publishing.

Alkandary, Y. H., & Alhallaq, F. M. (2016). Computer Security. *International Journal of Advanced Research in Computer and Communication Engineering, 5*(1), 1-6.

Almalki, S. (2016). Integrating Quantitative and Qualitative Data in Mixed Methods Research—Challenges and Benefits. *Journal of Education and Learning, 5*(3), 290-291.

Antwi, S., & Hamza, K. (2015). Qualitative and quantitative research paradigms in business research: A philosophical reflection. *European Journal of Business and Management, 7*(3), 217-225.

Avedian, A. (2014). Survey Design. Harvard: Harvard School of Computing.

Baloch, R. (2017). *Ethical Hacking and Penetration Testing Guide.* . UK: In Ethical Hacking and Penetration Testing Guide.

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

Banu, M. E. (2013). A Comprehensive Study of Phishing Attacks. *International Journal of Computer Science and Information Technologies (IJCSIT), 4*, 783-786.

Bhingardeve, N., & Franklin, S. (2018). A Comparison Study of Open Source Penetration Testing Tools. *International Journal of Trend in Scientific Research and Development, 2*(4), 2595–2597.

Blaikie, N. (2014). *Designing Social Research* (6 ed.). Librazel: Policy Press.

Braun, V., & Clarke, V. (2017). Thematic analysis: Providing accessible guidance on doing and understanding. *The Journal of Positive Psychology*, *12*(3), 1-2.

Brian, B. M., & Salvatore, S. (2014). *Measuring human factor of cybersecurity.* Columbia: Columbia University

Bureau, S. (2018). Human-centered cybersecurity: A new approach to securing networks. *Research at RIT*, 2017-2018.

cresswell, J. (2012). *Mixed methods research designs.* Margburg, University of Nebraska Lincoln, Germany: CAQD Workshop.

Creswell, J. (2014). *Research design: Qualitative, quantitative and mixed methods.* Cape Town: Capte Town press.

CSB. (2018). *Cyber Security Breaches Survey.* UK: Social Research Institute.

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behavior as an aspect of cybersecurity assurance. *Security and Communication Networks, 9*(17), 4667-4679.

Goel, J. N., & Mehtre, B. M. (2015). Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology. *Procedia Computer Science, 57*, 710–715.

Gyunka, B. A., & Christiana, A. O. (2017). Analysis of human factors in cyber security:A case study of anonymous attack on Hbgary. *Computing & Information Systems, 21*(2), 10-18.

Hadlington, L. (2017). *Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours* (Vol. 3). London: Heliyon.

Hadlington, L. (2018). The human factor in cybersecurity: Exploring the accidental insider. *In Psychological and Behavioral Examinations in Cyber Security*, 46–63.

Hasani, S., & Dode, A. (2016). Assessment of an IT network security with information gathering tools. *Problems and Challenges of Transformation of the Society towards Standards of the European Union Conference*, 2–13.

Helkala, K., & Bakås, T. H. (2014). Extended results of Norwegian password security survey. *Information Management & Computer Security, 22*(4), 346 - 357.

Kamara, S., Fahmy, S., Schultz, E., Kerschbaum, F., & Frantzen, M. (2010). *Analysis of vulnerabilities in internet firewalls.* Retrieved July 31, 2019, from https://www.cs.purdue.edu/homes/fahmy/papers/firewall-analysis.pdf

Kashefi, I., Kassiri, M., & Shahidinijad, A. (2013). A survey of on security issues in firewall: a new approach for classifying fire wall vulnerabilieties. *Internationla Journal of Engineering Researh and Applications (IJERA), 3*(2), 585-591.

Kearney, P. (2010). *Security: The Human Factor* . Cambridgeshire: IT Governance Publishing. .

Keller, S. (2005). Information Security Threats and Practices in Small Businesses. Information Systems Management. *Security, Ethics, and Legal Issues, 1*(1), 7-18.

Kizza, J. M. (2017). *Guide to Computer Network Security* (4th ed.). Chattanooga: Springer International Publishing AG.

Lab, K. (2013). *Software Vulnerabilities.* Retrieved July 20, 2019, from http://www.securelist.com/en/threats/vulnerabilities?chapter=35

Lamar, A. (2012). *Types of threats to database security.*

Laudon, K. C., & Laudon, J. P. (2014). *Management Information Systems: Managing the Digital Firm* (14th ed.). Essex: Pearson Education Limited.

Lee, H. (2018). *The human factor in cybersecurity: Exploring the accidental insider.* UK: IGI Global.

Lesia, L. C., & McCauley-Bell, P. R. (2007). The human factors issues in information security: What are they and do they matter? *In Proceedings of the Human Factors and Ergonomics Society*, 439–443.

Martin, P. (2019). *Top 10 database attacks.* The Chartered Institute for IT.

Marx, S., & Gardner, J. (2010). Theory and educational research: toward critical social explanation. *International Journal of Qualitative Studies in Education*, 4-5.

Microsoft. (2014). *Microsoft Safety & Security Center.* Retrieved from https://www.microsoft.com/security/pc-security/firewalls-whatis.aspx

Mugo, F. (2017). *Social Research Methods.* London. Retrieved September 15, 2019, from http:www.socialreseachmethods.net/tutorial/Mugo/htm

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

Namaya, A., & Mirza, A. (2018). Understanding Awareness of Cyber Security Threat among IT Employees. *International Journal of Civil Engineering and Technology*, 33-35.

Neely, L. (2017). *Threat Landscape Survey: Users on the front line.* Carlifonia: Sans Institute.

PWC. (2016).University Challenge: Cyber Attacks in Higher Education. VMware, Inc.

University of Hong Kong (2021).Physical Security - Best Practices for General User - ITS.hku.hk. Retrieved January 27, 2021 from https://www.its.hku.hk/sites/default/files/services/infosec/awareness/newsletters/general-users/201602-General-User-Physical-Security.docx

Safianu, O. (2016). *Information System Security Threats and Vulnerabilities.*

Sai, K. O., Gumbo, R., Mzikamwi, T., & Ruvinga, C. (2015). Classification of Point of Sale nformation Security Threats: Case of Smes In Zimbabwe. *Research Inventy: International Journal of Engineering And Science, 5*(9), 33-36.

Sai, K., Manjeese, C., Mawere, J., Denhere, T., & Prosper, T. (2016). An Overview of Information Systems Security Measures in Zimbabwean Small and Medium size Enterprises. *Research Inventy: International Journal of Engineering And Science, 6*(2), 21-26.

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, 2-11.

Security, A. N. (2015). *Science of Security (SoS) Initiative Annual Report 2015[*. Agency National Security. Retrieved Sepetember 12, 2019, from Retrieved from http://cps-vo.org/sos/annualreport2015

Shambalula, M. (2019). *Be Cyber Savvy.* UNAM Computer Centre.

Shanley, A., & Johnstone, M. N. (2015). Selection of penetration testing methodologies: A comparison and evaluation . . *AISMC - Australian Information Security Management Conference*, 65–72.

Shannon, S. (2019). *The human factor of cybersecurity.* CSO.

Shivam, L. (2019). Social Engineering: Hacking into Humans. *International Journal of Advanced Studies of Scientific Research, 4*, 1.

Sheikh, M. et al., (2020). Security and Privacy in Vehicular Ad Hoc Network and Vehicle Cloud Computing: A Survey. *Wireless Communications & Mobile Computing*, Volume: 2020

Singh, H., & Singh. (2017). Penetration Testing In Wireless,. *International Journal of Advanced Research in Computer Science, 8*(5), 2213–2216.

Soomro, A. W., Nizamudin, A., Iqbal, U., & Noorul, A. (2013). Secured symmetric key cryptographic algorithm for small amount of data. *3rd International Conference on Computer and Emerging Technologies (ICCET)*.

Suresh, N. (2016). *NRENs Cloud Architecture Framework (Nrens-Caf): Enhancing Cloud Connectivity Among National Research Education Networks In SADC* . Windhoek.

Taherdoost, H. (2016). Validity and Reliability of the Research Instrument; How to Test the Validation of a Questionnaire/Survey in a Research. *International Journal of Academic Research in Management, 5*(3), 1-2.

Taherdoost, H., & Lumpur. D. (2016). Validity and Reliability of the Research Instrument; How to Test the Validationof a Questionnaire/Survey in a Research.2016, 5. *International Journal of Academic Research in Management(IJARM)*, al-02546799 .

Xynos, K., Sutherland, I., Read, H., Everitt, E., & Blyth, A. (2010). Penetration Testing and Vulnerability Assessments: A Professional Approach. *Proceedings of the 1st International Cyber Resilience Conference*, 126–132.

Yaqoob, I., Hussain, S. A., Mamoon, S., Naseer, N., Akram, J., & Ur Rehman, A. (2017). Penetration Testing and Vulnerability Assessment. *Journal of Network Communications and Emerging Technologies (JNCET) Www.Jncet.Org*, *7*(8), 10-18.

Zadelhoff, V. (2016). *The Biggest Cybersecurity Threats Are Inside Your Company.* Harvard Business Review.

Zorzo, A. F., & Bertoglio, D. D. (2017). Overview and open issues on penetration test. *Journal of the Brazilian Computer Society*, *23*(1), 1–16.

Zhiying, W. et al., (2020). An empirical study on business analytics affordances enhancing the management of cloud computing data security. *IJIM*, V (50), 387-394

8. APPENDICES

APPENDIX A: QUESTIONNAIRE

Efficiency In Staff-Management Relationship

Please tick appropriately

1. Have you ever responded to an online request to provide your account or profile details?

O Yes

O No

2. Has your work or home computer ever been infected by malicious software? (E.g., virus, spyware)

O Yes

O No

3. Which of the following do you use to generate a password? Check all boxes that apply.

O Personal information (e.g., date of birth, place of birth, address, name)

O Phrases

O Numbers

O Symbols

O Lowercase letters

O Uppercase letters

O Combination of the above

O Other:

4. On average, how long in characters is your generated password

O Up to 7 characters

O 8 or more characters

OAs short as the system accepts

5. On an average, how often do you change your password?

O At least once every 3 months

O At least once every 6 months

O At least once every year

O Only when required by the system

O Never

6. Do you reuse the same password for several user accounts?

O Yes

O No

7. If your password is difficult to remember, would you write it down?

O Yes

O No

O May be

8. Do you prevent others from watching you type when you enter your username and password?

O Yes

O No

9. Would you open an email link or attachment from an email address you do not recognize?

O Yes

O No

10. Would you share your username and password with someone else? (E.g., friend, spouse, colleague)

O Yes

O No

11. Would you enter your username and password on a website whose address does not start with "https://"?

O Yes

O No

12. You received a message which is labelled as "critical security updates and installation instructions", would you install it?

O Yes

O No

O I don't know

13. When attending to other matters do you log off your computer?

a. When leaving work premises?

O Yes

O No

b. When attending to a meeting?

O Yes

O No

c. When using the bath room?

O Yes

O No

d. When closing from work?

O Yes

O No

APPENDIX B: INTERVIEW GUIDE

Interview guide

1. What are the existing IT security mechanisms in the University of Namibia?

   ……
   ……
   ……
   ……

a) Install and Properly Configure a Firewall

1. *Do you have a firewall installed?*

   ---

2. *If the response in (1) above is yes, is the firewall properly configured?*

   ---

i. How often is the firewall reconfigured?

---

b) Updating Software

1. Do you carry out software updates?

---

i. How often?

---

c) Protect against Viruses, Worms, and Trojans

1. Does your system have antivirus software?

---

i. How often do you update the software?

---

d) Implement a Strong Password Policy

1. Do you have a password policy?

---

i. *How long should be the password?*

---

ii. *What characters constitute your passwords?*

---

iii. *What other additional measures are included in your password policy? Please specify.*

---

e) Implement Physical Security Measures to Protect Computer Assets

1. Are there any physical security measures to protect computer assets?

---

f) Implement Company Policy and Training

1. Does your University have an IT POLICY?

---

i. If the response is yes above does it offer training on the policy?

---

g) Connect Remote Users Securely

1. *Do you have remote users?*

---

i. If the response is yes above, do you connect remote users securely?

---

h) Lock down Servers

1. Is the server room secured?

i) Implement Identity Services (Intrusion Detection)

1. Does the organisation have an intrusion detection mechanism?

i. How often is the mechanism configured?

---

2. Do you consider human beings as part of the security framework?

……
……
……
……

3. What are some of the human actions that can make information vulnerable or at risk of attacks?

……
……
……
…….

4. Do you have any recommendations that can avoid human actions which disclosures information?

.....
.....
.....
.....

APPENDIX C : PERMISSION LETTER COMPUTER CENTRE

P. O. Box 30743

Windhoek, Namibia

pkautwima@unam.na

Cell: 0814131922

30 July 2019

The Director

Computer Centre

University Of Namibia

P.O. Box 13301

Windhoek, Namibia

Dear Mr. Tuyoleni Hamata

Permission to Conduct Research: Vulnerability Assessment of Information Systems of the University of Namibia based on end users.

I am writing this letter to solicit permission to conduct a research study at UNAM. I am currently enrolled as a master student, Master of Science: Information Technology in the department of IT in the faculty of science and have the intention to conduct my mini thesis research.

If approval is granted, the researcher will interview personnel from computer centre and perform social engineering experiments on UNAM network to target system users on the network.

Should the above proposal be accepted by your good office, it will be highly appreciated if the permission is granted in writing.

Your approval to conduct this study will be greatly appreciated. For further information and verification, please contact my supervisor, Dr Valerianus Hashiyana at the School of Computing: Computer Science Department at vhashiyana@unam.na.

Thank you for your support.

Sincerely,

Paulus S Kautwima

(Student Number: 200841688)

University of Namibia, Private Bag 13301, Windhoek, Namibia
340 Mandume Ndemufayo Avenue, Pioneers Park
☎ +264 61 206 3111; URL.: http//www.unam.edu.na

UNAM
UNIVERSITY OF NAMIBIA

31 July 2019

Mr. Paulus Kautwima (MSC: IT candidate)
Department of Computer Science
School of Computing
University of Namibia

RE: APPROVAL FOR PERMISSION TO CONDUCT RESEARCH TITLED "INFORMATION SYSTEM SECURITY THREATS AND VULNERABILITIES: MITIGATING HUMAN ERROR IN INFORMATION SECURITY AT THE UNIVERSITY OF NAMIBIA (UNAM)."

Reference is made to the above heading.

I am pleased to inform you that approval has been granted to Mr. Paulus Kautwima to conduct research on our network and interview staff from Computer Centre. Further approval to carry out experiments under supervision of Computer Centre staff necessary for the study is hereby also given, as the findings of study will be useful to assist us improve on information security at the University.

UNIVERSITY OF NAMIBIA
P/Bag 13301, Pioneerspark, Windhoek
DIRECTOR
2019 -07- 31
COMPUTER CENTRE

Please feel free to contact me for more details, on 061 206 3031 or email me on hamata@unam.na

Sincerely,

Tuyoleni Hamata
Director: Computer Centre

APPENDIX D: INFORMED CONTENT LETTER

CONSENT LETTER TO PARTICIPATE IN RESEARCH

This is to state that I agree to participate in a program of research being conducted by Paulus Kautwima, a MSC candidate at the University of Namibia, Faculty of Science in the Department of Information Technology.

A) PURPOSE

I have been informed that the purpose of this research is to evaluate vulnerability of Information Systems of the University of Namibia based on end user.

B) PROCEDURES

The research study will take place at University of Namibia, Windhoek main Campus and Oshakati campus. It will take place in a survey form and interviews. The participants will be required fill in questionnaire or an interview question. The participants will be given time to fill in a questionnaire or answer interview questions.

C.) CONDITIONS OF PARTICIPATION

• I understand that I am free to withdraw my consent and discontinue my participation at any time without negative consequences.

• I understand that my participation in this study is confidential.

• I understand that the data from this study may be published.

I …….. HAVE CAREFULLY STUDIED THE ABOVE AND UNDERSTAND THIS AGREEMENT. I FREELY CONSENT AND VOLUNTARILY AGREE TO PARTICIPATE IN THIS STUDY.

Signature: Date:

APPENDIX E: ETHICAL CLEARANCE

ETHICAL CLEARANCE CERTIFICATE

Ethical Clearance Reference Number: SOS-0023 Date: 25 October 2021

This Ethical Clearance Certificate is issued by the University of Namibia Ethics Committee (REC) in accordance with the University of Namibia's Research Ethics Policy and Guidelines. Ethical approval is given in respect of undertakings contained in the Research Project outlined below. This Certificate is issued on the recommendations of the ethical evaluation done by the ethics committee.

Title of Project: VULNERABILITY ASSESSMENT OF INFORMATION SYSTEMS BASED ON END-USER ACTIONS: A CASE OF UNIVERSITY OF NAMIBIA

Student: PAULUS S KAUTWIMA

Student Number: 200841688

Supervisor(s): DR VALERLANUS HASHLYANA (University of Namibia);

Centre for Research Services Take note of the following:

1. Any significant changes in the conditions or undertakings outlined in the approved Proposal must be communicated to the ethics committee. An application to make amendments may be necessary.
2. Any breaches of ethical undertakings or practices that have an impact on ethical conduct of the research must be reported to the ethics committee
3. The Principal Researcher must report issues of ethical compliance to the ethics committee (through the Chairperson) at the end of the Project or as may be requested by the ethics committee
4. The ethics committee retains the right to:
   i) Withdraw or amend this Ethical Clearance if any unethical practices (as outlined in the Research Ethics Policy) have been detected or suspected,
   ii) Request for an ethical compliance report at any point during the course of the research.

The ethics committee wishes you the best in your research.

_____

Dr. Zivayi Chiguvare (Chairperson Ethics Committee)

_____

Prof. Davis Mumbengegwi (Head, Multidisciplinary Research)