EXPLORING THE AWARENESS OF SECURITY THREATS ASSOCIATED WITH SHORT-MESSAGE SERVICE (SMS) AND PROTECTIVE MEASURES AGAINST SMS SECURITY THREATS AMONGST STUDENTS AT THE UNIVERSITY OF NAMIBIA (UNAM)

A THESIS SUBMITTED IN PARTIAL FULFILMENT

OF

THE REQUIREMENTS FOR THE DEGREE

OF

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

OF

THE UNIVERSITY OF NAMIBIA

BY

ABRAHAM KALIPI

9996702

APRIL 2023

MAIN SUPERVISOR: PROF. NICOLA J. BIDWELL

CO-SUPERVISOR: PROF. LAWRENCE KAZEMBE (UNAM)

ABSTRACT

This study focussed on exploring the awareness of security threats associated with short-message Service (SMS) and protective measures against SMS security threats amongst students at the University of Namibia (UNAM). Preliminary interviews with six (6) students with different demographics, informed the design of a survey of students' encounters with, perception of and responses to SMS security threats. Two hundred and eighty-seven (287) students registered at UNAM's twelve (12) campuses countrywide in the 2019 academic year responded to a questionnaire that comprised of forty questions/sub-questions about participants' demographics, experiences and perspectives on security threats associated with the use of SMS. Data were analysed using descriptive and correlation statistics and structural equation models. Participants had some awareness of SMS security threats and used basic security measures such as passcodes, patterns, and biometric access. However, most did not have extensive knowledge of the types of fraudulent activities such as phishing, DoS attacks, relay attacks, and spamming, nor were they aware of protective measures to counter these threats. Only 4% of participants had installed antivirus software on their phones. Junior students comprised 77.7% of participants, which might explain the overall low awareness. Participants indicated that some organisations such as Namibian banks promoted their awareness of security threats, and they thus suggested that the university should run awareness programmes and campaigns. Based on insights about participant demographics and relationships to the university, recommendations were made about how a university might increase students' awareness of some protective measures. These include integrating a compulsory course on cyber security awareness into the university's curriculum.

DEDICATION

I am dedicating this work to my family, my wife: Selma Magano Ndakondjelwa Kalipi and my children: Princess-Rachel Maano Ndeshihafela Kalipi, Happy Maria Iyambo, Prince-Ismael Ndakondjelwa Kafula Kalipi and Ariana Iyaloo Daisy Kalipi. Moreover, I would like to dedicate this work to my parents: Onesmus Hafeni Kalipi and Anna Tulihaleni Kalipi as well as to my siblings: Rachel Maano Ndeshihafela Kalipi, Foibe Nauyele Fabiano, Rauna Dute Ndateelela Kalipi, Ismael Navakalengaho Kafula Kalipi, Josia Shiwa-Elao Kalipi and Gideon Shelikita Kalipi.

ACKNOWLEDGEMENTS

I would like to sincerely acknowledge and express my gratitude and appreciation to both my supervisor and co-supervisor, Prof. Nicola Bidwell and Prof. Lawrence Kazembe respectively. It was a great honour to work with these two professors. I thank them for their time and generous efforts in aiding and guiding me towards the completion of this study. At the same time, I would like to acknowledge my friend, Dr Ndeulipula Petrus Iyaloo Hamutumwa, for his generous assistance and contribution towards the achievements of this study. Last, but not least, I would like to express my sincere gratitude to my entire family and friends for their support towards this great achievement. My special thanks goes to my wife, Selma Magano Ndakondjelwa Kalipi, for the endless support that she offered me towards the achievement and completion of this study.

DECLARATION

I, Abraham Kalipi, hereby declare that this study is my own 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.

……

……

Name of Student Signature

……

Date

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

2FA	Two-Factor Authentication
APP	Application
BTS	Base Transceiver Station
CS	Circuit-Switched
DoS	Denial of Service
ESME	External Short Messaging Entities
FNB	First National Bank
GRN	Government of the Republic of Namibia
GSM	Global System for Mobile communication
H10	First Null Hypotheses
H11	First Alternative Hypothesis
H20	Second Null Hypotheses
H21	Second Alternative Hypotheses
H30	Third Null Hypotheses
H31	Third Alternative Hypotheses
IBM	International Business Machines
ICT	Information Communication Technology
IMS	IP Multimedia Subsystem
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology

LTE	Long Term Evolution
MFA	Multi-Factor Authentication
MMS	Multimedia Messaging Service
MOHSS	Ministry of Health and Social Service
MS	Mobile Station
MTC	Mobile Telecommunications Company
MTP	Message Transfer Part
OS	Operating System
OSI	Open Systems Interconnection
OTP	One-Time-Pin
PS	Packet-Switched
QR Code	Quick Response Code
RO1	First Research Objective
RO2	Second Research Objective
RO3	Third Research Objective
SIM	Subscriber Identity Module
SMS	Short Message Service
SMSC	Short Message Service Centre
SPSS	Statistical Package for the Social Sciences
SS7	Signalling System No.7
TLS	Transfer Layer Security
TN	Telecom Namibia
TUP	Telephone User Part

UID	Unique Identification
UNAM	University of Namibia
URL	Uniform Resource Locator
VMS	Voice Mail System

CHAPTER ONE

INTRODUCTION

1.1 Introduction

Short Message Service (SMS) has become a very popular way for mobile phone users to send and receive text messages (Sameh & Khanim, 2018). In 2018, 292 million people in North America were using text messages, which represents 80% of the total population (Statista Research Department, 2021). However, recent research suggests that while not everyone has a smartphone with internet access, 5 billion people, which is about 65% of the global population, send and receive SMS messages, with Russia having the highest percentage of mobile phone users (89%) of the population sending and receiving text messages. The number is expected to grow to six billion (about 78% of the world population) by the year 2025 (99firms, 2021).

Users are able to send or receive an SMS from a single person, or many people, be it personal messages, email notifications, information services, job dispatches, stock alerts, just to mention but a few. In this regard, mobile phones are essentially powerful handheld computers with operating systems. According to Statista Research Department (2021), there is a likelihood that 98% of the people that own a mobile device will open a text message once received. A mobile phone performs the traditional requirements of providing voice, SMS, MMS and video calling functionality, and it is capable of delivering an array of information processing functionalities including, but not limited to, accessing internet sites, banking and making payments, document editing, email, games and utilising location-based services. The mobile industry had a revenue of $1.05 trillion in 2017 and this indicates a 1.64% annual increase (Slick Text, 2021)

As mobile phones become more pervasive and powerful, security risks associated with Short Message Services have emerged with the mobile platforms. Such risks can include data leakage as a result of unauthorised access, theft or loss, and digital attacks from malicious applications (malware) that may try to spy on and steal the user’s personal data. Furthermore, everyone has easy access to a mobile phone in the event that it is lost or stolen (Holicza & Kadëna, 2018). Subsequently, this may compromise the security of SMS and other sensitive information stored in the mobile phone.

The increasing use of the SMS service in various areas and the growing number of exploits is one of the motivations for collecting, describing and evaluating the details for SMS security. The technical specifications of the mobile network architecture are not made public. Instead, mobile service providers preserve their mobile network architecture to keep it a secret. Bearing this in mind, many academic researchers have tried to find out the vulnerabilities and exploits in mobile network infrastructures and the victims that are affected by those vulnerabilities. This was done as a way to try and provide a unique solution. Whereas hackers perform attacks on a large scale by stealing confidential and sensitive information of the user, hence the need in the present study, to explore students' awareness of security threats and the protective measures that are associated with their use of SMS, using data obtained from UNAM students in Namibia. The rest of this chapter is structured as follows: Section 1.2 presents the background of the study, followed by problem statement in section 1.3 and research objectives in Section 1.4. Subsequently, Section 1.5 provides the hypotheses of the study. The significance of the study and overview of the rest of this thesis is given in Section 1.6 and Section 1.7 respectively. The chapter concludes with Section 1.8, which is a summary of the chapter.

1.2 Background of the study

Mobile phones have become a necessity for many students in Namibia, who widely use SMS to communicate. SMS is supported by every cellular-capable device and a wide range of web applications and it is used more than other communications technology globally (Reaves et al., 2016). Since the SMS does not have built-in security features, users are exposed to security threats, thus only an awareness of threats can avoid losses (Balduzzi et al., 2016). Research suggests that students' awareness and knowledge of security threats increase in relation to their length of stay at university (Mwiraria, 2022).

An SMS Centre (SMSC), usually owned and run by a telecommunications operator, is responsible for the routing and delivery of an SMS.

When an SMS message is delivered to the SMSC, a store-and-forward message mechanism is implemented, whereby the message is temporarily stored, and then forwarded to the recipient's phone when the recipient's device is available. Similar to

email messages, an SMS message may pass through a number of SMSC or other SMS gateways, which act as bridges between two or more SMSCs running different SMSC protocols before reaching the recipient's device. (Balduzzi et al., 2016)

An SMSC helps to route SMS messages and to manage the process. If the intended SMS recipient is not online, the SMSC will keep the stored SMS message for a "validity period" before deleting it from storage.

Mobile phones have become a necessity for many students who widely use SMS to communicate (Madikiza, 2018). Whilst students can suffer losses and damages from SMS security threats, there hasn't been any research that has been done on the types of security threats that Namibian students are exposed to or students' awareness of these threats and knowledge about how to avoid them.

One of the important challenges in the mobile communication industry is to ensure that mobile services are properly used and not open to abuse (Edeh, 2019). Additionally, unencrypted SMS content during the transmission allows the mobile operator's employee to read and modify the SMS content. Unfortunately, the SMS does not have any built-in vetting procedure to authenticate the text or provide security for the data/text transmitted (Zainab Khyioon Abdalrdha, 2019). It is obvious that parts of the SMS applications for mobile devices are designed and developed without taking into account the SMS security aspects.

Exchanging a normal SMS does not guarantee confidentiality as it is not totally secure and reliable since the messages are transferred in a text mode (readable) through an insecure transmitting channel. Due to the special nature of mobile communications and the lack of security of the transmitting channel, achieving the security issues can be considered a high-priority issue, besides improving and enhancing the secret of the SMS content without being unlawfully tempered (Zainab Khyioon Abdalrdha, 2019).

In simple terms, unprotected communication channels and the increasing popularity of wireless devices pose serious security vulnerabilities. Thus, it is important that both the mobile application developers and the mobile service providers (mobile operators) ensure the correct identities of the communicating parties while at the same time,

ensuring SMS content confidentiality and integrity during the data transmission period to avoid these threats (Shaker, 2014). One of the aims of this piece of work is to provide useful advice for further research on the SMS security topic.

1.3 Problem Statement

Mobile phones have become a necessity for many students (Ngoqo & Flowerday, 2015a), who widely use SMS to communicate (Reaves, Blue, Tian, Traynor, & Butler, 2016). While students can suffer loses and damages from SMS security threats there has been no research on the types of security threats that Namibian students are exposed to, or students' awareness of these threats and knowledge about how to avoid them.

1.4 Research objectives

The students' demographics were an opportunity to consider relationships surrounding awareness because most students tend to be oblivious to the threats surrounding their usage of the service unless such is brought to their attention. Hence the research objectives were posed as follows:

a) To discover the characteristics, prevalence and levels of risks associated with SMS security threats that students are exposed to.

b) To determine the students' awareness of SMS security threats and avoidance measures, and how variations amongst students relate to their characteristics or demographics.

c) To study the interventions that can be made to reduce SMS threat exposure to students.

1.5 Hypotheses of the study

$H_{1:}$ There are different levels of awareness of SMS security threats among students.

$H_{2:}$ Students' awareness of SMS security correlates with some demographic characteristics.

1.6 Significance of the study

Along with providing insights about SMS security awareness in Namibia, this study can offer strategic insights to UNAM so as to protect students and contribute to increasing

security awareness in Namibia. It may also inform Namibia's Ministry of Information, Communication and Technology (ICT) in reviewing the national information policy and drafting a programme in ICT Development (GRN, 2014).

1.7 Overview of the rest of this thesis

Chapter two: Literature review

This chapter outlines the backbone and supports the argument of the researcher in light of what has been already discovered by other researchers. The keywords of the research study are discussed in this chapter, which includes SMS security threats and protective measures.

Chapter three: Research methodology

The aim of this chapter is to explain the methodology and research design. The researcher used both the non-probability sampling method and the probability sampling method. The research population and sample are discussed in this chapter as well as the data collection tool. Data analysis and presentation are also well explained, including the manner of reporting the findings.

Chapter four: Data presentation and analysis

The researcher used both qualitative and quantitative data analysis methods to analyse the collected data from the respondents by using numerical and statistical approaches.

Chapter five: Discussions of the results

This chapter provides comprehensive discussions of the study's findings and all factors that have affected such findings both positively and negatively.

Chapter six: Summary, conclusions and recommendations

The summary, findings, conclusions and recommendations are drawn in this chapter. This chapter puts emphasis on what is recommended as per the research findings. This chapter also deals with recommended safety behaviours together with preventive measures concerning security threats associated with SMS.

1.8 Chapter summary

This chapter provided background to the study, its significance, problem statement, research objectives, as well as the hypothesis of the study. Chapter two deals with the theoretical background of relevant sources published in books, and electronic journals that are related to the study and have been used to support the study. The research instruments, data collection and analysis as well as the recommendations of the study.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter outlines security threats associated with SMS and potential protective measures and discusses literature about people's awareness of SMS security in the global south. It focuses on studies about university students' awareness of threats to identify knowledge gaps. The rest of the chapter is structured as follows: Section 2.2 presents the prevalence of SMS, followed by how an SMS works in Section 2.3. Security threats and their counter preventive measures are given in Section 2.4. Section 2.5 provides user awareness of SMS Security threats in the global south. Furthermore, Section 2.6 presented Student awareness and responses to SMS security threats in the global south. The chapter concludes with insights about cybersecurity awareness in Namibia in Section 2.7 and a chapter summary in Section 2.8.

2.2 Prevalence of SMS

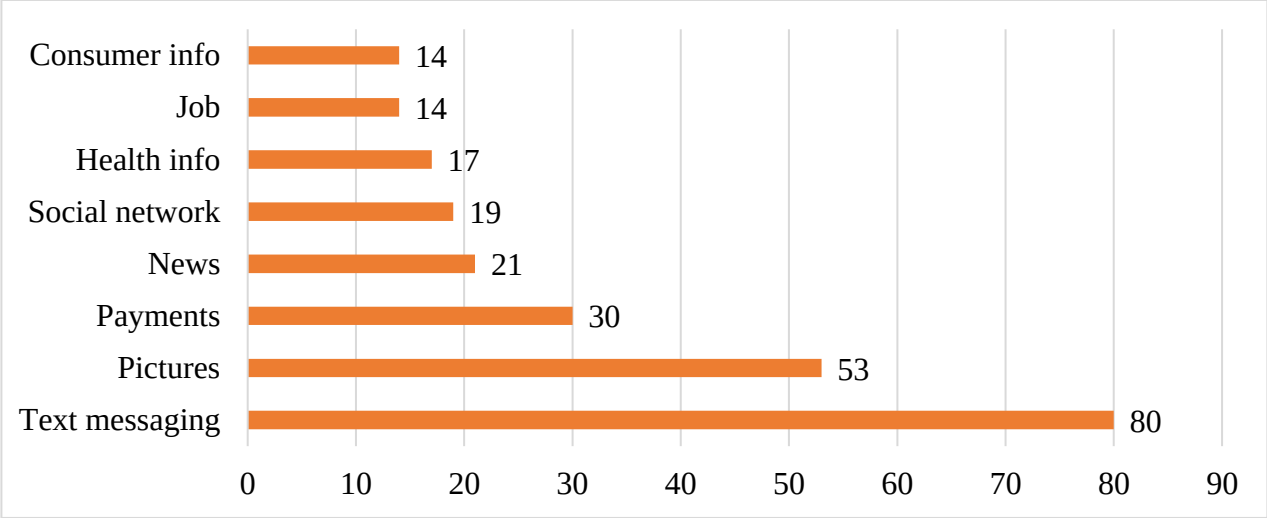


Figure 2.1: Purpose of a cell phone in AFRICA (Source, GE Reports, 2015)

SMS text messaging has become a prevalent communication medium in the forty years since Friedhelm Hillebrand and Bernard Ghillebaert, of GSM Corporation, first conceived it. Indeed, globally, five billion people, which is about 65% of the global population, send and receive SMS messages, and this is expected to grow to 6 billion by

2025 (99firms, 2021). In Africa, text messaging is the most used function on cellphones (Figure 2.1) and a significant volume of messaging is by SMS because not everyone has a smartphone or internet access. Indeed in Namibia, the major mobile network provider, Mobile Telecommunications Company (MTC), reports that SMS traffic volume has remained constant between 9.5 and 10.5 million messages annually since 2013 (Figure 2.2). Figure 2.2 illustrates the SMS traffic for the data which highlights the annual SMS traffic in Namibia from 2010 to 2020. There was a sharp rise in SMS traffic from 2011-2013 with an increase of over 10 million text messages annually. As of 2013, the figures have not significantly dropped (Figure 2.2).

The service is affordable to most subscribers, for instance, MTC's tariff is NAD 0.40 per SMS to national numbers. MTC also offers various prepaid packages, such as Aweh Oka, which costs N$ 7.00 for 3 days and it includes 20 calling minutes, 50 SMS, 20MB data and 20 MB for social media. MTC's most expensive prepaid package, Super Aweh, costs N$ 53.00 per week and this includes 1500 SMSes, 700 calling minutes, 3GB data and 700MB social media data (Mobile Telecommunications Company, 2020).

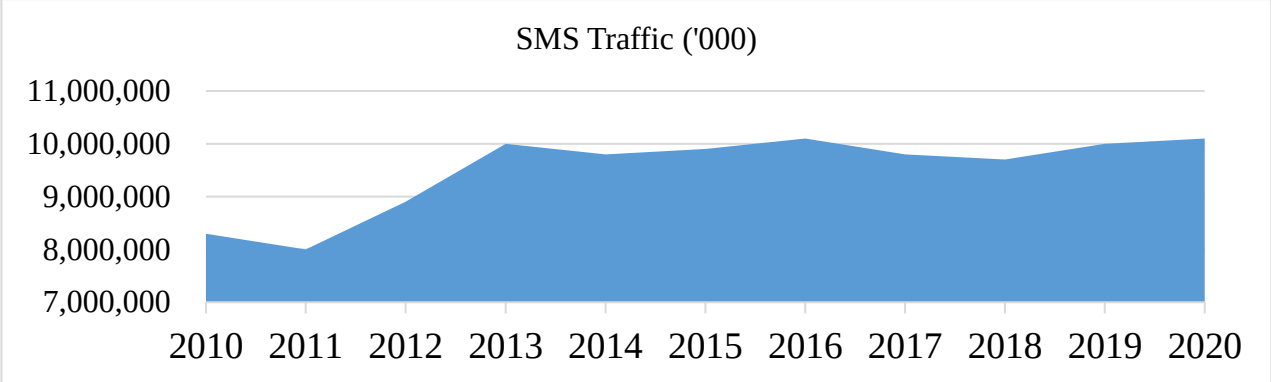


Figure 2.2 SMS traffic in NAMIBIA (Source: Mobile Telecommunications Company, 2020)

The SMS can be used in many different ways in addition to sending messages between people and the market of text messaging is expanding in Namibia. From the simplest use by mobile telecommunications companies, such as MTC and Telecom Namibia (TN), to notify subscribers whenever they have a voice message, organisations are increasingly using the SMS to communicate (Mobile Telecommunications Company, 2020). Not

only do many grocery shops and bookshops communicate with customers via SMS text messages to inform them about new stock arrivals and in-store specials for their goods and discounts, some organisations such as Agra, contain links to their web pages where they keep catalogues with items on special or promotion. Peer-to-peer texting allows the sending of messages to all subscribers who have registered cell phone numbers with telecommunication service providers and this was also used by the Ministry of Health and Social Service - Namibia (MOHSS) about Covid-19 awareness. Indeed, the SMS has become an easy and affordable way for people to access information such as global news, sports news, financial data and weather reports from various content providers.

Banks or e-commerce site servers also use the SMS platform. Not only do banks notify clients using the SMS such as about their downtimes, service unavailability, interruptions and planned maintenance and warnings of possible fraudulent activities during specific times, but they also use SMS for security authentication purposes. Multi-Factor Authentication (MFA) is a security mechanism in which authentication requires the use of more than one verification method (Microsoft, 2019). Online businesses and organisations that use the SMS-based MFA for registration and authentication require users to legitimate their use in the form of text messages to protect accounts and private information hosted by these websites. For instance, a One-Time-Pin (OTP), is often sent for authentication purposes when using bank debit cards or making e-commerce transactions. OTPs, Unique Identification (UID), passwords or other verification codes enable a key second factor as a security measure (Simmons et al., 2019).

2.3 How SMS works

The SMS network provides an infrastructure for delivering short messages to and from mobile clients or computing systems. This section outlines how the technology works in order to understand its particular security threats and the vulnerabilities that compromise safe use.

SMS is based on the Signalling System No.7 (SS7) protocol, which was developed to support calls, billing, routing, and information exchange functions of the public switched telephone network establishing (Erickson, 2012, Martin, 2012). SS7 is responsible for incoming messages at the entry point of networks, and it comprises of the Message Transfer Part (**MTP)** and the Telephone User Part **(TUP)**. The MTP is responsible for

transferring the message within a signalling network, from one network element to another network element and the entire SS7 is built on the foundation of MTP, which consists of three bottom sub-layers of the Open Systems Interconnection (OSI) model layers. All seven layers of the OSI model contribute to the flow of messages when computer systems communicate over a network. However, the 7th layer is most vulnerable to attacks as it is the application layer that connects to the end user. The MTP thus comprises the following layers:

1. The Physical Layer, which defines the connector and is responsible for the physical cable or wireless connection between network nodes (Patton Electronics Company, 2012). Signalling links utilise DS-0 channels and carry raw signalling data at a rate of 56 kbps or 64 kbps (56 kbps is the more common implementation).
2. The Data Link Layer, which ensures that the two end-points of a signalling link can reliably exchange signalling messages and incorporates error checking, flow control, and sequence checking (Patton Electronics Company, 2012).
3. The Network Layer, which extends MTP level 2 functionality to ensure that messages can be delivered between signalling points across the SS7 network whether or not they are directly connected. It includes such capabilities as node addressing, routing, alternate routing, and congestion control (Russell, 2014).

   The Telephone User Part **(TUP)** is responsible for transferring the message to the user using sets of messages that set up, supervise and clear the call (American National Standards Institute, 2011; Sauter, 2014). The TUP explains who the user is, whom the message is intended for as well as the content of the message.

SMS messages are delivered through a control channel of the network, which usually guarantees delivery. The heart of the SMS system is the Short Message Service Centre (SMSC) which acts as a store-and-forward system for short messages (Shaker, 2014). It receives the short messages from mobile clients inside the cellular network and External Short Messaging Entities (ESMEs) such as web-based SMS portals, voice mail systems (VMS), and email notification systems. When a short message arrives, the SMSC determines the content, transforms it into SMS format, and places it into the SMSC queue. The cellular network infrastructure finds the destination mobile client and routes

the message to the client. If the receiving mobile device is unreachable, the SMSC will store the short message until it becomes available. The SMS client maintains a session with the internet SMS provider's server which forwards SMS messages between the internet client and the SMS centre.

The IP Multimedia Subsystem (IMS) provides multimedia services in mobile networks (F5 Networks, 2015). The IMS switches and distributes information across diverse devices and networks into a single transport protocol IP using circuit switching (Salmon et al., 2017).

2.4 Security threats and their counter preventive measures

SMS lacks the basic elements of security, including confidentiality, integrity and endpoint authentication, and as such, security threats are prevalent, which impacts mobile phone subscribers daily (Tu et al., 2016). Some threats, such as denial-of-service (DoS) and some types of interception do not require their victims to do anything. Others, including SMS spoofing and phishing, involve manipulation, whereby an attacker uses "social engineering" to trick the victim in some way (Hadnagy & Schulman, 2021).

2.4.1 SMS client denial of service (DoS) attack

Security Threat: At its most basic, a security attack can make a computer resource unavailable to its intended users. A DoS attack can flood a targeted network with SMS messages at a sufficient rate to saturate the control channels (Ortiz, 2020), which constrains and blocks legitimate network traffic, or sends repeated messages to a target mobile phone to make it inaccessible (Gupta et al., 2018).

Preventive Measure: Mobile network providers could prevent some threats like DoS attack by determining whether a caller is deceiving the receiver by analysing messages (Fahri, 2021). However, this would infringe on the user's privacy, thus network providers prioritise improving security on the back end to protect SMS transmission.

2.4.2 Silent SMS attacks

Security Threat: Silent SMS attacks exploit SS7 vulnerabilities to reach their targeted victims (Olaleye et al., 2013). While initially used by governments and law enforcement agents to track criminals, Silent SMS attacks are now among the most worrying types of

threats because they are invisible to the victims and cannot be detected after they are executed (Dawson & Omar, 2015). They can be used by attackers to carry out activities like DoS, location, launch an internet browser with a specific Uniform Resource Locator (URL), send an SMS or start a call.

Preventive Measures: The improvement of security on the back end by network providers to protect SMS transmission can help to prevent Silent SMS attacks. Furthermore, Silent SMS attacks can be avoided by closing known vulnerabilities within the SS7.

2.4.3 SMS interception

Security Threat: SMS interception happens when attackers obtain a subscriber's SMS data and use it for selfish and or malicious purposes (Akamai, 2021), for instance, accessing a victim's private text messages or MFA codes to enter secured accounts and OTPs to conduct fraudulent banking activities. SMS messages can be intercepted in many different ways. Firstly, as messages are delivered in GSM signalling channels between the Mobile Station (MS) and the Base Transceiver Station (BTS) the contents of SMS messages are visible to the network operator's systems and personnel (Sexena & Chaudhari, 2012). Interception also includes instances when an attacker impersonates a targeted victim and requests their services to be transferred to another mobile service provider and then sets up the services with the new mobile service provider (Akamai, 2021); for example, requesting that MTC services are transferred to TN Mobile. Another way to intercept is when attackers take advantage of SS7 security flaws to intercept SMS data sent to a targeted victim's mobile phone.

Connecting to the internet affords other ways to intercept messages. Phones generate messages in plain text which can be easily read and modified before it reaches the receiver. Attackers can also access session information of messages and launch a variety of hijacking attacks from the session information (Stewart & Kinsey, 2020). Attackers can also misuse previously exchanged messages between the subscriber and network to perform a replay attack (Chowdary et al., 2018). Meanwhile, impersonating a server can also enable re-routing messages, and authentication processes are unable to differentiate between intruders and legitimate users (Maleh et al., 2018).

Interception can also involve “social engineering” when a subscriber requests their mobile service provider to swap their phone services to a new Subscriber Identity Module (SIM) card after their phone is lost or damaged. In a SIM swap scam, for instance, the subscriber is tricked into disclosing sensitive information or making security mistakes while they request a swap (Hadnagy & Schulman, 2021).

Preventive Measures: More secure platforms can reduce threats by identifying intrusions, disrupting malware communications, isolating infected resources, and protecting critical resources (Yadav & Kumar, 2018). Transfer Layer Security (TLS), for instance, was designed to prevent eavesdropping and with tampering SMS messages, and this uses public-and-private key encryption to prevent harmful malicious malware (Chowdary, Rajitha, Aneesha, & Babu, 2018). Anti-malware and host-based Intrusion Prevention System (IPS) collect system information from various parts of the network, identify abnormal activities from metadata and reputation data and analyse it for possible malicious security threats.

2.4.4 SMS spoofing

Security Threat: Spoofing attacks with messages that look harmless to users (IIyas & Ahson, 2018). SMS spoofing changes the sender’s information on a text so that the receiver assumes that the SMS is coming from a different sender whose phone number might be different from the initial phone number used to send the message (Salmon et al., 2017). While there can be a legitimate use of SMS spoofing by setting the company’s name or product name or a sender’s mobile number, illegitimate spoofing impersonates a company, products or another person for malicious purposes (Salmon et al., 2017).

Preventive Measure: Creating awareness about SMS security amongst subscribers can help to prevent spoofing.

2.4.5 SMS phishing (Smishing) and hacking via SMS

Security Threat: SMS phishing or smishing is used to lure a victim into revealing confidential information or getting them to install malware (Reynolds, 2016). Attackers send SMS messages containing a call to action for intended victims to respond, and a

link to a website that looks legitimate but can lead victims to expose financial or other sensitive information.

Cybersecurity researchers have also revealed a critical vulnerability in SIM cards that could allow attackers to access a smartphone by sending an SMS (Ryder, 2019). The phone is hacked when a victim opens a link in the SMS, which then sends a malicious SMS consisting of binary codes that enable hackers to access a phone and its location. Attackers can then perform various functions remotely, while the subscriber is unaware, such as surveillance or disabling their SIM cards.

Preventive Measures: Subscribers can avoid responding to SMSs from unknown senders. Additionally, subscribers can stay safe by only contacting senders through trusted channels, such as an organisation's official website. Lastly, subscribers can install antivirus software that analyses malware on their devices.

2.4.6 SMS spamming

Security Threat: SMS spam is an unsolicited and unwanted SMS text message (Jiang et al., 2012). Bulk SMS broadcasting is available for almost everyone to send out mass SMS messages (Maleh- et al., 2018) and spam is often sent as a commercial advertisement. While it can be a legitimate marketing channel, it also presents an inconvenience to recipients and can burden subscribers if their receipt of the SMS is charged to them by their network services provider. SMS spam can also make a subscriber's phone freeze or automatically dial emergency numbers (Jiang et al., 2012). While not as prevalent as email spam, SMS spam can flood phone networks, thereby causing delays and slowing down the rate they can transfer legitimate SMS.

Preventive Measure: Subscribers can protect themselves by keeping their phones safe, using strong passwords and reviewing their phone bills and use of airtime to identify unexpected charges that might have been caused by malware.

2.5 User awareness of SMS security threats in the global south

Some 62% of global organisations indicate that they are unable to handle cyber-attacks even when they are aware of the threats (Nick, 2021) and it is estimated that private and

public sector investment in raising citizen's and employees' awareness can reduce cyber-attacks from 70% to 45% (Nick, 2021). The importance of increased awareness of security threats is illustrated by print and broadcast media campaigns around the world. However, more attention tends to be paid to raising awareness of computer and internet threats, and less on how easy it is to intercept SMS messages. Indeed, while 61% of corporate users are aware of what phishing is, only 30% know about smishing techniques (Chickowski, 2020).

The lack of public awareness-raising campaigns contributes to the growing vulnerability of people in the global south to cyber-attacks (Bada et al., 2018). However, awareness campaigns must account for ICT literacy levels (Bada et al., 2018). ICT literate populations campaigns have contributed to some wider awareness of SMS threats. For instance, a study in five cities across Indonesia found that 80% of smartphone users were aware of SMS spam and fraud and the need to protect personal data, adhere to security policies and report security incidents (Sari, 2014). However, ICT literacy levels in countries such as The Democratic Republic of Congo, Nigeria, Ghana, Kenya, Botswana and South Africa contribute to the low awareness levels (Bada et al., 2018).

Awareness of threats does not necessarily translate into practising prevention. While this can be because people lack knowledge about security devices, it can also be due to complacency (Gupta et al., 2018). For instance, while 70% of South African users surveyed knew that they should regularly change their passwords, only 23% actually do (Chandarman & Van Niekerk, 2017) and only 28% used Two Factor Authentication (2FA) on their accounts (Chandarman & Van Niekerk, 2017). Similarly, while Indonesian users were aware of threats, non-adherence to security policies can reflect a lack of time to read all the items in a security policy (Sari, 2014).

2.6 Student awareness and responses to SMS security threats in the Global South

Various African governments, including Namibia, have committed to using ICTs to improve learning within the education system (Sylla et al., 2020), and SMS has been used to support knowledge-building platforms. For instance, M-Shule is used in Uganda to deliver reading lessons in local languages by SMS and audio to a parent's mobile phone to enable students who are unable to physically attend classes to participate (Van

Niekerk, 2020). Educational institutions also use the SMS to communicate with students and staff. In fact, universities around the world message students to welcome them, notify them about lectures/activities, class cancellations and administrative information; send instructions for submitting assignments; remind them to submit and collect assignments; and warn about absenteeism (Olaleye et al., 2013; Management Association Information, 2020). Thus, as well as using SMS to communicate with each other, friends, families and relatives via SMS (Chai, 2021), students also receive some SMS alerting them of activities, news, or invitations to participate in research, and often texts link to other communication channels, such as university web portals.

University students who use mobile phones for longer periods are more exposed to and thus tend to be more aware of SMS-related security threats (Garba et al., 2020). In Thailand, 84% of student smartphone users surveyed displayed a high level of awareness as they indicated that they always pay attention to permissions asked by the applications that they download, protect themselves from spyware and were concerned about privacy (Calderwood & Popova, 2019). However, despite their awareness, most students (82%) said that they sometimes clicked on links in phishing emails (Calderwood & Popova, 2019). Some 60% of college students surveyed in major cities in Tamil Nadu, India, had received phishing emails or messages, and while a few responded to phishing emails/messages, 11% had been victims of virus attacks (Senthilkumar & Easwaramoorthy, 2018). Some of the Indian students use countermeasures, such as antivirus software. However, students tend to be more aware of security threats that target computers. For instance, only 38% of university students in Jordan were aware of threats targeting phones, and 56% believed that it is more likely that their computers would be affected by malicious programmes (Taha & Dahabiyeh, 2021).

A study by Chandarman and Van Niekerk (2017) on three campuses of a private tertiary education institution in KwaZulu Natal, South Africa, indicated that, while they might be aware of some SMS security threats, students do not know about all the security risks and necessary security practices. The sampled population included first-year students and senior students over two semesters using online and paper-based questionnaires and found that 56% of the students did not correctly know about phishing and 43% of the

students did not correctly know about the purpose of anti-virus software. Student mobile phone users at a university in the Eastern Cape, South Africa, had low levels of information about security awareness and as such, they are prone to make bad security decisions (Ngoqo & Flowerday, 2015a). Regardless of the length of time, they have owned a mobile phone, students who use their mobile phones less frequently are likely to be less aware of SMS-related security threats. Some scholars proffer that students from urban areas in Nigeria are more aware of SMS security threats than those from rural areas (Garba et al., 2020), which might reflect the frequency of use, and it has been found that computer science students become more aware of mobile technology security risks, including those related to SMS, as they progress through their studies. However, often computer science programmes are gendered, for instance with regards to the Nigerian students, mostly aged 21-25 years, comprising 90% of men (Garba et al., 2020). This supports calls to integrate cyber security awareness efforts into ICT literacy courses as part of all curricula (Bada et al., 2018).

2.7 Insights about cybersecurity awareness in Namibia

Namibia is not an exception to cybersecurity impacts. Furthermore, a lack of cybersecurity frameworks in Namibia could be an obstacle towards fighting cybercrimes effectively (Nawa, 2021). Moreover, Nawa (2021) argues that Namibia lacks a recognised cybersecurity framework that is aimed at creating awareness and safeguarding sensitive financial data between banks and customers during online banking transactions. In the same vein, Nhinda and Shava (2021) argue that rural Africans suffer from cybersecurity risks as a result of low cybersecurity awareness. Namibian students from rural backgrounds might also fall victim to the same trend. Equally so, some scholars argue that Namibia has acquired more sophisticated surveillance technologies which can compromise her ordinary citizens' human rights to privacy if placed in the wrong hands (Mare, 2019). Furthermore, the involvement of ZTE and Huawei Technologies (Chinese telecommunication giants) in Namibia, the monopoly in the telecommunications sector by the Namibian government, the lack of an independent regulator in the country and the lack of a comprehensive data protection law are some of the factors that might lead to the misuse/abuse of surveillance technologies

in Namibia, which may impact the daily livelihoods of her ordinary citizens negatively (Mare, 2019).

2.8 Chapter summary

This chapter summarised SMS mobile security threats and countermeasures, including cyber security campaigns to increase people's awareness of threats. Research suggests that university students in Africa are often exposed to threats. However, there are no reports about awareness of SMS threats in Namibia. Thus, this study sought to determine the awareness of SMS security threats amongst students at UNAM and the next chapter (Chapter three) describes the methodology used to do this.

CHAPTER THREE

RESEARCH METHODS

3.1 Introduction

This chapter discusses the research methods used in this study. The rest of this chapter is structured as follows: Section 3.2 presents the research design, followed by Section 3.3 which contains the research objective, while associated research hypotheses are outlined in Section 3.4. Subsequently, Section 3.5 provides research instruments. The target population and study sample are given in Sections 3.6 and 3.7 respectively. Data management procedures and analysis are presented in Sections 3.8 and 3.9. The chapter concludes with Section 3.10 on research ethics and Section 3.11 is the chapter summary.

3.2 Research design

Tshabangu et al. (2020) explain that research designs control the process and the way in which researchers undertake their studies. A research design is defined as an overall approach to data collection. Research designs control the selection of sample size, data collection and analysis techniques. This section describes how the research was designed in terms of the techniques used for data collection, sampling strategy, and data analysis.

The embedded mixed-method research design was used in this research. Figure 3.1 presents the research design framework. The qualitative research approach was used to inform a quantitative research approach, which is the main approach for this study. For the qualitative research approach, a focus group of six (6) students was selected and preliminary interviews using semi-formal interviews were administered to find out about students' knowledge of SMS security awareness, protective measures and technical terms. The information gathered from preliminary interviews was used to help in formulating the draft questionnaire. The draft questionnaire was piloted with ten (10) students. After the pilot process, a final questionnaire was formed and administered to collect quantitative data from students registered at UNAM for the 2019 academic year.

The collected data were used to identify and verify valid questions to be included in the research questionnaire. Furthermore, questionnaires were used to collect primary quantitative data. The data collected were exported to Microsoft Excel and then cleaned

to achieve more sensible data before the data could be analysed. Last but not least, the clean data were analysed using IBM SPSS 20.

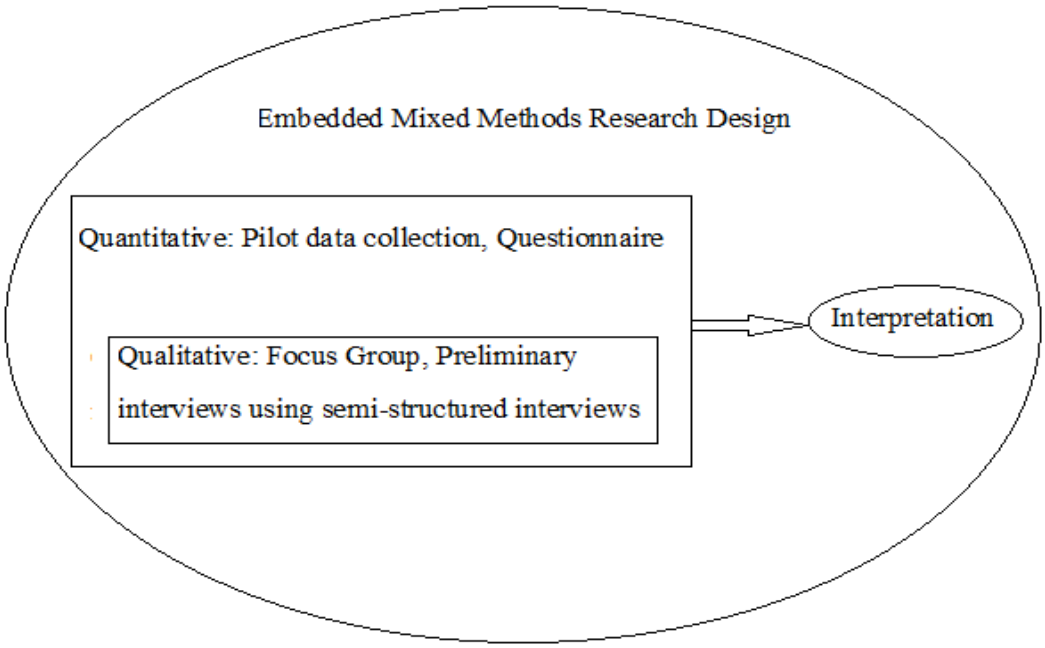


Figure. 3.1 Research design framework

Different sampling techniques were used in this study. During the preliminary interviews, stratified sampling was used, with the Faculty being considered as a stratum. Within each stratum, six (6) students were selected, balancing across the year of study (ranging from the first-year to fifth-year students) and gender. The same stratification was used to select participants for the focus group discussion (FGD). Additionally, for the pilot questionnaires, convenience sampling was used to select ten (10) students to participate. Lastly, for questionnaires, convenience sampling was again used to select the participants to participate voluntarily online and through paper mode.

3.3 Research objectives

The main research objective was to determine the awareness of SMS security threats amongst students at the University of Namibia (UNAM), and interventions that can reduce their exposure. The sub-objectives were:

RO1 – To discover the characteristics, prevalence and levels of risk associated with SMS security threats that students are exposed to.

RO2 – To determine students' awareness of SMS security threats and avoidance measures, and how variations amongst students relate to their characteristics or demographics.

RO3 – To study interventions that can increase students' protection.

3.4 Hypothesis

Syafriandi (2020) proffers that a hypothesis is defined as a statement summarising the prediction of what the findings of the research study will reveal.

The current study was based on the qualitative research approach, which made it paramount to develop the hypothesis that would be used as a test standard for the qualitative design approach. There are sets of two hypotheses that were formulated to be tested in this study and they are as follows:

H10: There are no different levels of awareness of SMS security threats amongst students.

H11: There are different levels of awareness of SMS security threats amongst students.

H20: Students' awareness of SMS security does not correlate with some demographic characteristics.

H21: Students' awareness of SMS security does correlate with some demographic characteristics.

H30: There are no interventions that can increase students' protection.

H31: There are interventions that can increase students' protection.

3.5 Research instruments

Cost et al. (2020) detail that research instruments are tools and instruments that are used for collecting, measuring and analysing the data that are related to the research of interest. The instruments can include interviews, surveys, tests, observation checklists and all other means of recording data needed for the execution of the study.

The researcher outlines the process of choosing and selecting the research instruments as well as supporting the reasons for choosing the proposed instruments and tools for the

study. The main research instruments were semi-structured interviews and questionnaires. Semi-structured interviews were used to collect qualitative data because of their flexibility. Since the questions were prepared beforehand, this gave the researcher ample time for preparation. The interviews allowed participants to express their views as freely as they could and this in turn allowed the researcher to collect more extensive data. Questionnaires were used to collect quantitative data as this proved to be advantageous as questionnaires provide the benefits of covering a large group when collecting data.

3.5.1 Questionnaires

The questionnaire contained sixteen (16) questions and twenty-four (24) sub-questions. Seven (7) questions were study-specific questions, and nine (9) questions gathered demographic information, and it took respondents an average time of fifteen (15) minutes to complete. UNAM's Computer Centre staff with assistance from the UNAM Institutional Statistician uploaded the final questionnaire to the UNAM portal.

The questionnaire remained on the portal for ten (10) weeks and by then, the sampling criteria were met. Students were invited to complete the questionnaire through a message on the UNAM students' portal dashboard. At the same time, posters with a QR Code and a link to the questionnaire were plastered all around campus to invite and encourage students to participate. The printed questionnaires were distributed and administered during first-year students' registration over a period of one week. During this practice, students who volunteered to participate were randomly selected. The survey was conducted throughout the week as students from different faculties registered on different days.

After piloting the questionnaire, a final questionnaire was administered to collect quantitative data and two hundred and eighty-seven (287) students responded. The questionnaires were administered using two methods, online through Google forms as well as manually by paper. Questionnaires were used in this study because of their ability to collect both qualitative and quantitative primary data.

In this regard, questionnaires were used to collect demographic data, data pertaining to characteristics, prevalence and levels of risk associated with SMS security threats that

students are exposed to. Additionally, questionnaires were used to collect data pertaining to levels of SMS security threats awareness as well as data pertaining to preventive measures used by students against SMS security threats. Moreover, questionnaires were also used to collect data on interventions used by students to reduce security risks associated with SMS usage. Likewise, questionnaires collected data on confidence levels among students regarding protecting themselves against SMS-related security threats.

3.5.2 Preliminary interviews

Myers (2019) proffers that semi-structured interviews sit in between structured and unstructured interviews. Semi-structured interviews involve the use of some pre-formulated questions, but there is no adherence to them.

The preliminary interviews were carried out and semi-structured interviews were preferred to be used to administer the interviews because of the flexibility of the method itself. Semi-structured interviews were chosen because of their ability to get students' perspectives regarding their experiences pertaining to the awareness of SMS-related security threats. Additionally, semi-structured interviews were also preferred for their effectiveness in assessing, validating, confirming, elaborating and refuting the existing knowledge about the awareness of SMS-related security threats among students.

Furthermore, semi-structured interviews were used to discover new knowledge pertaining to the awareness of SMS-related security threats among students. Moreover, semi-structured interviews were used to collect information related to the aspects of security awareness and preventive measures known or used by students. Finally, semi-structured interviews provided insights into the aspects of security technical language/terms that were used to form questions in the questionnaire. Other insights worth mentioning relate to the various text messaging platforms that students use other than SMS, and an example is WhatsApp. Consequently, preliminary interview results gave clear-cut insights and guidance on the type of questions to include in the research questionnaire.

3.5.3 Pilot data collection

Ekinci (2015) states that pilot testing is an essential part of questionnaire development to ensure that potential problems are identified and eliminated before moving on to the data

collection stage. Furthermore, Ekinci (2015) asserts that pilot testing determines how long it will take to administrate a questionnaire, as a result, this will help the researcher to know how long it will take to complete and which questions are most essential. Upon completion of preliminary interviews and transcribing, a draft questionnaire was formulated. The draft questionnaire was piloted on ten (10) students with the purpose of confirming the clarity of questions to students, ensuring that questions yield meaningful results and data, as well as discovering and clearing out any practical problems. At the same time, the draft questionnaire was piloted to verify that the survey was in compliance with UNAM research ethics. Consequently, the piloting process cleared the researcher's uncertainties regarding which questions to include or exclude from the final questionnaire.

3.6 Population

Thomas (2021) clarifies that a population is a group of individuals having one or more characteristics in common. The target population for this study was 13,073 students registered at the UNAM Main Campus for the 2019 academic year. The target population included students from all UNAM faculties and they were of different demographics as well as different backgrounds.

3.7 Sample

Sampling is the process of selecting a few individuals from a bigger group (sampling population) as the basis for estimating or predicting the prevalence of an unknown piece of information, situation or outcome regarding a bigger group (Kumar, 2018).

The researcher preferred to work with two sampling methods, both nonprobability sampling and probability sampling. The researcher opted to use both sampling techniques to attain better representation. The researcher wanted every participant to be represented in the study. In nonprobability sampling, the members of the population are selected in a non-random manner and on the other hand, in probability sampling, members of the population have a known non-zero probability of being selected (Vasuki, 2021).

Ekinci (2015) declares that convenience sampling is used in exploratory research where the researcher is interested in gathering an inexpensive approximation of the truth. Thus,

the researcher opted to use convenience sampling to select students of all different demographics who participated in the preliminary interview. The reasons were to acquire a substantial amount of information needed and since the study involves awareness of students to security threats, hence the choice to use convenient sampling.

Thomas (2021) states that stratified sampling is a stratum subset of the population that shares at least one common characteristic. Hence the choice by the present researcher to select a group of six (6) students who were sampled to participate in the preliminary interview.

As for the final questionnaire, convenience sampling was used again to draw representative proportions of students from each category: gender, year of study and faculty/field of study. In the same vein, a sample of five hundred and seventy-four (582) students was proposed and two hundred and eighty-seven (287) students responded to the survey. In this regard, one hundred and eighty-seven (187) students responded online and one hundred (100) students responded through the paper based questionnaires. Out of one hundred and eight (108) students who received paper based questionnaires, a total of eight (8) students did not return them back. Despite this, the number of students who responded exceeded the researcher's expectations, and the rate of response was quite overwhelming. More students responded online- and this indicates how technology has advanced as several people are now switching to online-based platforms. Hence the 100 students who responded through paper-based questionnaires reflect how dominant modern methods such as online-based platforms are compared to traditional methods.

In regard to this, participants for the focus group were drawn from all UNAM faculties from the main campus to attain diversity. The focus group consisted of six (6) students, four (4) females and two (2) males. The age group for the female respondents were 19, 22, 23 and 25. One (1) of the female students was in her first (1^{st}) year of study and two (2) were in their second (2^{nd}) year of study and third (3^{rd}) year of study respectively, with the last female student being in her fourth (4^{th}) year of study. On the other hand, the age group for the male respondents was 18 and 23. Additionally, one (1) of the male students was in his first (1^{st}) year of study and the other one was in his fifth (5^{th}) year of study. This was achieved by making appointments with students from different faculties

during their face-to-face classes and requesting them to participate in the interview. Consequently, the information obtained from the preliminary interview was used to formulate the draft questionnaire.

The draft questionnaire was created in Google forms. The draft questionnaire was refined iteratively until saturation, or until interviews produced no further changes. This draft questionnaire was then piloted among ten (10) UNAM students.

3.8 Procedure

Clearance approval: This study started with getting the research topic approved and obtaining the ethical clearance from the University of Namibia with the reference number FOS/363/2018, to carry out the research. After obtaining the research topic approval as well as the ethics clearance approval, the researcher proceeded with data collection which was followed by data analysis and later by the results of the analysis. The data collection process went through the following stages.

The data collection for this study started with preliminary interviews, which were followed by the piloting of the questionnaire and lastly, the administration of the questionnaire via both Google docs and paper questionnaires.

Preliminary interviews: Ten (10) questions with the last question consisting of five (5) sub-questions formed the semi-structured interview questions which were used with a focus group of six (6) students during the preliminary interviews. Additionally, the preliminary interviews were recorded and later transcribed. It is worth mentioning that the preliminary interviews provided insights into students' aspects of awareness of security threats related to SMS.

Focus group discussions: Participants for the focus group discussions were drawn from every UNAM faculty so as to achieve maximum diversity. Furthermore, this was achieved by making appointments with students from different faculties during their face-to-face classes and requesting them to avail time to participate in the focus group discussions. Consequently, the information obtained from the preliminary interview was used to formulate the draft questionnaire.

Draft questionnaire: The draft questionnaire was created in Google forms. The draft questionnaire was refined iteratively until saturation, or until interviews produced no further changes. This draft questionnaire was then piloted among ten (10) UNAM students.

Questionnaire: The questionnaire contained sixteen (16) questions and twenty-four (24) sub-questions. Seven (7) questions were study-specific questions, and nine (9) questions gathered demographic information, and it took respondents an average time of fifteen (15) minutes to complete the questionnaire. UNAM's Computer Centre staff and the UNAM institutional statistician helped to upload the final questionnaire to the UNAM portal.

The questionnaire remained on the portal for ten (10) weeks and by then, the sampling criteria were met. Students were invited to complete the questionnaire through a message on the UNAM students' portal dashboard. At the same time, posters with a QR Code and a link to the questionnaire were plastered all around campus to invite and encourage students to participate in the study. At the same time, printed questionnaires were distributed and administered during first-year students' registration over a period of one week. During this period, students who volunteered to participate in the study were randomly selected. The survey was conducted throughout the week as students from different faculties registered on different days.

Retrieval of questionnaires: After all the respondents were done answering, the researcher immediately proceeded with the collection of the questionnaires. This stage was only concluded when all the necessary data were collected from the respondents. Upon completion, the responses were tailed, analysed and interpreted.

3.9 Data analysis

According to Bazeley (2021), data analysis is the process of deconstruction and the reconstruction of evidence that involves purposeful interrogation and critical thinking about how to produce a meaningful interpretation and relevant understanding to answer the questions asked or that arise in the process of investigation during the study. The researcher opted to use both descriptive analysis and thematic analysis for this study.

3.9.1 Preliminary analysis

It was imperative for the researcher to do a preliminary analysis to have insights on how to approach the data analysis. An exploratory analysis of the data sets was employed as a quick way to get insights into important characteristics of the data. This helped the researcher to have a clear visual perspective as to how to proceed with the data analysis.

3.9.2 Confirmatory analysis

Both descriptive analysis and modelling were applied to answer the research objectives and hypotheses. Descriptive statistics is a set of statistical procedures that summarises the essential characteristics of the distribution through calculating or plotting. The researcher opted to use descriptive statistics to analyse the geographic context of the population. By so doing, this enabled the researcher to get an understanding of the data variability and this also allowed the researcher to identify possible errors. In addition, this further allowed the researcher to get insights into the data distribution by calculating specific characteristics such as the average or standard deviation.

RO1 was addressed with descriptive statistics. The researcher used bar charts and pie charts to display descriptive characteristics of participants through percentages and the number of participants. The demographic characteristics displayed by different bar charts are the faculty of participants, gender and age group of participants, previous high school attended and the place of residence for the participants. Furthermore, bar charts were used to display respondents' responses to questions asked in the questionnaire. Bar charts were used to display responses in relation to the question, "Which organisations have sent you SMS warnings about threats before?". Moreover, a bar chart was used to display participants' responses to the question: "Do you feel confident in protecting the privacy of your phone?". Another bar chart was plotted to display the participants' responses to the question: "Do you pick up a call from a phone number you do not recognise?" and "Do you respond to SMS texts from numbers that you do not recognise?". The last bar chart was used to display the participants' responses to the question: "Please describe all the different types of SMS security threats that require you to protect items stored in your phone". A pie chart was used to display the percentage of participants' years of study. Another pie chart was used to display the number of

participants and the sources which they have heard about SMS security from. Furthermore, a pie chart was used to display the percentage of participants' responses to the question: "Please explain all the different ways you use to protect items stored in your phone". RO2 was addressed with regression or correlation statistics. Binary logistics targeted the question: "Have you ever received a threatening SMS?" and "Have you heard of any security threats associated with the use of SMS?". On the other hand, ordinal logistic regression addressed the question: "How long have you had a cell phone?".

RO3: Participants in a focus group were asked questions on how often they use the SMS and what they use the SMS for. Participants were also asked if they know or are aware of terms like hacking, phishing, smishing, DoS, spam and vulnerability. Likewise, the participants answered questions about the protective measures they use to protect their SMS contents.

All the collected data were exported to Microsoft Excel. Needless to say, the data were cleaned to achieve more sensible data before they could be analysed. Last but not least, the clean data were analysed using IBM SPSS 20.

3.10 Research ethics

Ethical clearance and permission to conduct the research were obtained from UNAM's Research and Ethics Committee from the then Research and Publications Office. The researcher abided by UNAM's rules of professional conduct obtained permissions from the Centre for Postgraduate Studies, and abided by the rules pertaining to ethical research. All data collected were used for research purposes only. Before completing the questionnaire, participating students provided their consent after the researcher had clearly explained the study's aims, the purposes of the data collected, and that they could decline to answer any question.

Participants' identities were kept anonymous in data the analysis process and in all reports so as to ensure participants' privacy. Any comments made in reports will not link to any participant so to ensure confidentiality. All data collected were encrypted and they will be kept securely in a locked office for five years after the research has been concluded and thereafter it will be destroyed. The full details of any weaknesses or

vulnerabilities in SMS communications that could be exploited by hackers or intruders were not disclosed publicly.

3.11 Chapter summary

The embedded mixed-method research design employed in this study was a success. Furthermore, the choice of Semi-structured interviews and questionnaires benefited the study with flexibility and ability to collect a large set of primary data. Moreover, the non-probability and the probability sampling techniques used in this study helped in attaining better representation.

Data analysis highlighted imperative information which proved to be relevant to the study. Additionally, descriptive statistics, regression and correlation aided the study to address its objectives. It is worth mentioning that research ethics were respected and adhered to throughout the study.

CHAPTER FOUR

RESULTS

4.1 Introduction

This chapter describes the results generated through preliminary interviews and survey questionnaires, and the results are presented through various statistical methods. The rest of this chapter is structured as follows: Section 4.2 presents the characteristics of the participants, followed by Section 4.3 which contains the participants' views on the prevalence of SMS security threats. After that, there are participants' awareness of SMS Security threats and multiple linear regression results in Section 4.4 and 4.5 respectively. The chapter continues with Section 4.6, which presents results from the binary logistic regression and ordinal logistic regression in Section 4.7, followed by focus group results in Section 4.8. The chapter then concludes with a chapter summary in Section 4.9.

4.2 Characteristics of the participants

Of the 287 respondents who participated in the study, the highest number of participants came from the Faculty of Economics and Management Science and the Faculty of Science as shown in Figure 4.1.

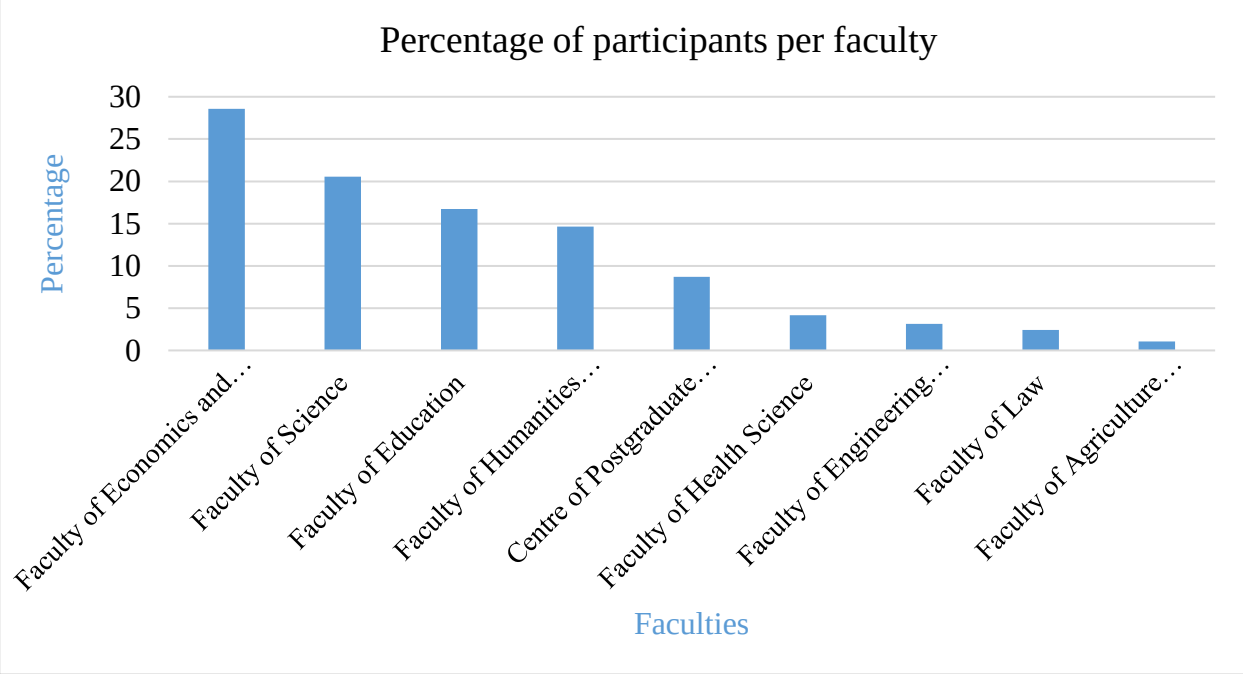


Figure 4.1 Distribution of participants by faculty

A few participants came from the Faculties of Engineering and Information Technology, the Faculty of Law as well as the Faculty of Agriculture and Natural Resources. This can be linked to the small size of these faculties and the small number of students.

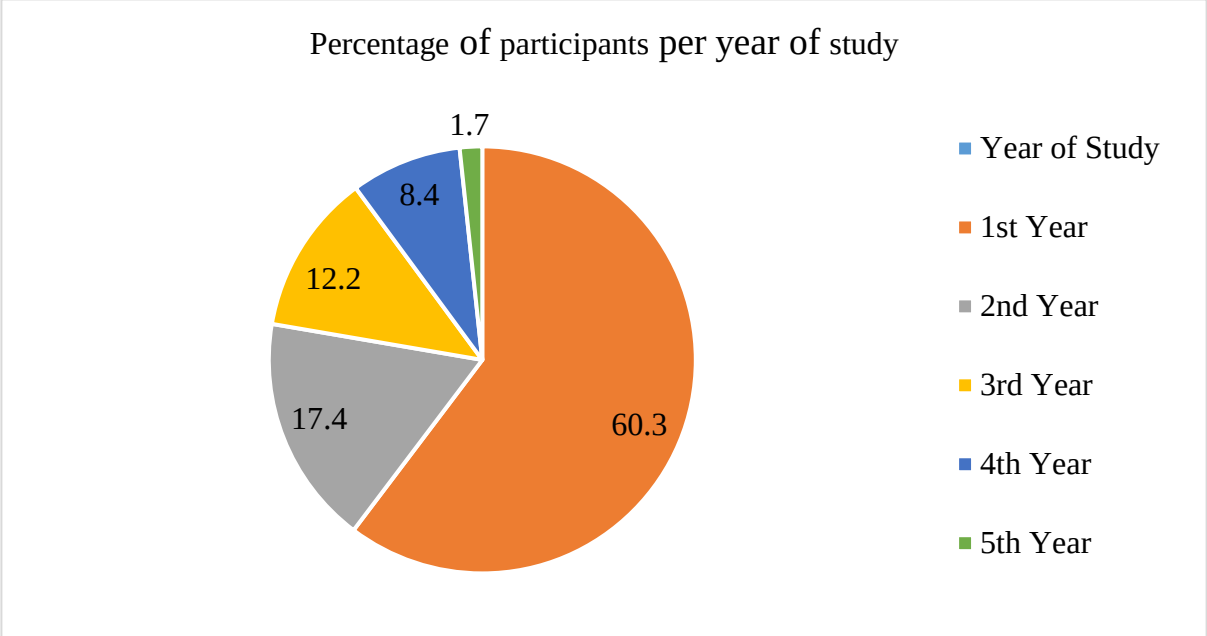


Figure 4.2 Distribution of participants by year of study

The majority of participants (60.3%) were first-year students and a substantial fraction was from second-year students as shown in Figure 4.2. Junior students felt more obliged to participate in the survey as compared to their senior counterparts.

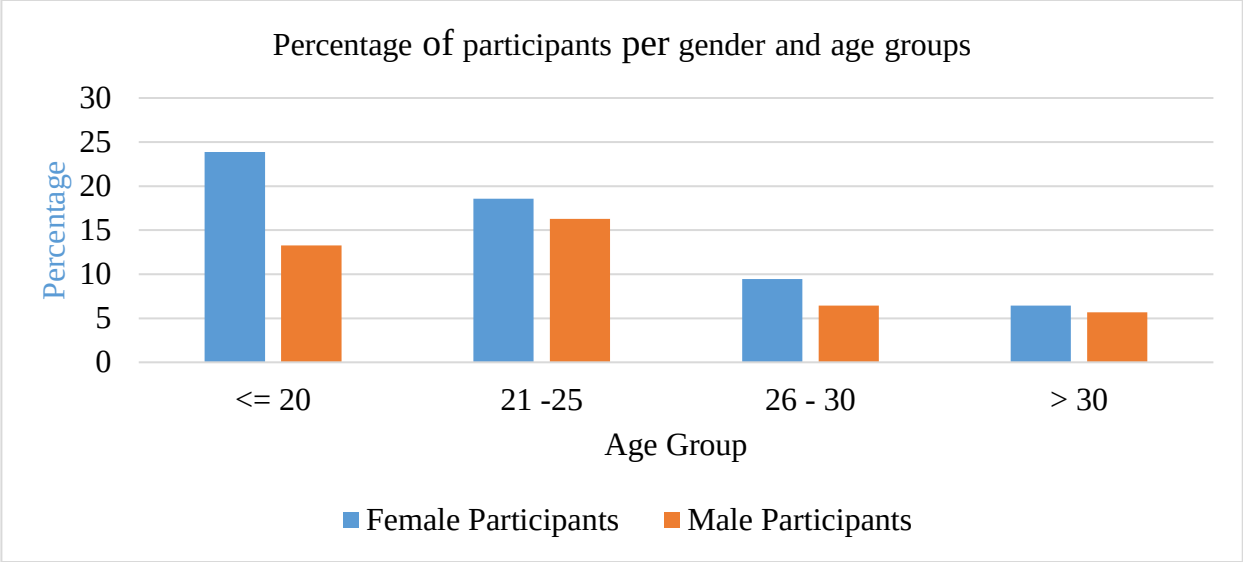


Figure 4.3 Distribution of participants by gender and age group

For the participants in the age group under 20 years, there were nearly twice the number of females as males as shown in Figure 4.3. This is because female students were more willing to participate in the survey as compared to their male counterparts.

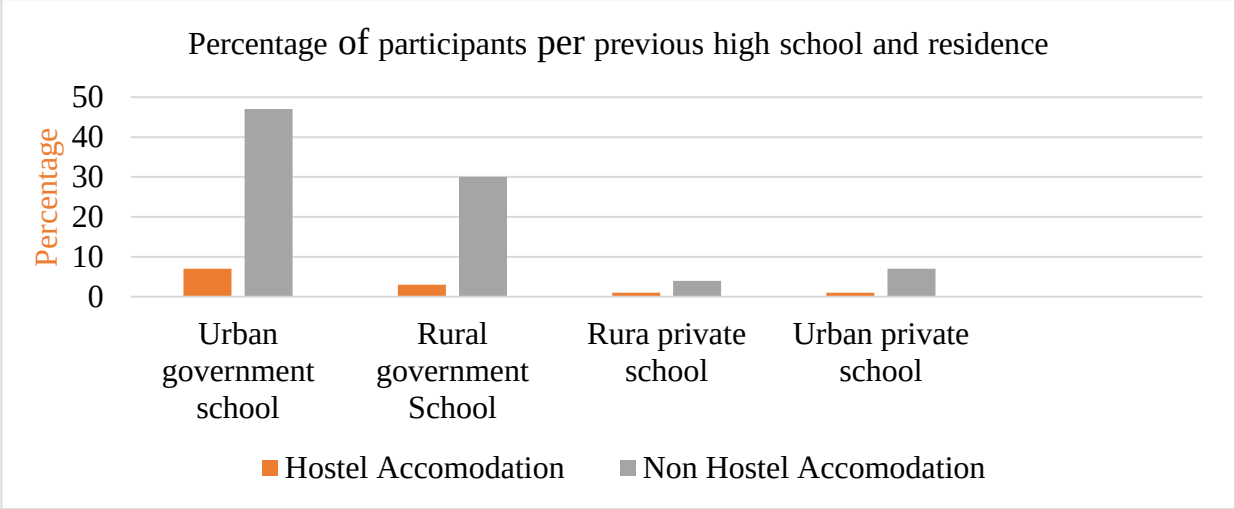


Figure 4.4 Distribution of participants by high school attendance and residency

Most participants had attended government schools, in urban areas (53%) and also rural areas (32%). A small fraction of participants had lived in hostel accommodation whilst at school as shown in Figure 4.4.

4.3 Participants' views on the prevalence of SMS security threats

Eighty percent (80%) of participants indicated that they have indeed received a threatening SMS. According to Zhang and Li (2015), students experiencing security incidents are more aware of security risks, hence 80% are more diligent due to past experiences.

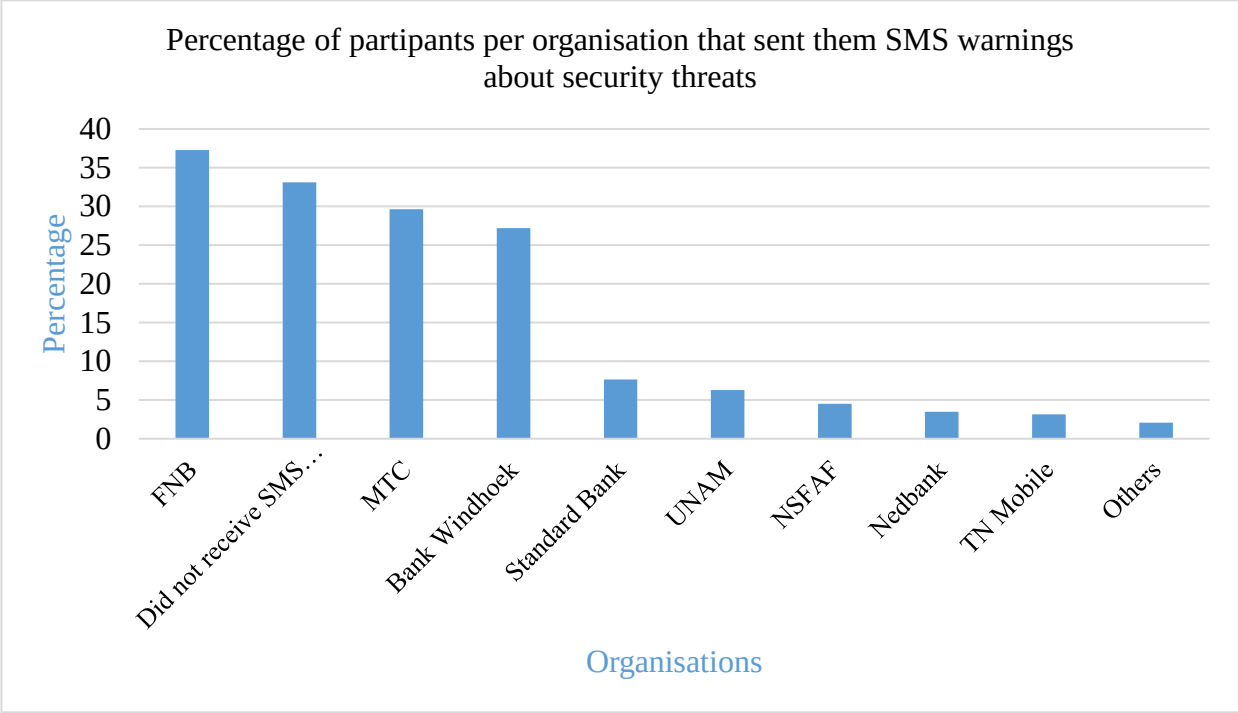


Figure 4.5 Distribution of participants per organisation that had sent them SMS warning threats in the past

While a significant percentage (33.1%) of participants indicated that they had never received any SMS threat warnings from any organisation, many participants indicated that a number of organisations, such as banks, and telecommunications operators had sent them SMS warnings about threats as illustrated in Figure 4.5. Over 35% of the participants were account holders at FNB bank and they indicated that they had received warnings. The telecommunications provider, MTC, had also sent warnings. Only 6.3% of the participants reported receiving warnings from the university.

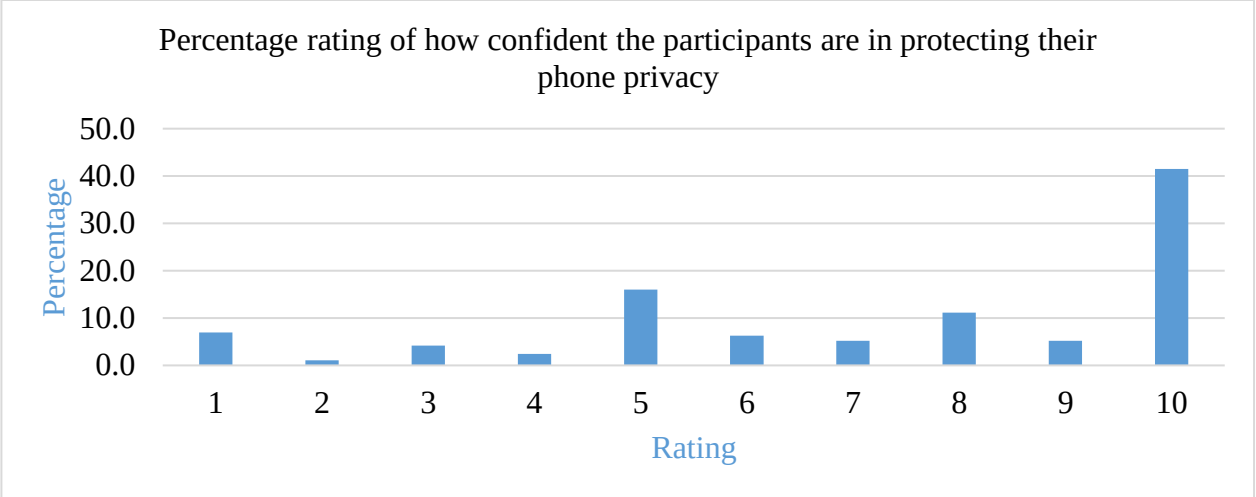


Figure 4.6 Participants' confidence with regards to how well they are protected, evaluated on a scale from 1 to 10

When asked to rate how confident they are that the information on their mobile is protected, the majority (41.5%) of respondents expressed that they were fully confident and 43.9% indicated that they were moderately confident as shown by Figure 4.6. A significant but small fraction (14.6%) indicated that they were less confident about the protection of information on their mobile phones.

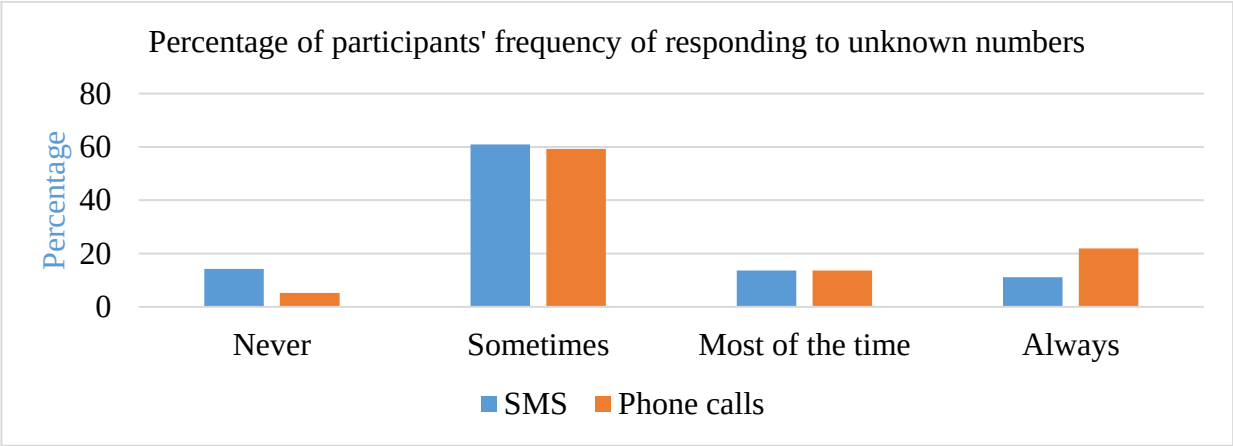


Figure 4.7 Participants' frequency of responding to unknown numbers by SMS or calls

A majority of participants (81%) said that they sometimes or always answered calls from unknown numbers as illustrated in Figure 4.7. An almost similar majority of participants

(79%) said that they sometimes or mostly respond to text messages from unknown numbers. Moreover, 14% of the participants indicated that they never respond to text messages from unknown numbers, while the remaining 11% acknowledged always responding to text messages from numbers they do not recognize.

4.4 Participants' awareness of SMS security threats

When asked if it is their first time being told about SMS security, 61.7% of the participants stated that it was their first time hearing about SMS security, while the remaining 38.3% stated that it was not their first time hearing about SMS security.

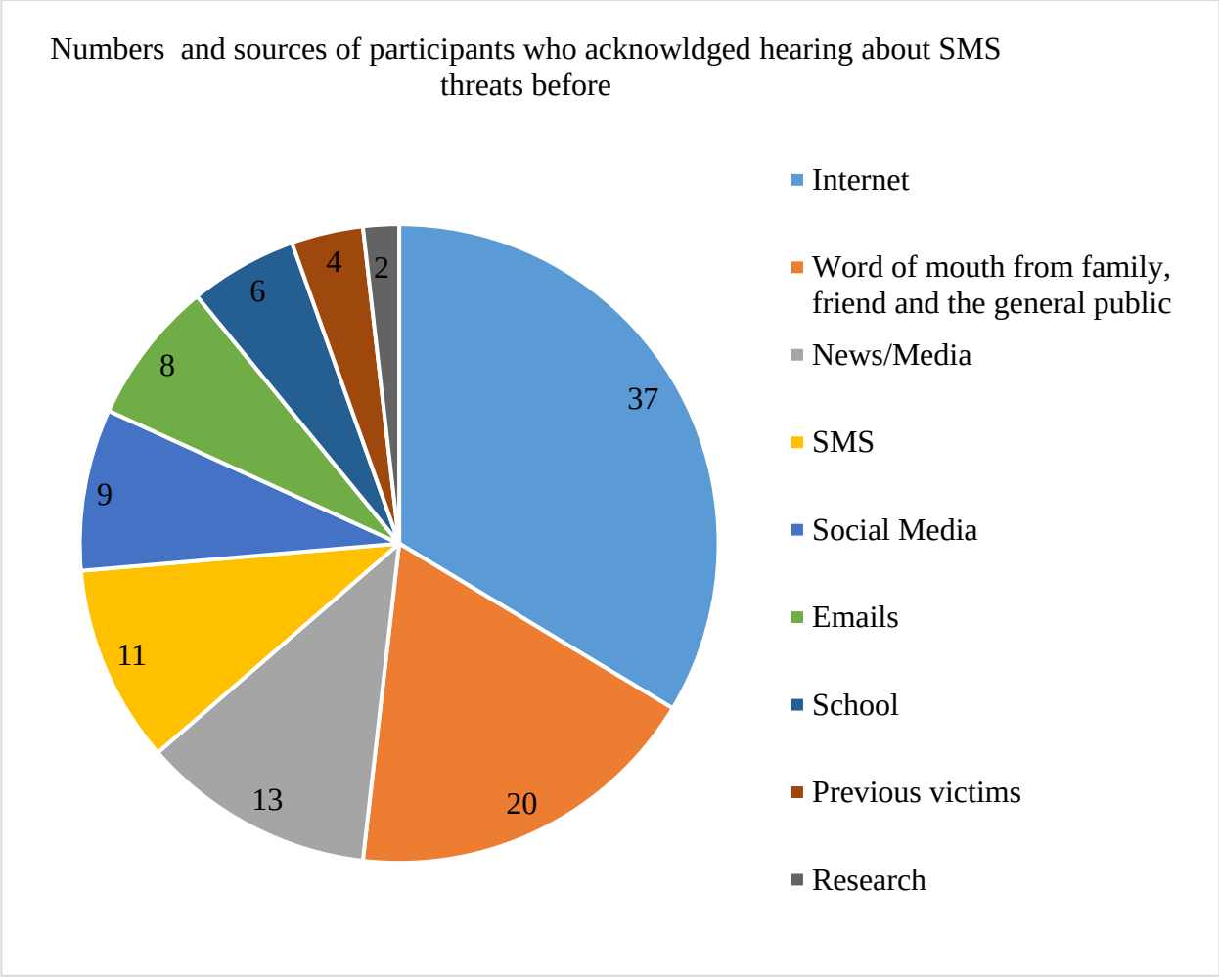


Figure 4.8 Participants' source of knowledge about SMS threats

Of the 38% who said that they already knew of SMS security threats, 37 participants stated that their knowledge came from the internet while 20 participants said that they gained the knowledge through word of mouth as illustrated in Fig 4.8. A small fraction noted that they became aware of it from news and the media, the SMS platform, social media, emails or information at school. A few participants (4) stated that they gained awareness because they had been victims or they had done their research to know about SMS security threats.

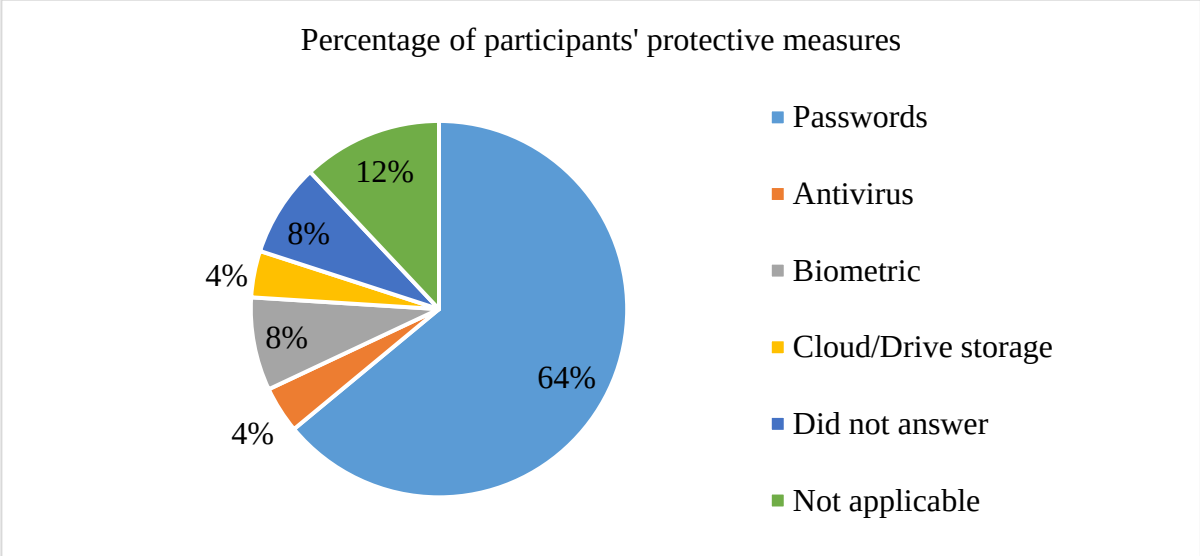


Figure 4.9 Distribution of protective measures used by participants

Sixty-four percent (64%) of the participants indicated that they use passwords on their devices as a means to protect information on their devices (Figure 4.9). Furthermore, 8% of the respondents stated that they use biometric security locks such as fingerprints and face recognition for protective measures. However, only 4% of the participants indicated that they use Antivirus software to protect the information on their mobile devices

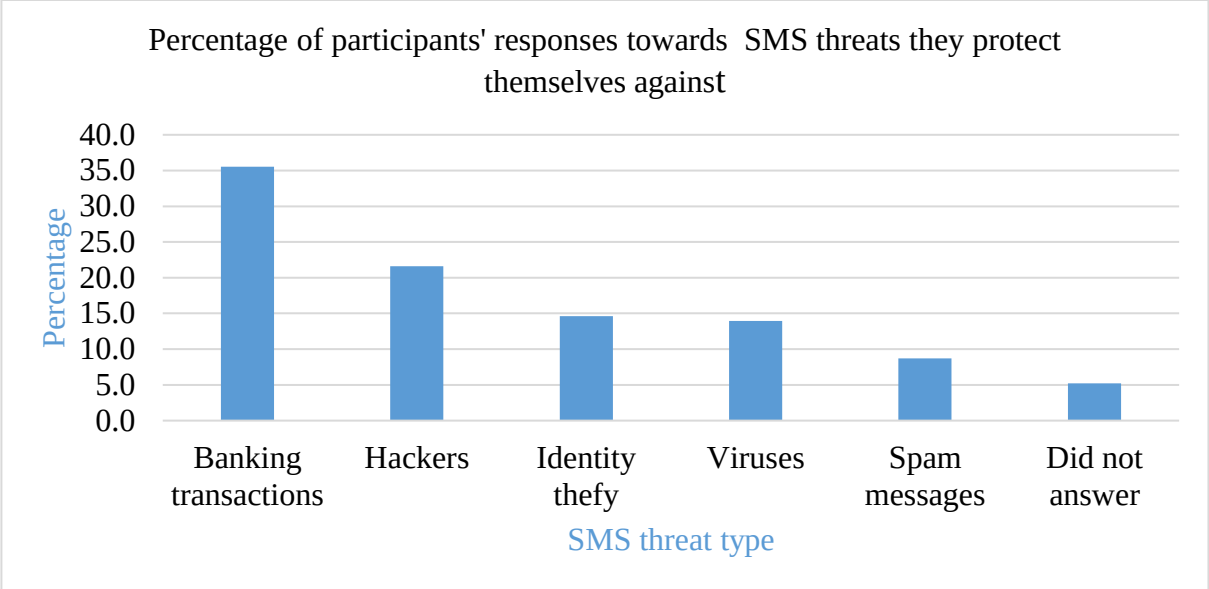


Figure 4.10 Distribution of types of SMS threats that led to protective measures

A high number of participants (57.1) indicated that they felt compelled to protect their information due to the fear of exposing personal banking information and due to the rise of hackers. Furthermore, identity theft, viruses and spam messages accounted for 37.2% of the reasons why participants used protective measures to protect their phones as illustrated in Fig 4.9.

4.5 Multiple linear regression

The participants were asked to indicate the period or duration that they have owned a mobile device. A multiple linear regression was run to predict participants' length with a cell phone from gender, age, residence, home language and previous high school. Generally, the model proved to offer the best fit (Table 4.1 and 4.2). The Deviance, AIC and BIC in Table 4.1 clearly demonstrated the model as a significantly fit as supported by the omnibus test (Table 4.2). Similarly, the Wald test results show the significance of each variable in the model.

Table 4.1. Multiple Linear Regression tables for participants' length with a cell phone

	Value	df	Value / df
Deviance	3283.944	267	12.299

Scaled Deviance	287.000	267	
Pearson Chi-Square	3283.944	267	12.299
Scaled Pearson Chi-Square	287.000	267	
Log Likelihood	-756.991		
Akaike's Information Criterion (AIC)	1555.981		
Finite Sample Corrected AIC (AICC)	1559.468		
Bayesian Information Criterion (BIC)	1632.830		
Consistent AIC (CAIC)	1653.830		

Dependent Variable: How long had a cell phone

Model: (Intercept) gender, age, residence, home language, previous high school

a. Information criteria are in the smaller-is-better form

b. The full log likelihood function is displayed and used in computing information criteria

Table 4.2 Omnibus Test[a]

Likelihood Ratio Chi-Square	df	Sig.
148.661	19	0.000

Dependent Variable: How long had a cell phone

Model: (Intercept) gender, age, residence, home language, previous high school

Compares the fitted model against the intercept-only model

Here, the chi-square is highly significant (chi-square =148.7, df = 9, $p < 0.000$) so our new model is significantly better.

Table 4.3 Tests of Model Effects

Source	Type III		
	Wald Chi-Square	df	Sig.
(Intercept)	50.252	1	.000

Gender	.007	1	.932
Age	166.802	4	0.000
Residence	2.575	2	.276
Home Language	6.090	8	.637
Previous High School	4.919	4	.296

Dependent Variable: How long had a cell phone

Model: (Intercept) gender, age, residence, home language, previous high school

Among all variables tested using multiple linear regression on the length of period with a cell phone, age was the only variable that was significant for $p < 0.05$. The results in Table 4.4 further reveal that participants under 20 years of age and participants aged between 20 years and 25 years of age used cell phones for 6.1 years and 4.3 years lesser than participants aged between 26 years and 30 years of age. Furthermore, participants over 30 years of age used cell phones for 1.8 years longer than participants aged between 26 years and 30 years of age.

Table 4.4 Parameter estimates

Parameter	B	Std. Error	95% Wald Confidence Interval		Hypothesis Test		
			Lower	Upper	Wald Chi-Square	df	Sig.
(Intercept)	13.561	1.2526	11.106	16.016	117.204	1	0.000
[Gender = Female]	-0.036	0.4254	-.870	.798	.007	1	0.932
[Gender = Male]	0[a]						
[Age=]	-2.303	0.8874	-4.043	-.564	6.738	1	0.009
[Age = Age <= 20]	-6.093	0.6477	-7.362	-4.823	88.480	1	0.000
[Age = Age 21 to 25]	-4.267	0.6420	-5.525	-3.008	44.167	1	0.000
[Age = Age 26 to 30]	0[a]						
[Age = Age > 30]	1.769	0.8183	0.165	3.373	4.674	1	0.031
[Residence =]	-3.920	3.4762	-10.734	2.893	1.272	1	0.259

[Residence = Hostel Accommodation]	-.784	.6719	-2.101	.532	1.363	1	0.243
[Residence = Non-Hostel Accommodation]	0[a]						
[Home Language =]	.905	1.4512	-1.939	3.749	.389	1	0.533
[Home Language = Afrikaans]	1.201	1.1110	-.976	3.379	1.169	1	0.280
[Home Language = English]	.594	1.1319	-1.625	2.812	.275	1	0.600
[Home Language = Nama/Damara]	.651	1.3667	-2.028	3.330	.227	1	0.634
[Home Language = Oshiwambo]	-.048	.9426	-1.896	1.799	.003	1	0.959
[Home Language = Other]	2.409	1.6464	-.818	5.636	2.141	1	0.143
[Home Language = Otjiherero]	.017	1.1663	-2.269	2.303	.000	1	0.988
[Home Language = Rukavango]	.590	1.2526	-1.865	3.045	.222	1	0.637
[Home Language = Silozi]	0[a]						
[Previous High School =]	-2.955	2.3262	-7.514	1.605	1.613	1	0.204
[Previous High School = Rural Government School]	-.964	.8259	-2.582	.655	1.361	1	0.243
[Previous High School=Rural Private School]	-2.098	1.1074	-4.269	.072	3.591	1	0.058
[Previous High School = Urban Government School]	-.749	.7705	-2.259	.761	.945	1	0.331
[Previous High School = Urban Private School]	0[a]						
(Scale)	11.442[b]	.9552	9.715	13.476			
(Intercept)	13.561	1.2526	11.106	16.016	117.204	1	0.000
[Gender = Female]	-.036	.4254	-.870	.798	.007	1	0.932

Dependent Variable: How long had a cell phone

Model: (Intercept) gender, age, residence, home language, previous high school

a. Set to zero because this parameter is redundant

b. Maximum likelihood estimate

4.6 Predicting the likelihood of receiving threatening SMS from gender, age and home language

Binary logistic regression was fitted to estimate and predict the likelihood of ever receiving a threatening SMS from gender, age and home language. However, none of the variables tested using binary logistic regression was significantly associated with ever receiving a threatening SMS at $p < 0.05$ (Table 4.5).

Table 4.5 Parameter estimates for binary logistic regression

			95% Wald Confidence Interval		Hypothesis Test				95% Wald Confidence Interval for Exp(B)	
Parameter	B	Std. Error	Lower	Upper	Wald Chi-Square	df	Sig.	Odds Ratio	Lower	Upper
(Intercept)	2.577	1.1178	.386	4.768	5.313	1	0.021	13.153	1.471	117.637
[Gender = Female]	.220	.3179	-.403	.843	.480	1	0.488	1.246	.668	2.324
[Gender = Male]	0[a]							1.00		
[Age =]	.760	.8557	-.918	2.437	.788	1	0.375	2.137	.399	11.435
[Age = Age <= 20]	.059	.5099	-.940	1.058	.013	1	0.908	1.061	.391	2.882
[Age = Age > 30]	-.489	.5881	-1.641	.664	.690	1	0.406	0.613	.194	1.942
[Age = Age 21 to 25]	-.304	.4940	-1.272	.664	.378	1	0.539	0.738	.280	1.943
[Age = Age 26 to 30]	0[a]							1.00		
[Home	-.876	1.3017	-3.427	1.675	.453	1	0.501	0.417	.032	5.341

Language =]										
[Home Language = Afrikaans]	-1.751	1.1283	-3.962	.461	2.407	1	0.121	0.174	.019	1.585
[Home Language = English]	-1.033	1.1775	-3.340	1.275	.769	1	0.380	0.356	.035	3.579
[Home Language = Nama/Damara]	-.328	1.4819	-3.233	2.576	.049	1	0.825	0.720	.039	13.149
[Home Language = Oshiwambo]	-1.201	1.0631	-3.285	.882	1.277	1	0.258	0.301	.037	2.416
[Home Language = Other]	-1.772	1.3599	-4.437	.893	1.698	1	0.193	0.170	.012	2.444
[Home Language = Otjiherero]	-.778	1.2200	-3.169	1.614	.406	1	0.524	0.460	.042	5.021
[Home Language = Rukavango]	-1.585	1.1891	-3.915	.746	1.776	1	0.183	0.205	.020	2.108
[Home Language = Silozi]	0[a]							1		
(Scale)	1[b]									

Dependent Variable: Have you ever received a threatening SMS?

Model: (Intercept) gender, age, home language

a. Set to zero because this parameter is redundant

b. Fixed at the displayed value

4.7 Estimation of the frequency of receiving threatening SMS from gender and age

Parameter		B	Std. Error	95% Wald Confidence Interval		Hypothesis Test			Exp(B)	95% Wald Confidence Interval for Exp(B)	
				Lower	Upper	Wald Chi-Square	df	Sig.		Lower	Upper
Threshold	How frequently do you receive threatening SMS =										
	[1.0]	-0.449	0.795	-2.007	1.109	0.319	1	0.572	0.638	0.134	3.032
	[2.0]	0.886	0.8078	-0.697	2.47	1.204	1	0.273	2.426	0.498	11.817
	[3.0]	1.895	0.8542	0.221	3.569	4.921	1	0.027	6.653	1.247	35.491
	[4.0]	2.232	0.8813	0.505	3.96	6.416	1	0.011	9.321	1.657	52.432
	[5.0]	2.69	0.9307	0.866	4.514	8.355	1	0.004	14.735	2.377	91.326
	[6.0]	4.154	1.267	1.671	6.637	10.749	1	0.001	63.69	5.316	763.054
Gender = Female		0.641	0.5197	-0.378	1.659	1.52	1	0.218	1.898	0.685	5.255
Gender = Male		0a	.	.	.	.	.	.	1.00	.	.
Age <= 20		-0.222	0.8811	-1.949	1.505	0.064	1	0.801	0.801	0.142	4.502
Age 21 to 25		0.009	0.8526	-1.662	1.681	0	1	0.991	1.009	0.19	5.369

Age 26 to 30		0a	.	.	.	.	.	.	1.00	.	.
Age > 30		-0.367	0.9337	-2.197	1.463	0.154	1	0.694	0.693	0.111	4.319
(Scale)		1c									

Furthermore, ordinal logistic regression was fitted to estimate and predict the frequency of receiving a threatening SMS from gender and age. However, both variables tested using ordinal logistic regression were not significant for $p < 0.05$. Results provided in Table 4.6 also show that the chance of receiving a threatening SMS increased with the frequency of use with a threshold value of -0.449 at level 1 and increased to 4.154 at level 6.

Table 4.6: Parameter estimates for ordinal logistic regression table for the frequency of participants receiving threatening SMS

Dependent variable: How frequently do you receive threatening SMS?

Model: (Threshold) gender, age

a Set to zero because this parameter is redundant

b Set to system missing due to overflow

c Fixed at the displayed value

4.8 Focus group results

This section discusses different uses of SMS and experiences that participants had encountered with SMS usage in the past. Furthermore, participants' knowledge of different terms used in cyber security is discussed.

As for SMS usage, participants confirmed that they use SMS on a daily basis to accomplish some of their daily chaos.

When you can't answer a call then you reply with an SMS, say I am in class. (Participant 2, male, 23 years old, 4th-year student)

And you can also help someone with their assignment, answer questions through SMS or doing group work. (Participant 4, female, 25 years old, 5th-year student)

Chatting and making people aware, maybe someone was robbed on campus then you circulate an SMS around. And mostly we use SMS in cases where we don't have enough

credit, so if you don't have enough credit to call the person an SMS is cheaper it is just 40c, so we use that SMS to contact that person instead of calling or borrowing other people's phones. (Participant 6, female, 23 years old, 3rd year student)

It is important when you have for instance FNB, you register for cell phone banking, immediately when you withdraw money, it will report on your phone or in case if you lose your bob card (ATM Card) if someone withdraws money, it will report on your phone. Or in case you go to town and you have left your card, you can withdraw money, just request the amount you want to withdraw then they give you a Pin. (Participant 5, male, 18 years old, 1st year student)

With regards to the use of SMS, there were security threats that were known by the participants. Additionally, participants explained some useful methods they have used to safeguard themselves from such security threats.

Yes, there was that incident where you get a text from a certain number and if you dial it, it will eat up your money, you don't remember (asking others), I think it was at the beginning of the year. MTC also circulates that if they call you and ask, because they call you and confirm all your details and Pin. You should not do it. (Participant 6, female, 23 years old, 3rd year student)

And also your phone is not safe, the phone can be stolen and there are important documents in my phone, people with technology nowadays can hack into your phone and whatever is there, they can expose it to public. Even right now ne, if you go to the computer centre up there, where the 4th year Lab is, people there, I don't know what they do, they just hack your phone. (Participant 1, female, 22 years old, 2nd year student)

Once my friend's phone was hacked and it just started doing funny things. And especially now with WhatsApp, there is that WhatsApp web scanner mos, I can take her phone and go in WhatsApp and then scan her code, and then whenever she receives a message, I am also receiving it. (Participant 1, female, 22 years old, 2nd year student)

So many problems, especially SMS, a person can forward SMS from your phone to their phones. I can screenshot if I have a smartphone and send it to myself still. Usually, I can even forward it. (Participant 2, male, 23 years old, 4th-year student)

There was even a time we were also told not to save our parents numbers as mom or dad, if someone snitches your phone, they can tell your mom saying Mom e-wallet me money. (Participant 3, female, 19 years old, 1st year student)

Protective measures

But there is an app like on my phone. I have vault, and if I know that I don't want people to read messages that I get from her (pointing to her neighbour) I put her number on vault, so the message just go straight to vault, it doesn't display on the phone. Even like my pictures and every private things that I don't need people to know are in vault, the rest I can give you my phone. Because the moment you try to go into my vault it takes a picture of you and then it sent it via my e-mail and it says this person is trying to log in, because you also don't know my password. (Participant 5, male, 18 years old, 1st year student)

Technical terms around cybersecurity

Phishing? It's a first time. (Participant 4, female, 25 years old, 5th year student)

We only know of hacking. (Participant 1, female, 22 years old, 2nd year student)

We have never heard about it before, snitching yes but not smishing. (Participant 2, male, 23 years old, 4th year student)

All I know is if you can't find an e-mail it can be at the spam box. (Participant 6, female, 23 years old, 3rd year student)

It is just like being a victim and is like when I don't have a password on my phone then I am vulnerable. (Participant 3, female, 19 years old, 1st year student)

We learned two words, phishing and smishing. (Participant 2, male, 23 years old, 4th year student)

Maybe if you go to computer science students they will understand. (Participant 1, female, 22 years old, 2nd year student)

All participants in the focus group suggested that more awareness campaigns on SMS related security threats among students are needed to help protect them against such

threats. In the same vein, 50% of the participants suggested that UNAM management should take it upon itself to run such awareness campaigns in an effort to reach out to UNAM's entire student population. Moreover, one of the participants suggested that a basic cyber security course be introduced at UNAM and be made compulsory for all UNAM students. The participant suggested that this would enrich all students with knowledge about security threats and help them to be vigilant. The idea was supported by the whole group, saying that an aware and knowledgeable student will be more likely to get adapted to safety habits and be able to protect themselves from different security threats most of the times.

4.9 Chapter summary

All participants had used a cell phone for some time. Furthermore, many participants were aware of the security threats associated with the use of SMS. However, there is a gap in knowledge with regards to what to do and to what extent to go to protect yourself from SMS security threats. The key findings point to three distinct areas, firstly, awareness of SMS security threats, secondly, lack of awareness programmes from educational institutions and lastly, inadequate knowledge of protective measures to protect oneself. Most participants (72%) use basic security measures on their phones, such as passcodes, patterns, and biometric access, but did not use antivirus software to protect against unauthorised remote access, or the insertion of malware or spyware. Only 5% of participants indicated that they had heard about SMS security threats from schools, thereby suggesting educational institutions' lack of awareness or that they are unable to teach students about cybercrimes and cyber security. Only 14% of participants indicated that they had never responded to text messages from numbers they do not recognise. Moreover, there was a significant link between the length with the cell phone and participants' age.

CHAPTER FIVE

DISCUSSION

5.1 Introduction

This brief chapter discusses the findings about the University of Namibia's students' awareness of SMS security threats and the avoidance measures in relation to the literature, and variations amongst students related to their characteristics or demographics. Based on the findings, the chapter also considers interventions that can increase students' protection. The rest of the chapter is structured as follows: Section 5.2 presents how low awareness of security threats may reflect infrequent access, followed by Section 5.3 on Namibian students' low use of protective security measures. Furthermore, Section 5.4 gives the interventions required. The chapter concludes with Section 5.5 which is a chapter summary**.**

5.2 Low awareness of security threats may reflect infrequent access

In 2019, most (97%) respondents had not previously heard of any specific security threats associated with the use of SMS, and 62% indicated that the questionnaire represented the first time they had been told about SMS security threats. This is consistent with findings that suggest that SMS security awareness amongst students elsewhere in Africa was lower at around that time than in Asia, Europe and North America (Bada et al., 2018). For instance, Sari (2014) found that 80% of Indonesian smartphone users were aware of information security. In some countries such as Jordan, students' awareness of security threats targeting mobile phones is lower than their awareness of security threats and procedures that target computers (Taha & Dahabiyeh, 2021). However, reflecting on their study of cyber security awareness in Botswana, South Africa, Nigeria, Ghana, Kenya and the Democratic Republic of Congo, Bada et al. (2018) propose that low ICT literacy rates and a lack of national cyber security awareness programmes contribute to a lack of awareness. Given the fact that the Namibian students surveyed had some ICT literacy and adopted basic measures to protect their privacy by restricting physical access to their devices, it is proposed that their comparatively low awareness of SMS security threats might reflect barriers to frequent use of phones.

The majority (81%) of respondents had owned a mobile phone for at least 6 years, and 29% said that they had owned a mobile phone for more than 12 years. Exposure to and awareness of, SMS- related security threats, however, will relate to the frequency of phone use as well as the duration of ownership. At the time of the study, mobile networks barely covered rural populations, who comprise of half of Namibia's population (World Bank 2016), and some 76% of rural dwellers also lived without electricity (Government of Namibia 2017). Indeed, in 2020, LTE infrastructure increased from 40% to 79% of population coverage by area, which contributed to an 8.5% increase in mobile broadband subscriptions (Lancaster, 2022). While there are now around 1.877 million mobile broadband subscriptions (equivalent to 74% of the population) (Lancaster, 2022), this would not have been indicative of the years leading up to the study. Indeed, in 2018 the full use of mobile services was a reality only for the richest 20% of the population (A4AI, 2018). Garba et al. (2020) found that Nigerian students arriving at university from rural backgrounds had less awareness of security issues. However, in the current study, there was no significant difference in awareness found for the 55% and 33% of students who attended urban and rural public high schools, respectively. It is possible that the additional challenges for people from rural areas to attend university mean that those who do are likely to have also been those in rural areas who have greater exposure. It is also likely that students' awareness relates to how long they have been at university, since low awareness is directly proportional to the distribution of participants' year of study, and the first-year and second-year students accounted for 77.7% of the respondents. A study in Nigeria found greater awareness of SMS related security threats amongst senior rather than junior students (Garba et al., 2020).

5.3 Namibian students' low use of protective security measures

Ngoqo and Flowerday (2015) in their study at Fort Hare University revealed that mobile users with low or natural levels of information security awareness are prone to make bad security decisions. While respondents widely used measures to constrain physical access to their phones such as passcodes, patterns and biometric recognition, very few (4%) indicated that they use antivirus to protect the information in their mobile devices. This compares with findings about students on three campuses of a private tertiary institution

in South Africa, Kwazulu Natal Province (Chandarman & Van Niekerk, 2017). In the South African study, 43% of students did not know the correct purpose of antivirus software, which contrasts with a study in colleges in major cities of Tamil Nadu, India, where over 70% of students were much aware of basic virus attacks and used antivirus as a countermeasure (Senthilkumar & Easwaramoorthy, 2018).

More than 80% of respondents in this study respond to SMSs from numbers they do not recognize. However, responding in ways that expose users to security risks does not simply reflect whether or not users are aware of the risks. Using the example that a few of the 70% of South African users who know that they should regularly change their passwords actually do so, Chandarman and Van Niekerk (2017) argue that knowledge does not necessarily translate into good practice. In their study in Kwazulu Natal Province, they found that while students might be aware of some SMS security threats, they might not know all associated security risks and all the necessary security practices. Likewise, Calderwood and Popova (2019) found that even though 84% of Thai students displayed a high level of awareness of security threats, 82% of students using smartphones always or sometimes click on links in phishing emails.

5.4 Interventions required

Bada et al. (2018) suggest that much needs to be done in Africa so as to increase security awareness and advocates for integrating cyber security awareness efforts into ICT literacy courses as part of the curriculum. Only 4% of respondents to the questionnaire indicated that they had heard about SMS security threats from school. Indeed, all six participants in the formative focus group suggested that campaigns raising awareness about SMS related security threats among students were needed to help protect them. Half indicated that UNAM's management should specifically run awareness campaigns to target the entire student population and one participant suggested that UNAM should introduce a mandatory basic course to expand students' knowledge about cyber security threats and help them to be vigilant. All participants in the group agreed that more aware and knowledgeable students would develop safety habits to protect themselves from different security threats most of the time. It is notable that suggestions for the university to implement cybersecurity awareness campaigns and training indicated that this should

not be delivered via phones per se. They remarked that the communication medium used should be the ones that students are most familiar with and use regularly, such as the portal, the institution's website and e-mails.

5.5 Chapter summary

The findings suggest that Namibian educational institutions, such as the University of Namibia, should promote cyber security awareness and contribute to educating their populations. The Namibian government has been active in recent years to encourage telecommunications companies to increase the accessibility of mobile phone networks. However, prior lack of access amongst the population contributes to a legacy of lack of awareness about evolving cyber threats and the need and know-how to install antivirus software on mobile devices, which will make it difficult for the government to curb cyber-crimes. Furthermore, without cyber security awareness programmes, it would be difficult for the government to curb the issue of cyber security. Thus, individuals should be encouraged to be proactive when it comes to combating cybercrimes. Everyone is required to make efforts to use protective measures against SMS security threats as well as to educate others about such threats, as this will limit the number of victims.

CHAPTER SIX

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

6.1 Overview of the study

This study explored students' awareness of security threats that are related to SMS. The main research objective sought to determine the awareness level of SMS security threats amongst students at UNAM, and interventions that can reduce their exposure. This comprised of three sub-objectives. This study explored students' awareness of security threats that are related to SMS. The main research objective sought to determine the awareness level of SMS security threats amongst students at UNAM, and interventions that can reduce their exposure. This comprised of three sub-objectives.

RO1 addressed the characteristics and the prevalence and levels of risk associated with SMS security threats that students are exposed to.

The literature showed that SMS traffic volume has remained constant in Namibia, between 9.5 and 10.5 million messages annually since 2013 (Mobile Telecommunications Company, 2020). Furthermore, there was a sharp rise in SMS traffic from 2011-2013 with an increase of over 10 million text messages annually. As of 2013 the figures have not significantly dropped (Mobile Telecommunications Company, 2020).

Other literature revealed that SMS lacks the basic elements of security, including confidentiality, integrity and endpoint authentication, and as such, security threats are prevalent, which impacts mobile phone subscribers daily (Tu, Li, Peng, Li, & Lu, 2016). Moreover, it is argued that some threats, such as denial-of-service (DoS) and some types of interception do not require their victims to do anything. Others, including SMS spoofing and phishing, involve manipulation, whereby an attacker uses "social engineering" to trick the victim in some way (Hadnagy & Schulman, 2021).

The current study revealed that the Namibian government has been active in recent years to encourage telecommunications companies to increase the accessibility of mobile phone networks. However, prior lack of access amongst the population contributes to a legacy of lack of awareness about evolving cyber threats and the need and know-how to

install antivirus software on mobile devices, which will make it difficult for the government to curb cyber-crimes. Therefore, at the time of this study, students at university of Namibia were exposed to high risks from security threats associated with their use of SMS.

RO2 dealt with students' awareness of SMS security threats and avoidance measures, and how variations amongst students relate to their characteristics or demographics.

It is opined that university students who use mobile phones for longer periods are more exposed to and thus tend to be more aware of SMS-related security threats (Garba et al., 2020). Additionally, a study in Nigeria found greater awareness of SMS related security threats amongst senior rather than junior students (Garba et al., 2020). Regardless of the length of time, they have owned a mobile phone, students who use their mobile phones less frequently are likely to be less aware of SMS-related security threats.

Some scholars proffer that students from urban areas in Nigeria are more aware of SMS security threats than those from rural areas (Garba et al., 2020), which might reflect the frequency of use, and it has been found that computer science students become more aware of mobile technology security risks, including those related to SMS, as they progress through their studies. However, often computer science programmes are gendered, for instance with regards to the Nigerian students, mostly aged 21-25 years, comprising 90% of men (Garba et al., 2020).

In the same vein, Nhinda and Shava (2021) argue that rural Africans suffer from cybersecurity risks as a result of low cybersecurity awareness. Namibian students from rural backgrounds might also fall victim to the same trend.

However, in the current study, there was no significant difference in awareness found for the 55% and 33% of students who attended urban and rural public high schools, respectively. It is possible that the additional challenges for people from rural areas to attend university mean that those who do are likely to have also been those in rural areas who have greater exposure. It is also likely that students' awareness relates to how long they have been at university, since low awareness is directly proportional to the

distribution of participants' year of study, and the first-year and second-year students accounted for 77.7% of the respondents.

Furthermore, in Thailand, 84% of student smartphone users surveyed displayed a high level of awareness as they indicated that they always pay attention to permissions asked by the applications that they download, protect themselves from spyware and were concerned about privacy (Calderwood & Popova, 2019). However, despite their awareness, most students (82%) said that they sometimes clicked on links in phishing emails (Calderwood & Popova, 2019). Similarly, some 60% of college students surveyed in major cities in Tamil Nadu, India, had received phishing emails or messages, and while a few responded to phishing emails/messages, 11% had been victims of virus attacks (Senthilkumar & Easwaramoorthy, 2018). In other literatures, some of the Indian students use countermeasures, such as antivirus software. However, students tend to be more aware of security threats that target computers. For instance, only 38% of university students in Jordan were aware of threats targeting phones, and 56% believed that it is more likely that their computers would be affected by malicious programmes (Taha & Dahabiyeh, 2021).

The current study tent to differ because low awareness of security threats among students were found. The know how and usage of antivirus software by students were also significantly low, at 4% of the respondents.

RO3 addressed the interventions that can increase students' protection.

It is estimated that private and public sector investment in raising citizen's and employees' awareness can reduce cyber-attacks from 70% to 45% (Nick, 2021). The importance of increased awareness of security threats is illustrated by print and broadcast media campaigns around the world. However, more attention tends to be paid to raising awareness of computer and internet threats, and less on how easy it is to intercept SMS messages. Indeed, while 61% of corporate users are aware of what phishing is, only 30% know about smishing techniques (Chickowski, 2020).

It is argued that awareness of threats does not necessarily translate into practising prevention. While this can be because people lack knowledge about security devices, it

can also be due to complacency (Gupta et al., 2018). For instance, while 70% of South African users surveyed knew that they should regularly change their passwords, only 23% actually do (Chandarman & Van Niekerk, 2017) and only 28% used Two Factor Authentication (2FA) on their accounts (Chandarman & Van Niekerk, 2017). Similarly, while Indonesian users were aware of threats, non-adherence to security policies can reflect a lack of time to read all the items in a security policy (Sari, 2014).

A study by Chandarman and Van Niekerk (2017) on three campuses of a private tertiary education institution in KwaZulu Natal, South Africa, indicated that, while they might be aware of some SMS security threats, students do not know about all the security risks and necessary security practices. The sampled population included first-year students and senior students over two semesters using online and paper-based questionnaires and found that 56% of the students did not correctly know about phishing and 43% of the students did not correctly know about the purpose of anti-virus software. Other scholars suggests that student mobile phone users at a university in the Eastern Cape, South Africa, had low levels of information security awareness and as such, they are prone to make bad security decisions (Ngoqo & Flowerday, 2015a).

This agrees with this study's findings. The study found that students lacked awareness about evolving cyber threats and the importance and know-how to install antivirus software on mobile devices. Furthermore, without cyber security awareness programmes, it would be difficult to curb the issue of cyber security. Thus, individuals should be encouraged to be proactive when it comes to combating cybercrimes. Everyone is required to make efforts to use protective measures against SMS security threats as well as to educate others about such threats, as this will help to limit the number of victims. This thesis presented the study as follows:

Chapter 1 sketched the background of the research problem by asserting the problem, identifying the research objectives, and introducing the research approach.

Chapter 2 summarised literature relating to the prevalence of SMS, the use of SMS by university students, the types of SMS threats, as well as the levels of SMS awareness globally. This literature informed the creation of a theoretical framework for the research.

Chapter 3 discussed the research design and methods to collect and analyse data, the instruments and the research methods. It described the preliminary interviews that informed the design of a survey of students. The chapter discussed and examined the reasoning for the research design and methodology. The sample area and the population of the study were described.

Chapter 4 presented the outcomes and results from preliminary interviews and the research questionnaire. Some of the results were presented using graphs, tables and diagrams to achieve clarity.

Chapter 5 presented the results of the study, and its statistical analyses and interpretation.

Chapter 6 drew conclusions from the key findings, and made some recommendations.

The rest of this chapter is structured as follows: Section 6.2 presents the conclusions, followed by the recommendations in Section 6.3. The chapter concludes with the limitations of the study and recommendations for future research in Section 6.4.

6.2 Conclusions

The use of basic security measures such as passcodes, patterns, and biometric access, by most students in the sample, acknowledged the reality of security threats about their mobile devices. However, regardless of whether or not they are aware of SMS threats specifically, most of the students do not take preventative measures such as installing anti-virus software on their mobile devices. This suggests that the situation in Namibia is consistent with Chandarman and Van Niekerk's (2017) study in South Africa, which found that while students in higher education are not ignorant of security concerns regarding smartphones, they are also not fully aware of all the security risks and the necessary security practices. The study revealed that students show more fear towards the security incidents reported in the media despite the fact that their vulnerability to the threat can be limited (Sarathchandra, Haltinner, & Lichtenberg, 2016). UNAM students indicated that several organisations notified them to be wary of fraudulent activities. However, the university was one of the least that sent students warning notifications about fraudulent activities. Students also considered that the university should take

responsibility to raise student awareness with regards to SMS security threats and protections. However, for effective protection, students must have sufficient technology literacy for them to use protective measures.

The study found that while students may know of SMSs threats, they do not know how to counter these threats. Most students do not have extensive knowledge about the types of fraudulent activities such as phishing, spamming, DoS attacks, reply attacks, and social engineering. This suggests that the institution should ensure that security awareness is linked to technological literacy as part of the curriculum, while also promoting a security-minded culture.

Students were surveyed in 2019 and, since then, geographical coverage by mobile networks has significantly increased. Not only is it likely that current university students have had greater exposure to mobile services and the internet, but it is also essential to educate and empower high school students, prior to their arrival at university, about the safe and responsible use of online resources and platforms. UNAM is responsible for training most of Namibia's schoolteachers and these in turn play an important role in establishing a culture of awareness in schools. Indeed, the people who are exposed to and trained in cyber security are expected to be the country's future source of cyber defence (Rahman et al., 2020).

6.3 Recommendations

Based on the conclusions of this study, the researcher recommends three practical strategies to increase security awareness and protection. These strategies are as follows:

1. Some scholars argued that a lack of cybersecurity frameworks in Namibia could be an obstacle towards fighting cybercrimes effectively (Nawa, 2021). Additionally, Nawa (2021) argues that Namibia lacks a recognised cybersecurity framework that is aimed at creating awareness and safeguarding sensitive financial data between banks and customers during online banking transactions. In the same vein, it was revealed by this study that only 4% of respondents to the questionnaire indicated that they had heard about SMS security threats from school.

   Owing to this, it is recommended that a compulsory Cyber Security Awareness module for all first-year students into the educational curricula of all tertiary institutions in the

country should be introduced. This module should be mandatory and without exemption in all faculties and not just for Information and Technology students. The module should be revised regularly to ensure that it includes up-to-date information, and all staff should understand the importance of the module.

2. Public awareness campaigns are key to fighting cybercrime. It is opined that the lack of public awareness-raising campaigns contributes to the growing vulnerability of people in the global south to cyber-attacks (Bada, Von Solms, & Agrafiotis, 2018). However, awareness campaigns must account for ICT literacy levels (Bada, Von Solms, & Agrafiotis, 2018). This agrees with the findings of this study. The study revealed that in 2019, most (97%) respondents had not previously heard of any specific security threats associated with the use of SMS, and 62% indicated that the questionnaire represented the first time they had been told about SMS security threats.

   Therefore, it is recommended that a security awareness campaigns at tertiary institutions is implemented to educate and update students as follows:

- Institutions should make use of the main electronic communication medium with the students, such as UNAM's web portal and ensure that information about security awareness and precautions are relevant and current. To engage students and support their learning, the platform could include interactive elements such as quizzes.

- Institutions should install posters about cyber security awareness and preventive measures in classrooms, hostels, sport fields, food outlets, bathrooms and other places around campuses which are routinely visible to students.

3. Previous literatures revealed that various African governments, including Namibia, have committed to using ICTs to improve learning within the education system (Sylla, Ndiaye, Ouya, & Mendy, 2020), and SMS has been used to support knowledge-building platforms. For instance, M-Shule is used in Uganda to deliver reading lessons in local languages by SMS and audio to a parent's mobile phone to enable students who are unable to physically attend classes to participate (Van Niekerk, 2020). This makes it important to train future teachers and educators about the importance of the awareness of security related threats.

Hence, it is recommended to ensure that students in UNAM's Faculty of Education, who will be the school teachers of the future are competent in teaching security awareness.

6.4 Limitations of the study and recommendations for future research

The study sampled two hundred and eighty-seven (287) participants from UNAM but not all of universities in Namibia. With a total population of thirteen thousand and seventy-three (13073) students, this presents marginal significance. Nonetheless, with no prior studies about SMS security awareness in Namibia, the research contributes to knowledge by indicating the need for more attention to integrating security awareness and technological literacy. Further studies should identify the impediments to awareness campaigns and training programmes and identify opportunities to address these. This could include investigating how smartphone users' self-protective practices relate to their personal confidence in their abilities to protect themselves and to their perceptions of the effectiveness of existing security or privacy-preserving solutions.

References

99firms. (2021). *SMS Marketing Stats*. Retrieved from 99firms: https://99firms.com/blog/sms-marketing-stats/

A4AI. (2018). *A4AI, Alliance for Affordable Internet (2018). AffordabilityReport.* Washington DC 20005: Alliance for Affordable Internet. Retrieved from https://1e8q3q16vyc81g8l3h3md6q5f5e-wpengine.netdna-ssl.com/wp-content/uploads/2018/10/A4AI-2018-Affordability-Report.pdf

Akamai. (2021, March 3). *Risk Assessment: Multi- Factor Authentication (MFA) Security: Understand The Risk Scale of Today's Authentication Solutions.* Retrieved June 23, 2021, from Akamai: https://www.akamai.com/us/en/multimedia/documents/white-paper/risk-assessment-multi-factor-authentication-security.pdf

American National Standards Institute. (2011). *Signaling System No7 (SS7): SS7 Network and NNI Interconnection Security Requirements and Guidelines.* Washington: Alliance for Telecommunications Industry Solutions.

Bada, M., Von Solms, B., & Agrafiotis, I. (2018). Reviewing National Cybersecurity Awareness in Africa: An Empirical Study. *The Third International Conference on Cyber-Technologies and Cyber-Systems, CYBER 2018* (pp. 78-83). London: University of Cambridge. Retrieved August 24, 2021, from https://www.thinkmind.org/index.php?view=article&articleid=cyber_2018_6_20_80051

Balduzzi, M., Gupta, P., Gu, L., Gao, D., & Ahamad, M. (2016, June). MobiPot: Understanding Mobile Telephony Threats with Honeycards. 723-724. doi:http://dx.doi.org/10.1145/2897845.2897890

Bazeley, P. (2021). *Qualitative Data Analysis: Practical Strategies.* London: SAGE.

Calderwood, F., & Popova, I. (2019, December 14). Smartphone Cyber Security Awareness in Developing Countries: A case of Thailand. *ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, 79–86. Retrieved from https://eudl.eu/pdf/10.1007/978-3-030-05198-3_7

Chai, B. (2021, January 5). *Person to Person Messaging.* Retrieved June 23, 2021, from Person to Person Messaging: https://www.twilio.com/docs/glossary/what-p2p-sms-person-person-messaging

Chandarman, J., & Van Niekerk, B. (2017). Students' Cybersecurity Awareness at a Private Tertiary Educational. *The African Journal of Information and Communication (AJIC)*(20), 133-150. Retrieved August 5, 2021, from https://doi.org/10.23962/10539/23572

Chickowski, E. (2020, October 30). *What is Smishing? SMS phishing explained*. Retrieved from CyberSecurity AT&T: https://cybersecurity.att.com/blogs/security-essentials/sms-phishing-explained-what-is-smishing

Chowdary, N., Rajitha, P., Aneesha, M., & Babu, J. (2018). Security for Short Message Peer-To-Peer Protocol. *ICONIC RESEARCH AND ENGINEERING JOURNALS, 1*(9), 294-298. Retrieved from https://irejournals.com/formatedpaper/1700465.pdf

Cost, A., Reis, L., & Moreira, A. (2020). *Computer Supported Qualitative Research: New Trends on Qualitative Research.* Gewerbestrasse: Springer.

Dawson, M., & Omar, M. (2015). *New Threats and Countermeasures in Digital Crime and Cyber Terrorism.* Pennsylvania: Information Science Reference.

Edeh, M. O. (2019). Opportunities and challenges of the use of mobile phone technology in teaching and learning in Nigeria-A Review. *International Journal of Research in Engineering and Innovation (IJREI), Vol-3*(Issue-6), 352-358. Retrieved from http://doi.org/10.36037/IJREI.2019.3601

Ekinci, Y. (2015). *Designing Research Questionnaires for Business and Management Students.* London: SAGE Publications.

Erickson, C. (2012, September 21). *A Brief History of Texting Messaging.* Retrieved from Mashable: https://mashable.com/2012/09/21/text-messaging-history/

F5 Networks. (2015). *Introduction to the IP Multimedia Subsytem (IMS).* Seattle: F5 Networks, INC. Retrieved from https://worldtechit.com/wp-content/uploads/2015/07/f5-white-paper-introduction-to-the-ip-multimedia-subsystem-ims-

Fahri, O. (2021). *Handbook of Research on Policies, Protocols and Practices for Social Work in The Digital World .* Pennsylavania: IGI Global.

Garba, A., Siraj, M., Othman, S., & Musa, A. (2020, July 18). A Study on Cybersecurity Awareness Among Students in Yobe State University, Nigeria: A Quantitative Approach. *International Journal on*

Emerging Technologies, 11(5), 41-49. Retrieved August 5, 2021, from https://www.academia.edu/43840636/A_Study_on_Cybersecurity_Awareness_Among_Students_in_Yobe_A_Quantitative_Approach

GRN, G. o. (2014). *Ministry of Information and Communication Technology Strategic Plan 2014-2017.* Government of the Republic of Namibia.

Gupta, M., Sharman, R., Walp, J., & Mulgund, P. (2018). *Information Technology Risk Management and Compliance in Morden Organisation.* Pennsylvania.: IGI Global.

Hadnagy, C., & Schulman, S. (2021). *Human Hacking: Win Friends, Influence People, and Leave Them Better Off for Having Met You.* New York: HapperCollins Publishers.

Ilyas, M., & Ahson, S. (2018). *IP Multimedia Subsystem.* London: CRS Press.

Jiang, N., Jin, Y., & Skudlark, A. &. (2012). *Understanding SMS Spam in a Large Cellular Network: Characteristics, Strategies and Defences.* Minneapolis: University of Minnesota. Retrieved June 24, 2021, from https://www-users.cs.umn.edu/~zhang089/Papers/raid2013_jiang_spam

Kumar, R. (2018). *Research Methodology: A Step by Step Guide for Beginners.* London: SAGE Publications.

Lancaster, H. (2022). *Namibia Telecoms Market Report: Telecoms, Mobile and Broadband - Statistics and Analyses.* BuddeComm. Retrieved from https://www.budde.com.au/Research/Namibia-Telecoms-Mobile-and-Broadband-Statistics-and-Analyses

Maleh, Y., Ezzati, A., & Belaissaoui, M. (2018). *Security and Privacy in Smart Sensor Networks.* Pennysylavania: IGI Global.

Management Association Information. (2020). *Mobile Devices in Educationa: Breakthroughs in Research and Practice.* Pennysylavania: IGI Global.

Mare, A. (2019). *Communication Surveillance In Namibia: An exploratory study.* Media Policy and Democracy Project. Retrieved from https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/namibia_report_3rd_pages.pdf

Martin, R. (2012). *Signaling System 7 (SS7).* Retrieved June 22, 2021, from Rutgers University: https://www.cs.rutgers.edu/-rmartin/teaching/fall04/cs552/reading/ss7

Mobile Telecommunications Company. (2020). *Intergrated Annual Report 2020.* Windhoek: Mobile Telecommunications Company.

Myers, M. (2019). *Qualitative Research in Business and Management.* London: SAGE Publications.

Nawa, E.-L. T. (2021). Developing a cybersecurity framework for the banking sector of Namibia . In F. B. Mercy Chitauro (Ed.), *"Assessing Patterns of Cybercrimes Associated with Online Transactions in Namibia Banking Institutions' Cyberspace." In 2021 3rd International Multidisciplinary Information Technology and Engineering Conference (IMITEC), pp. 1-6. IEEE, 2021.* Namibia University of Science and Technology. Retrieved from https://ir.nust.na/handle/10628/817

Ngoqo, B., & Flowerday, S. (2015a, May 25). Information Security Behaviour Profiling Framework (ISBPF) for student mobile phone users. *Computers and Security*, 132-142. doi:http://dx.doi.org/10.1016/j.cose.2015.05.011

Ngoqo, B., & Flowerday, S. V. (2015b, June). Information Security Behaviour Profiling Framework (ISBPF) for student mobile phone users. *Computers & Security, 53*, 132-142. doi:10.1016/j.cose.2015.05.011

Nhinda, G. T., & Shava, F. B. (2021). Towards the use of Participatory Methods in Cybersecurity research in rural Africa: A grassroots Approach. *2021 3rd International Multidisciplinary Information Technology and Engineering Conference (IMITEC).* Windhoek: IEEE. doi:10.1109/IMITEC52926.2021.9714649

Nick, G. (2021, April 2). *The Most Telling Cyber Security Statistics in 2021*. Retrieved from TechJury: https://techjury.net/blog/cyber-security-statistics/

Olaleye, O., Olaniyan, A., Eboda, O., & Awolere, A. (2013). SMS- Based Event Notification System. *Journal of Information Engineering and Application, iii*(10), 56-60. Retrieved June 23, 2021, from https://www.iiste.org/Journals/index.php/JIEA/article/viewFile/7637/8056

Ortiz, J. H. (2020). *Mobile Computing.* London: IntechOpen.

Patton Electronics Company. (2012). *Introduction to SS7 Signaling.* Retrieved June 22, 2020, from Introduction to SS7 Signaling: https://www.patton.com/whitepapers/intro_to_ss7_tutorial

Rahman, N. A., Sairi, I., Zizi, N. A., & Khalid, F. (2020, December 30). The Importance of Cybersecurity Education in School. *International Journal of Information and Education Technology, 10*(5), 378-382. doi:10.18178/ijiet.2020.10.5.1393

Reaves, B., Blue, L., Tian, D., Traynor, P., & Butler, K. R. (2016, July 18 - 20). Detecting SMS Spam in the Age of Legitimate Bulk. *WiSec ' 16 Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, 165 - 167. doi:http://dx.doi.org/10.1145/2939918.2939937

Reynolds, G. (2016). *Information Technology for Managers.* Boston: Cengage Learning.

Russell, T. (2014). *Signaling System #7, Sixth Edition* (sith ed.). New York: McGraw-Hill Education.

Ryder. (2019, November 28). *How Hackers Hack Phone Using SMS.* Retrieved June 24, 2021, from How Hackers Hack Phone Using SMS: https://myhackingworld.com/how-hackers-hack-phone-using-sms/

S Syafriandi, A. F. (2020). Designing hypothetical learning trajectory for learning the importance of hypothesis testing. *Journal of Physics: Conference Series*. doi:10.1088/1742-6596/1554/1/012045

Salmon, A., Levesque, W., & McLafferty, M. (2017). *Applied Network Security.* Birmingham: Packt Publishing.

Sameh G. Khanim, F. .. (2018). Utilization of Short Message Services (SMS) for Library Notification System. *International Journal of Applied Engineering Research ISSN 0973-4562, Volume 13, Number 9* , 6503-6513. Retrieved from http://www.ripublication.com

Sarathchandra, D., Haltinner, K., & Lichtenberg, N. (2016). 'College Students' Cybersecurity risk perceptions, awareness, and Practices. *Cybersecurity Symposium (CYBERSEC)*, 68-73. doi:Sarathchandra, Dilshani & Haltinner, Kristin & Lichtenberg, Nicole. (2016). C 10.1109/CYBERSEC.2016.018.

Sari, P. (2014, June). Measuring Information Security Awareness of Indonesian Smartphone Users. *TELKOMNIKA, 12*(2), 493-500. doi:10.12928/TELKOMNIKA.v12i2.2015

Sauter, M. (2014). *From GSM to LTE-Advanced: An Introduction to Mobile Networks and Mobile Broadband.* New Jersey: Wiley.

Senthilkumar, K., & Easwaramoorthy, S. (2018). A Survey on Cyber Security awareness among college in Tamil Nadu. *IOP Conference Series: Materials Science and Engineering* (pp. 1-10). Vellore: IOP Publishing. Retrieved from https://iopscience.iop.org/article/10.1088/1757-899X/263/4/042043/pdf

Sexena, N., & Chaudhari, N. S. (2012). *A Secure Digital Signature Approach for SMS Security.* Indore: Indian Institute of Technology. Retrieved June 24, 2021, from https://research.ijcaonline.org/ipmc/number1/ipmc022.pdf

Simmons, D., Rowe, G., Myracle, J., & Slaymaker, S. (2019, January 25). *Multi-Factor Authentification (MFA): Enterprise Strategy and Market Assessment.* Retrieved June 23, 2021, from Tech Vision research: https://techvisionresearch.com/wp-content/uploads/2019/01/MFA-20190126-Final-1-1.

Slick Text. (2021, January 4). *44 Mind-Blowing SMS Marketing and Texting Statistics*. Retrieved December 7, 2021, from 44 Mind-Blowing SMS Marketing and Texting Statistics: https://www.slicktext.com/blog/2018/11/44-mind-blowing-sms-marketing-and-texting-statistics/

Statista Research Department. (2021, September 14). *Number of A2P and P2A SMS messages sent worldwide by region from 2011 to 2018(in billions).* Retrieved from Statista: https://www.statista.com/statistics/485141/a2p-and-p2a-sms-traffic-worldwide-by-region/

Stewart, M., & Kinsey, D. (2020). *Network Security, Firewalls and VPNs.* New York: Jones and Barlett Learning.

Sylla, K., Ndiaye, N., Ouya, S., & Mendy, G. (2020). Towards The Use of A Contact Center for The Socialization and Capacity Reinforcement of Learners of African Digital Universites. *2020 22nd International Conference on Advanced Communication Technology (ICACT).* Gangwon-do: IEEE. doi:10.23919/ICACT48636.2020.9061548

Taha, N., & Dahabiyeh, L. (2021, September 16). College Students Information Security Awareness: A Comparison Betweeen Smartphones and Computers. *Education and Information Technologies, 26*(2), 1721–1736. Retrieved August 23, 2021, from https://link.springer.com/article/10.1007%2Fs10639-020-10330-0

Thomas, G. (2021). *Research Methodology and Scientific Writting.* Gewerbestrasse: Springer Publications.

Tshabangu, I., Ba', S., & Madondo, S. (2020). *Approaches and Processes of Social Science Research.* Leeds: IGI Global .

Tu, G., Li, C., Peng, C., Li, Y., & Lu, S. (2016). New Secutity Threats Caused by IMS-Based SMS Service in 4G LTE Networks. *New Secutity Threats Caused by IMS-Based SMS Service in 4G LTE Networks*, 1119-1129. doi:/10.1145/2976749.2978393

Van Niekerk, L. (2020, March 12). *How Africa Creates Unique Use Cases For SMS*. Retrieved from How Africa Creates Unique Use Cases For SMS: https://itouch.co.za/news/sms-uses-africa.php

Vasuki, D. A. (2021). *Research Methodology for Beginners.* North Carolina: LuLu Publication.

World Bank. (2016). *International Energy Agency and the Energy Sector Management Assistance Program. Database from sustainable energy for all SE4AL, global tracking framework.* Retrieved from https://data.worldbank.org/indicator/EG.ELC.ACCS.ZS)

Yadav, S., & Kumar, S. (2018, May 7). Web Application Security: Protection from Advanced Persistent Threat. *INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN TECHNOLOGY, iv*(12), 954-960. Retrieved August 18, 2021, from https://www.academia.edu/42114081/Web_Application_Security_Protection_from_Advanced_Persistent_Threat

Zainab Khyioon Abdalrdha, F. N.-Q. (2019, October). Review on SMS Encryption of Android Mobile by Using Cryptography Algorithm. *International Journal of Engineering Research and, 5*(10). doi:10.31695/IJERAT.2019.3577

Zhang, P., & Li, X. (2015). Determinants of information security awareness: An empirical investigation in higher Education. *Thirty Sixth International Conference on Information Systems,.* Fort Worth.

APPENDICES

Appendix A:

Permission Letter

UNAM
UNIVERSITY OF NAMIBIA

ETHICAL CLEARANCE CERTIFICATE

Ethical Clearance Reference Number: FOS /363/2018 **Date: 20 February, 2018**

This Ethical Clearance Certificate is issued by the University of Namibia Research Ethics Committee (UREC) 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 Faculty/Centre/Campus Research & Publications Committee sitting with the Postgraduate Studies Committee.

Title of Project: Exploring Students Awareness Of Security Threats And Protective Measures Associated With Their Use Of Short Message Service (Sms) At The University Of Namibia

Researcher: Abraham Kalipi

Student Number: 9996702

Supervisor(s) Prof. N. J. Bidwell (Main) Prof Lawrence Kazembe (Co)

Take note of the following:

(a) Any significant changes in the conditions or undertakings outlined in the approved Proposal must be communicated to the UREC. An application to make amendments may be necessary.
(b) Any breaches of ethical undertakings or practices that have an impact on ethical conduct of the research must be reported to the UREC.
(c) The Principal Researcher must report issues of ethical compliance to the UREC (through the Chairperson of the Faculty/Centre/Campus Research & Publications Committee) at the end of the Project or as may be requested by UREC.
(d) The UREC 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.

UREC wishes you the best in your research.

Prof. P. Odonkor: UREC Chairperson

Ms. P. Claassen: UREC Secretary

Appendix B:

Structured Questionnaire

EXPLORING STUDENTS' AWARENESS OF SECURITY THREATS AND PROTECTIVE MEASURES ASSOCIATED WITH THEIR USE OF SHORT MESSAGE SERVICE (SMS) AT THE UNIVERSITY OF NAMIBIA

Abraham Kalipi 9996702 Research Questionnaire

* Required

1. **Faculty Name** *

Mark only one oval.

Centre of Postgraduate Studies

Faculty of Agriculture and Natural Resources

Faculty of Economic and Management Science

Faculty of Education

Faculty of Engineering and Information Technology

Faculty of Humanities and Social Sciences

Faculty of Law

Faculty of Science

Namibia Business School

School of Medicine

School of Nursing

School of Pharmacy

School of Public Health

2. **Mode of Study** *

Mark only one oval.

Full time study

Part-time study

Distance study

3. **Year of Study** *

Mark only one oval.

1st year

2nd year

3rd year

4th year

5th year

6th year

Other:

4. **Gender** *

Mark only one oval.

Female

Male

Prefer not to say

5. **Date of Birth** *

Example: December 15, 2012

6. **Residence** *

Mark only one oval.

Hostel Accommodation

Non-Hostel Accommodation

7. **Previous High/Secondary School** *

Mark only one oval.

Urban Private School

Urban Government School

Rural Private School

Rural Government School

8. **Home language** *

Mark only one oval.

Afrikaans

English

German

Nama/Damara

Otjiherero

Oshiwambo

Rukavango

San

Setswana

Silozi

Others

9. **How long have you had a cell phone? Please provide your answer in number of year(s).** *

10. **In the past 24 hours estimate how many SMS you have sent?** *

11. **In the past 24 hours estimate how many SMS you have received?** *

12. **In the past 24 hours estimate how many WhatsApp messages you have sent?** *

13. **In the past 24 hours estimate how many WhatsApp messages you have received?** *

14. **In the past 24 hours estimate how many phone calls you have made?** *

15. **In the past 24 hours estimate how many phone calls you have received?** *

16. **In the past 24 hours estimate how many Emails you have sent?** *

17. **In the past 24 hours estimate how many Emails you have received?** *

18. **Have you ever received a threatening SMS?** *

Mark only one oval.

Yes

No

19. **If your answer to the previous question is yes, why did you feel threatened?** *

20. **Have you heard of any security threats associated with the use of SMS?**

Mark only one oval.

Yes

No

21. **Which organizations have sent you SMS warnings about threats before? (tick all that applies)***

Bank Windhoek

FNB

MTC

NASFAF

Nedbank

Standard Bank

TN Mobile

UNAM

Other:

22. **Which organizations have you seen/heard broadcasting warnings about SMS threats before? (tick all that applies)** *

Radio

TV

Newspapers

Other:

23. **Do you feel confident in protecting the privacy of your phone?** *

Mark only one oval.

1 2 3 4 5 6 7 8 9 10

Not confident at all Totally confident

24. **Do you pick up a call from a phone number you do not recognize?** *

Mark only one oval.

Never answer

Sometimes answer

Mostly answer

Always answer

25. **Do you respond to SMS texts from numbers that you do not recognize?** *

Mark only one oval.

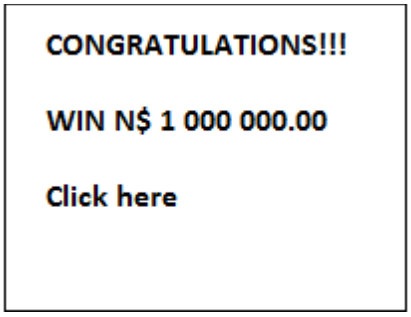
Never respond

Sometimes respond

Mostly respond

Always respond

26. **Imagine you receive the following text message.** *



27. **How do you react?** *

Mark only one oval.

1 2 3 4 5 6 7 8 9 10

Relaxed Nervous

28. **How do you react?** *

Mark only one oval.

1 2 3 4 5 6 7 8 9 10

Uninterested Curious

29. **How do you react?** *

Mark only one oval.

1 2 3 4 5 6 7 8 9 10

Click the text Delete immediately

30. **Please indicate how threatening it is to put your cell phone down at home.** *

Mark only one oval.

1 2 3 4 5 6 7 8 9 10

Less threatening Extremely threatening

31. **Please indicate how threatening it is to put your cell phone down at the lecture halls.** *

Mark only one oval.

1 2 3 4 5 6 7 8 9 10

Less threatening Extremely threatening

32. **Please indicate how threatening it is to put your cell phone down at the Grub / Cafeteria.***

Mark only one oval.

1 2 3 4 5 6 7 8 9 10

Less threatening Extremely threatening

33. **Please indicate how threatening it is to put your cell phone down at the dining hall. ***

Mark only one oval.

1 2 3 4 5 6 7 8 9 10

Less threatening Extremely threatening

34. **Please indicate how threatening it is to put your cell phone down at shops. ***

Mark only one oval.

1 2 3 4 5 6 7 8 9 10

Less threatening Extremely threatening

35. **Please indicate how threatening it is to put your cell phone down at UNAM library. ***

Mark only one oval.

1 2 3 4 5 6 7 8 9 10

Less threatening Extremely threatening

36. **Please indicate how threatening it is to put your cell phone down in a public transport: Taxi, Bus, Train, Plane. ***

Mark only one oval.

1 2 3 4 5 6 7 8 9 10

Less threatening Extremely threatening

37. **Please indicate how threatening it is to put your cell phone down in the bank. ***

Mark only one oval.

1 2 3 4 5 6 7 8 9 10

Less threatening Extremely threatening

38. **Please indicate how threatening it is to put your cell phone down at the bar / pub.** *

Mark only one oval.

1 2 3 4 5 6 7 8 9 10

Less threatening Extremely threatening

39. **Please indicate how threatening it is to put your cell phone down at UNAM computer labs.** *

Mark only one oval.

1 2 3 4 5 6 7 8 9 10

Less threatening Extremely threatening

40. **Please indicate how threatening it is to put your cell phone down at public places.** *

Mark only one oval.

1 2 3 4 5 6 7 8 9 10

Less threatening Extremely threatening

41. **Please indicate how threatening it is to put your cell phone down at offices.** *

Mark only one oval.

1 2 3 4 5 6 7 8 9 10

Less threatening Extremely threatening

42. **Please indicate how threatening it is to put your cell phone down in town.** *

Mark only one oval.

1 2 3 4 5 6 7 8 9 10

Less threatening Extremely threatening

43. **Please describe all the different types of SMS security threats that require you to protect items stored in your phone.** *

44. **Please explain all the different ways you use to protect items stored in your phone.** *

45. **Is this the first time you have been told about SMS security?** *

Mark only one oval.

Yes

No

46. **If your answer to the previous question is No, how did you hear about it?** *