Phishing attack awareness amongst users at a university of technology in the Western Cape

by

Mutomb Japhet Kayomb

Dissertation submitted in partial fulfilment of the requirements for the degree

Master of Information and Communication Technology

in the Faculty of Informatics and Design

at the Cape Peninsula University of Technology

Supervisor: Dr. E. Francke

Co-supervisor: Dr. T. Ncubukezi

Cape Town

Date submitted October 2024

DECLARATION

I, Mutomb Japhet Kayomb, declare that the contents of this dissertation/thesis represent my own unaided work and that the dissertation/thesis has not previously been submitted for academic examination towards any qualification. Furthermore, it represents my own opinions and not necessarily those of the Cape Peninsula University of Technology.

Signed  **Date 5 October 2024**

ABSTRACT

Phishing attacks have emerged as a significant cybersecurity threat, particularly for university students who heavily rely on institutional networks for their academic and personal activities. These attacks often deceive users into revealing sensitive information, such as login credentials, leading to potential data breaches and financial losses. Numerous studies have highlighted the growing prevalence of phishing in academic environments, emphasising the need for enhanced awareness and preventive measures.

This study aims to develop a phishing attack awareness framework for users at a University of Technology in the Western Cape. Through a qualitative case study approach, data was collected via surveys from students, academics, and IT staff within the university's Department of Information Technology. The data was analysed using thematic analysis, revealing key insights into the frequency, strategies, and user awareness of phishing attacks.

The findings show that phishing attacks are common within the university, with many users unaware of the sophisticated tactics used by attackers. The research also identified critical gaps in the current awareness programs, including inconsistencies in phishing reminders and low participation in awareness training. Based on these findings, this study recommends a more structured and frequent phishing awareness program, incorporating real-time phishing simulations and regular training to strengthen user defences against phishing attacks.

The proposed framework addresses the urgent need for heightened cybersecurity education among university users. It aims to reduce end-users' vulnerability to phishing attacks and enhance overall institutional cybersecurity resilience.

ACKNOWLEDGEMENTS

I wish to thank:

- My parents: Mutomb & Mujinga.
- My wife: Celeste.
- My supervisors: Dr. Errol and Dr. T. Ncubukezi.
- Anyone else who supported this research.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

GLOSSARY

AOL	**America Online**
BYOD	**Bring Your Own Device**
CCTV	**Closed-circuit television**
GDT	**General Deterrence Theory**
HTTP	**Hypertext Transfer Protocol**
IS	**information systems**
IT	**Information Technology**
MIT	**Man in the Middle attack**
PBC	**Perceived Behavioural Control**
SA	**South Africa**
TTAT	**Technology Threats Avoidance Theory**
VoIP	**Voice over internet protocol**

1 CHAPTER ONE: INTRODUCTION

1.1 Introduction

The widespread use of technologies has brought many successes among organisations such as the University of Austin Peay State. This university used data mining technology to assist enrolling students in receiving a course recommendation where they have a higher chance of succeeding. This process involved checking data on the students' profiles and transcripts. Furthermore, the advancement of computer networks has helped companies improve their business operations. Walmart in the United States of America used the computer network to connect suppliers to inventory, sales, and forecasting data. It also implemented a wireless network in the warehouse to track the flow of goods to its distribution centres (Bidgoli, 2021). However, these advancements brought some cybersecurity challenges such as phishing attacks as described in the section below.

Phishing attacks received much attention in recent years because of the ever-increasing number of online victims. A phishing attack is a practice in which the attacker lures an online user into revealing personal information about themselves. The phisher uses authentication information to obtain personal information such as credit card information, national identification numbers, and passwords. The attacker obtains this information by posing as a trusted individual or organization (Dean, 2013: 493). To avoid becoming victims, internet users should, therefore, be aware of the various techniques employed in phishing attacks. While many organizations, including university networks around the globe, are suffering from phishing attacks. Some of these cyberattacks cause indirect financial loss. Mimecast published a report that showed that 67 percent of organizations had experienced phishing attacks, and 73 percent of victims had experienced a direct financial loss (Mimecast, 2019).

Many educational institutions do not have an effective anti-phishing program for users. This issue was demonstrated in a study among 1200 students at a university. This study showed that only 10 percent of these students detected phishing attacks via email and Facebook and followed the university’s cybersecurity policies (Benenson, Gassmann & Landwirth, 2017). Another study conducted at a large university in the US showed poor participation in anti-phishing activities among employees. It involved the detection of phishing attacks via email messages (Canham, Posey & Constantino, 2022). The above awareness campaigns evaluated mitigation techniques against phishing attacks and included not the threat appraisal.

The threat appraisal is a process within the TTAT (Technology Threats Avoidance Theory) framework where users are persuaded to avoid IT threats (Liang & Xue, 2009: 71-90).

Besides persuasion of IT threats, TTAT includes another process that educates IT users about the techniques to counter IT threats (Liang & Xue, 2009). Teaching IT users about the attributes of IT threats may help combat phishing attacks, and an investigation among 480 undergraduate students in Nigeria showed that hackers tricked users with phishing. The findings of this investigation in Nigeria revealed that 23 percent fell to spear phishing, and phishers directed these attacks to specific individuals. Additionally, phishers deceived 42 percent of users through generic phishing, which mimicked email service providers with messages “Update Mailbox Capacity” and “Mailbox full.” Lastly, the hackers tricked 35 percent of students with tailored phishing messages with the note “Semester Results.” (Yoro, Aghware, Akazue, Ibor & Ojugo, 2023).

1.2 Research Background

Computer networks were traditionally isolated from each other and connected only a few end-users within a specific geographic area. Users on these networks had data repositories at their local networks, and this data could not be accessible from outside of the organization’s network. Data on these computing systems were less prone to unauthorised access as only users on the corporate network had access to the data. However, modern networks are now interconnected globally, and data on corporate networks are accessible from anywhere with an internet connection. This interconnectivity of networks has put confidential data at risk of unauthorised access despite the use of usernames and passwords to authenticate users who access data on the network (West, Andrews, & Dean, 2019).

Thomas, Li, Zand, Barrett, Invernizzi, Markov, Comanescu, Eranti, Moscicki, Margolis, Paxson & Bursztein (2017) demonstrate in their recent study that hackers stole millions of usernames and passwords from various online services between 2016 and 2017. The cybercriminals sold those online credentials on the black market for a large amount of money. These criminals are also able to log onto the victims’ bank accounts, steal money from their accounts or hold hostage the user’s sensitive information and request a ransom in exchange. The gathering of many passwords and usernames from different users requires sophisticated tools such as keyloggers and phishing kits. For these tools to work, the attacker needs to conceal these malicious tools in software intended to perform some regular tasks on the computer while doing nefarious activities in the background, such as collecting personal information. The introduction of Bring Your Own Device (BYOD), which means the end-users bring their mobile devices onto

the corporate network, has created a new challenge for cybersecurity experts. Security experts have difficulties defending against cyber-attacks because users of these mobile devices can be lured into installing malicious software while working away from the corporate network (West et al., 2019).

Besides the websites, phishing attacks have also been targeting mobile computing devices. On the mobile device, some applications enable users to perform specific tasks. The attackers create malicious applications like malicious websites that give unauthorized access to personal information such as passwords, credit card numbers, and so on. Human errors like failure to check the authenticity of the application before the installation play a role in the data breach. Users can use the application security indicators to check for malicious applications; however, the study demonstrates that most users do not monitor these indicators. Users who do not possess any security tools for authenticating applications are more vulnerable to phishing attacks (Marforio, Masti, Soriente, Kostiainen & Capkun, 2015). Besides mobile technology users, more cloud computing users are becoming victims of phishing attacks.

Cybersecurity training can equip online users with the ability to counter phishing attacks. A study demonstrated that a lack of cybersecurity training could lead to malicious social engineering attacks, a type of phishing attack that tricks users into disclosing personal information to an unauthorised user (Mouton, Teixeira & Meyer, 2017). Some of this training includes phishing awareness campaigns to safeguard against phishing attacks. However, another study has shown that many IT users in South Africa (SA) have not gone through adequate phishing awareness. A researcher demonstrated the awareness issue through an online survey amongst over 100 IT users in Johannesburg, where users were not aware of the operational risk of disclosing personally identifiable information on social media (Rajkumar & Njenga, 2022).

Furthermore, more studies show that SA is lagging in terms of effective cybersecurity awareness and education among internet users. An investigation into organizational information security in SA through a web-based survey in which 356 internet users participated. This survey showed that IT specialists needed to deliver cybersecurity awareness training focusing on these three issues: internet usage, safe email usage, and social media usage (Kritzinger, Da Veiga & van Staden, 2023). Additionally, the study about the susceptibility of phishing attacks in SA showed that IT users aged 25 years and younger did not receive phishing awareness training before entering the workforce (Wannenburg, M.C., Nieman, A., Steyn, B. & Wannenburg, D.G., 2023).

Moreover, many organisations and individuals are prone to phishing attacks as illustrated in the Mimecast report that showed that 67 percent of organizations had experienced phishing attacks, and 73 percent of victims had experienced a direct financial loss and on the other hand, Thomas et al. (2017) demonstrate in their recent study that hackers stole millions of usernames and passwords from various online services between 2016 and 2017. The study proposed improvements to the authentication mechanism.

Many IT security experts have attempted to implement countermeasures. They used human education as a countermeasure tool to minimize the impact of phishing attacks, and they delivered awareness training to users. Furthermore, the researchers attributed 95 percent of phishing incidents to human errors (Alkhalil, Hewage, Nawaf, L. & Khan, 2021). However, as discussed in the previous paragraphs, many organizations do not possess proper cyber awareness training for users, and cyber experts proposed technologies such as VPN and multi-factor mechanisms against phishing attacks during the COVID-19 pandemic. The VPN encrypts the data between networked computers through public networks, while the multi-factor authenticator reinforces the authentication mechanism (Al-Qahtani & Cresci, 2022).

1.3 Research Problem

Despite the use of security products such as anti-virus and other related security technologies, phishing attacks are continually increasing and remain stressful for internet users. Kritzinger, Da Veiga, and van Staden (2023) discussed recent reports of personal data breaches for 24 million people in South Africa. Phishers are using spoofed emails of business partners and vendors to trick end-users into disclosing their usernames and passwords. This problem could negatively affect university end-users who store their personal information and other confidential information on a university's computer network. This could be because end-users on the University's network do not possess the necessary skills to secure their accounts. A cause of this problem is an ineffective awareness of phishing attacks. Perhaps a study that develops a phishing attack awareness program based on TTAT framework could reduce the amount of these attacks on a University of Technology's computer network.

1.4 Research Aim

The study aims to develop a phishing attack awareness framework for users in a University of Technology in the Western Cape. Furthermore, to investigate the nature of a phishing attack awareness program at the University of Technology

1.5 Objectives

1. To identify the frequency of phishing attacks at a University of Technology
2. To determine the strategies used to deploy phishing attacks on a University of Technology network
3. To establish the awareness level of phishing attacks among end-users at a University of Technology
4. To investigate the nature of a phishing attack awareness program at a University of Technology

1.6 Research Questions

1.6.1 Main Research Question

The main research question the study seeks to answer is:

How can a phishing attack awareness framework be developed to help reduce the number of attacks on a University of Technology's computer network?

1.6.2 Sub Questions

1. What is the frequency of phishing attacks at a University of Technology?
2. What are the strategies used to deploy phishing attacks at on a University of Technology network?
3. What is the awareness level of phishing attacks among end-users at a University of Technology?
4. What is the nature of a phishing attack awareness program at a University of Technology?

1.7 Significance

The study is significant in the following ways:

• The outcome has the potential to help protect the university data. The university computer network contains confidential data. Additionally, the study could reduce the downtime on the University's computer network by reducing the number of cyber-attacks.

- The outcome can also address the online behaviour of end-users to reduce the number of phishing attack victims on the internet.

1.8 literature review summary

1.8.1 Phishing Attacks

Jakobsson & Myers (2006) stated that phishing attacks were detected for the first time in 1990 when America Online (AOL) network systems discovered that its networks had many fake accounts. These fraudulent accounts were created by registering false identity numbers and credit card numbers. After AOL became aware of these fake accounts which had access to its online resources, it started verifying the ID numbers and credit cards with an institution such as banks before allowing any AOL user to create an account. To bypass the measures taken by AOL, the hackers started looking for legitimate passwords from AOL users by posing as AOL agents (Jakobsson & Myers, 2006).
Phishing is an electronic message that seems to originate from a trusted source and requests authentication information such as a username and password to gain access to an individual or organisation account hosted on the internet and containing confidential information (West et al., 2019: 532).

1.8.2 Phishing Attack: Dumpster Diving

In dumpster diving, the attacker through the trash to collect valuable information that can be useful to penetrate a computer network. Many trash receptacles contained items that had personal and sensitive information, such as papers and computer devices. These items had names, cell phone numbers, and identity numbers, which were used to create usernames and passwords that an attacker could use to commit fraud. There were also computer devices that were disposed of without removing all personal information on them. The disposal of these computer devices had the same devastating consequences as the paper-based materials with valuable information (Shimonski, 2014: 89-90).

1.8.3 User Awareness of Phishing Attacks

Gardner & Thomas (2014) stated that cybersecurity awareness is defined as a program that enables an organization to inform end-users about potential cyber threats and leads to responsible behaviour that does not put the organization’s data at risk. Phishers exploit the behaviour of end-users, making them vulnerable to attack. Some of these behaviours include clicking on the link without checking the authenticity of the source, responding to suspicious

emails due to curiosity, and so on. Victims of phishing attacks were deceived because many emails and websites visited seemed to originate from trusted sources. Thus, the lack of awareness programs led to an increase in the number of victims (Gardner & Thomas, 2014). Even though some organizations launched phishing awareness campaigns, many end-users were still unwilling to change the behaviours that exposed them to cyber-attacks. These end-users ignored the company's policies and procedures that contained various countermeasures and risks of phishing attacks (Hadlington et al., 2019).

1.9 Delineation

The researcher aimed to develop a framework for phishing attack awareness in this study. This study included one University of Technology in Cape Town due to time constraints. However, the researcher employed a qualitative approach to collect rich and in-depth data to reach the study's objectives.

1.10 Summary of Research Methodology

1.10.1 Qualitative approach

The researcher will use a quantitative approach in this investigation to meet the study's goal. This approach will allow the collection of rich and in-depth information (Neville, 2005).

1.10.2 Research strategy: case study

The study will include a case study of a University of Technology. The University of Technology will represent a subgroup of a large population. This strategy will align with the research approach in this study.

1.10.3 Target population

The population will consist of academics, students, and industry experts. This population will represent a larger group.

1.10.4 Sampling techniques

The researcher will use purposive sampling as it aligns with the research strategy.

1.10.5 The Sample

Data was collected from 28 first-year (n=8) and third-year students (n=20), 15 academics and two IT technical experts. The total of participants was 45.

1.10.6 Data collection

The researcher will use a questionnaire with open-ended questions as a data collection tool.

1.10.7 Data analysis

The investigator will select a thematic analysis to analyse data. This analysis tool will allow the researcher to identify patterns and relationships between them and report on the collected data (Braun & Clarke, 2006).

1.11 Thesis Structure

Table 1.1 outlines the structure of the thesis.

Table 1.1 Thesis Structure

Activities	Description
Chapter 1: Introduction	Chapter One consists of an introduction and background to the study and also a problem statement.
Chapter 2: Literature Review	Chapter Two is an analysis of previous studies and the identification of gaps.
Chapter 3: Research Methodology & Underpinning Theory	Chapter Three comprises steps that enable the researcher to answer the research questions and the adoption of a framework for this study.
Chapter 4: Results and Discussion of Findings.	Chapter Four presents, analyses, and interprets the collected results of the study and discusses the findings.
Chapter 5: Conclusion and Recommendations	Chapter Five concludes the thesis and revisits the research objectives, summarises findings and outlines recommendations.

1.12 Outcomes & Contribution

The outcome of this study was the development of a framework depicting the process of avoiding phishing attacks among end-users on a computer network. This model informed and

educated users within the institution about precautionary measures to prevent phishing attacks and the impact of these attacks on the organisation.

This study is important in addressing the problem using the TTAT theoretical framework, and a qualitative research approach could give another view of phishing awareness. The preliminary literature showed that many phishing attack studies focused on the adaptation and development of cybersecurity tools rather than on end-users.

1.13 Summary

A phishing attack is a cyberattack that tricks internet users into revealing their credentials to an online account. This online account holds confidential information that can be used to commit cybercrimes. Cybercrimes have a high chance of succeeding when the phishers impersonate legitimate organisations in their communication with the victim. Phishing attacks are widespread in many organisations' computer networks, which include universities. Phishing attacks are increasing because they have a high chance of succeeding as they target end-users. The end-users are considered the weakest link in the line of defence against unauthorised access to data on computer networks.

A phishing awareness program enables users to understand the mitigation techniques of phishing attacks. A qualitative study produced detailed information that supported an understanding of phishing attacks and developed a phishing awareness program. The program was developed based on the TTAT framework, which is pertinent to this study as it has been used in many cybersecurity studies.

2 CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

The literature review focused on the relevant body of knowledge to investigate and develop a phishing awareness program that can be used to raise end-user awareness about phishing attacks.

This chapter includes the following elements: the benefits of cyberspace (2.2), the openness of cyberspace (2.3), the challenges of cyberspace (2.4), cyber security (2.5), phishing attacks (2.6), the types of phishing attacks (2.7), the frequencies of phishing attacks (2.8), phishing awareness programs (2.9), the types of phishing awareness programs (2.10), phishing attacks at Institutions of higher education (2.11), and summary (2.12).

2.2 Benefits of Cyberspace

In this modern age, the internet enables users to access computer resources such as email services, eCommerce services, learning management systems, and other related technologies from any location around the globe. These computer resources hold personal information and private information for businesses that are only accessible by authorised users (Andreasson, 2012). Computer resources are crucial to learning processes in many higher education institutions (Hasudunganlubis, Idrus, & Sarji, 2018). The quality of the learning process included the following: access to more information, enabling collaboration among students and experts around the globe, and provision of a simulation environment (Costello, Corcoran, Barnett, Birkmeier, & Cohn, 2014). However, the internet is interconnected with many of these computer technologies. The internet is a public network that poses security threats to the end-users. To address the online security threats that put users' personal and sensitive information at risk, computer experts introduced the concept of network security (Andreasson, 2012).

2.3 Openness of Cyberspace

The number of networked devices on the internet is estimated at 5.3 billion by 2023 (Cisco, 2020). Computer experts have defined the internet as a collection of different types of computers and networks around the globe (Bidgoli, 2012). The internet ensures that the networked computers' users have access to IT resources such as email services, e-learning content, etc. These IT resources are accessible from a local or remote network. Computer

experts have taken advantage of this accessibility to develop the technology called cloud computing. This technology has the main objective, which is to distribute IT resources to many internet users (Erl, Mahmood & Puttini, 2013).

2.4 Challenges of Cyberspace

The global network interconnects end devices around the world. The internet contained network devices that facilitated the transmission of data from point A to point B. The data went through many networks that were not under the control of the sender or receiver. Data could be intercepted along the way and retransmitted to the destination in man-in-the-middle attacks (Wang & Kissel, 2015). This attack occurred in the transmission of data between an ordinary computer and an HTTP server. The HTTP protocol initiates the communication between these devices, but it does not encrypt data. This encrypted data can be monitored and changed by an unapproved outsider. The outsider monitored and changed confidential information without leaving any trace (Mallik, 2018).

Confidential data monitored by the attacker can be the identities of the entities involved in the communication. Hackers are using identities that they gather through man-in-the-middle attacks in the impersonation of these entities. This impersonation can lead to unauthorised disclosure of data (Wang & Kissel, 2015). Other information that attackers disclose is the IP addresses of devices, which the hackers use to redirect data to unauthorised devices (West et al., 2018). These incidents are more common on a computer network without a robust encryption mechanism. These incidents could be caused by people who maintain the computer network's lack of awareness of an encryption mechanism (Mallik, 2018).

Lack of awareness of the robust encryption protocols among the operators of a small IoT wireless network led to an MIT (Man in the Middle attack), and the attackers used the MIT to tamper with the IPv6 packets sent between two devices on an IoT network. Weak encryption puts confidential information in transit between any source and destination at risk of a breach (Navas, Cuppens, Cuppens, Toutain & Papadopoulos, 2021).

2.5 Cyber Security

Computer security experts defined network security as a combination of security techniques. These techniques included the following security: protecting physical equipment on the computer network, the encryption of data-in-transit, protecting data at rest, software products, security appliances, control access to the network resources, and network security policies.

(White, 2015:340). Furthermore, other security experts also defined information security as a combination of techniques that ensure the availability, integrity, and confidentiality of information assets on computer networks and paper-based systems (Calder & Watkins, 2012: 9-20).

A network security policy is one of the security measures that protect a computer network. This protection consists of guidelines for end-users to perform their task without compromising the security of the network. Therefore, end-users need to be aware of the security policy (White, 2015:340). A study conducted in Delhi among universities' libraries showed security policies as a security concern to the computer networks (Singh & Margam, 2018). Additionally, studies of wireless networks within other universities in Kenya revealed the inefficacy of security policies within a wireless network (Ooko & Shadrack, 2019). Besides the network policy, physical security is another mechanism that protects computer networks.

Physical security protects resources within the computer network. This security mechanism consisted of barriers, Technology, and control systems. Physical security barriers such as locks, fencing, keys, and so on were implemented around critical computer systems to prevent unauthorised access from intruders. Another mechanism used in physical security is Technology and control systems such as CCTV to detect any unauthorised access to critical computer systems. The other component of physical security is the human element. Humans are responsible for the enforcement of physical security (Hefty, 2013). The enforcement of physical security is part of network security and guides the users' behaviour within the network (Ooko & Shadrack, 2019).

2.6 Phishing Attacks

Jakobsson & Myers (2006) stated that phishing attacks were detected for the first time in 1990 when America Online (AOL) network systems discovered that its networks had many fake accounts. These fraudulent accounts were created by registering false identity numbers and credit card numbers. After AOL became aware of these fake accounts that had access to its online resources, it started verifying the ID numbers and credit cards with institutions such as banks before allowing any AOL user to create an account. Threat actors bypassed these measures by impersonating AOL agents who collected the passwords of AOL users. These passwords gave threat agents access to AOL resources (Jakobsson & Myers, 2006).

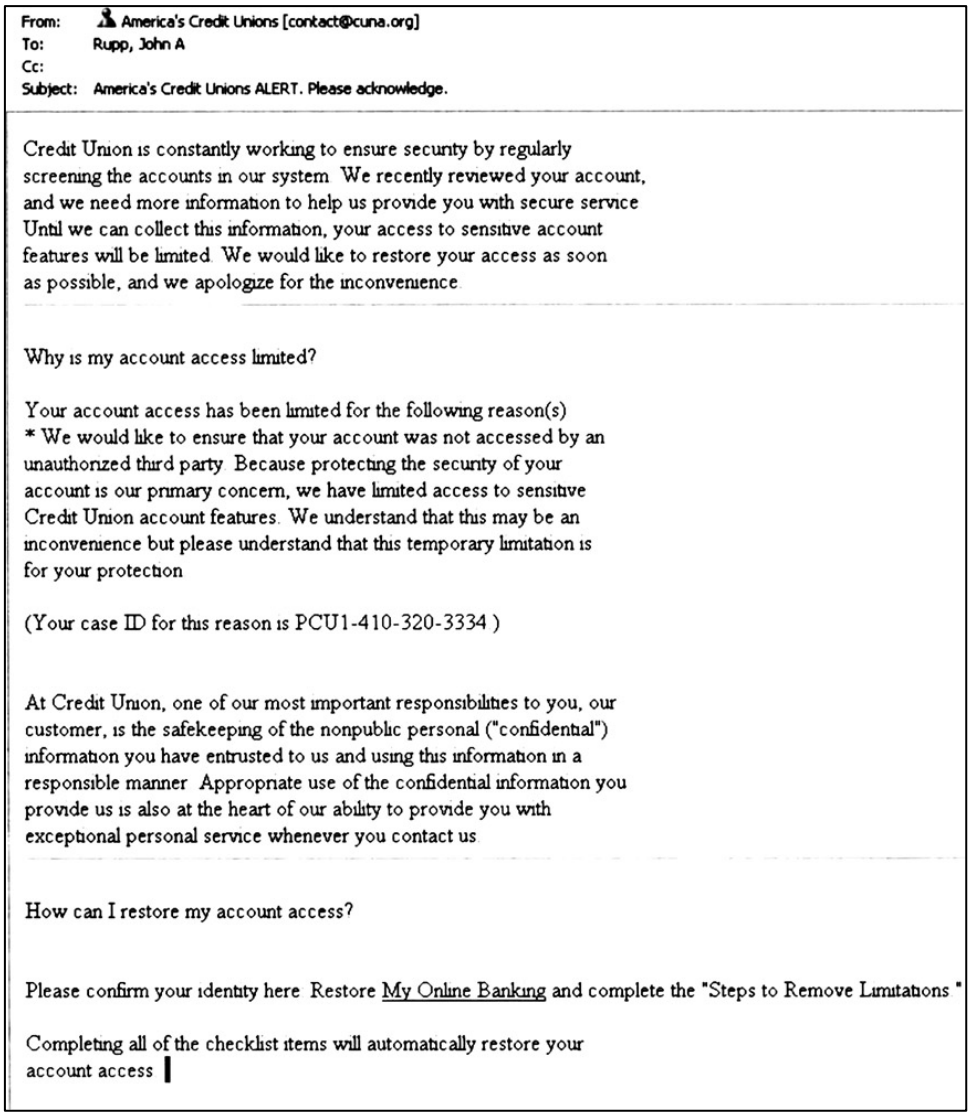
The phishing attack had two parts. The first one is social engineering, and the second part is malware. In the first part of the attack, the phisher tries to convince the victim to perform an

action that compromises the computer system or gives unauthorized access to confidential information, as illustrated in Figure 1 below. In the second part, an attacker installs malicious software on the computer system. For instance, many victims received an electronic message that told them to install recent anti-virus software. Still, this anti-virus was a malicious code that performed nefarious actions such as collecting users' personal information and browser activities. (White, 2015: 340).

2.7 Types of Phishing Attacks

2.7.1 Email phishing

Email phishing is an electronic message that seems to originate from a trusted source. The trusted party requests authentication information such as username and password. Phishers obtain this authentication information that they use to gain access to an individual or organisation account. These accounts contain confidential information and are accessible through computer networks or the internet (West et al., 2019: 532). Hackers used email phishing to target users of major IT companies such as Google. A 2018 report showed that phishers targeted 71 per cent of their users (Pompon, Walkowski, & Boddy, 2018).



From: America's Credit Unions [contact@cuna.org]
To: Rupp, John A
Cc:
Subject: America's Credit Unions ALERT. Please acknowledge.

Credit Union is constantly working to ensure security by regularly screening the accounts in our system. We recently reviewed your account, and we need more information to help us provide you with secure service. Until we can collect this information, your access to sensitive account features will be limited. We would like to restore your access as soon as possible, and we apologize for the inconvenience.

Why is my account access limited?

Your account access has been limited for the following reason(s):
* We would like to ensure that your account was not accessed by an unauthorized third party. Because protecting the security of your account is our primary concern, we have limited access to sensitive Credit Union account features. We understand that this may be an inconvenience but please understand that this temporary limitation is for your protection.

(Your case ID for this reason is PCU1-410-320-3334.)

At Credit Union, one of our most important responsibilities to you, our customer, is the safekeeping of the nonpublic personal ("confidential") information you have entrusted to us and using this information in a responsible manner. Appropriate use of the confidential information you provide us is also at the heart of our ability to provide you with exceptional personal service whenever you contact us.

How can I restore my account access?

Please confirm your identity here. Restore My Online Banking and complete the "Steps to Remove Limitations."

Completing all of the checklist items will automatically restore your account access.

Figure 2.1 Phishing email (Jakobson & Myers, 2006)

Attackers embed a malicious link into the phishing email, which mimicked popular websites by creating copies of the original website from reputable organizations. The victims of these attacks were internet users who frequently accessed websites from these organizations. This attack required the victim to click on the embedded link in the email, which redirected them to a fake website. The website prompted the users to provide sensitive information such as usernames, and passwords, and the hackers captured this private information (Wu, Miller & Garfinkel, 2006).

Besides the IT companies' website links, hackers used the university's website, such as a blackboard in the email phishing. University computer network users used blackboard websites to conduct their daily tasks, and hackers sent email phishing that included a malicious link to the fake backboard. Hackers sent these malicious links at the beginning and the end of the

semester since many users accessed the university website during that time of the semester (Gutierrez, C. N., Kim, T., Corte, Avery, Goldwasser, Cinque, & Bagchi. 2018). A study of email phishing at the University of West in England showed that ten thousand email users were victims of phishing attacks in September 2018. These victims were among 4000 Staff, and 28790 students had email addresses issued by the University (Legg & Blackman, 2019). Another study revealed that many students opened phishing emails with malicious links because the hacker offered a reward and, in this case, it was a free concert ticket (Maimon, Howell, Perkins, Muniz & Berenblum, 2021).

Many email users were victims of phishing attacks because phishers used various persuasion techniques in the email subject lines to lure them into opening email phishing. An automated detection tool was proposed to filter email subject lines to identify phishing emails (Ferreira & Teles, 2019). Despite an increase in email filtering tools, there were still many undetected phishing emails. Security experts introduced email filtering tools with machine learning algorithms. The experts conducted an experimental test on an enormous set of emails within a university's computer network. The study showed that tools with machine learning algorithms were more accurate compared to traditional filtering techniques (Gutierrez et al., 2018).

2.7.2 Spear-phishing

Cybersecurity experts defined spear-phishing as a phishing attack. The attacker personalized this phishing attack to a specific recipient. Phishers are tailored to a recipient using the information found on social media and corporate websites. The personalization of this attack led to the disclosure the valuable information (Hadnagy & Fincher, 2015: 27-29). The defence against this attack was difficult to defend against because the phisher spent a lot of time gathering information about the target before the attack. The phisher knew what the victim could expect. An experiment on spear-phishing took place at a higher institute of learning where 1200 students were selected. The results of the research showed 20 per cent of victims were email users, and 42.5 per cent were Facebook users (Benenson et al., 2017). However, a study conducted on the university community revealed that there was not any significant difference between generic and spear-phishing attacks (Broadhurst, Skinner, Sifniotis, Matamoros-Macias & Ipsen, 2018).

2.7.3 Vishing

A vishing attack was another phishing attack in which the phisher approached the victim through a telephone. The attacker trapped the victim to provide confidential information by requesting a call back for an issue that required certain information to be solved. Once the

victim supplied sensitive data, the hacker used them to gain unauthorized access to the computer network. In this phishing attack, the phisher could also alter the voice-over internet protocol (VoIP) packet by changing the telephone number of the caller (Bosworth, Michel & Whyne, 2014).

2.7.4 Dumpster diving

In dumpster diving, the attacker went through the trash to collect valuable information that can be useful to penetrate a computer network. Many trash receptacles contained items that had personal and sensitive information, such as papers and computer devices. These items had names, cell phone numbers, and identity numbers that the attacker could use to create usernames and passwords and later used in fraud (Krombholz, Hobel, Huber & Weippl, 2015). There were also computer devices that the owners disposed of without removing all personal information on them. The disposal of these computer devices had the same devastating consequences as the paper-based materials with valuable information (Shimonski, 2014: 89-90).

2.8 Phishing Attacks Frequencies

Cyberattacks were on the rise during the covid-19 pandemic as many organisations relied on computer networks and related technologies to conduct their day-to-day operation. The healthcare institution is one of the organisations that was affected by cyberattacks due to the fact it uses technologies to store confidential information about patients. The other institution affected by the cyber-attacks is the financial services which also confidential information of its customers such as banking details. Entities were not spared by the cyber criminals who seek sensitive information from it (Chigada & Madzinga, 2020).

One of the cyber-attacks that was more frequent during the COVID-19 pandemic was a phishing attack. Many studies, governments, and security firms reported on the increased number of phishing attacks (Al-Qahtani & Cresci, 2022). The Anti-Phishing Working Group report of 2020 reported on the last three quarters as follows on the number of phishing sites detected: quarter two 182 465 sites, quarter three 266 387, and four quarter 138 328 (Anti-Phishing Working Group, 2020). Furthermore, the Anti-Phishing Working Group reported in the same year the following number of email phishing: quarter two 112 163, quarter three 122 359, and quarter four 132 553 (Anti-Phishing Working Group, 2020). Similarly, The Mimecast report of 2021 shows that 36% of data breaches were done through phishing attacks (Mimecast, 2019). Moreover, the Kaspersky report of 2022 showed that the number of victims

of phishing attacks at the individual and corporate level in Africa was estimated at 8.7% (Kaspersky, 2022).

2.9 Phishing Awareness Program

The cyber security experts developed a phishing awareness program at university for end users. This program included tools and knowledge that are necessary to minimize phishing attacks. The program also included periodic campaigns that consisted of simulated attacks and successful attacks directed users to a web page. The web page contained warning messages and tips about phishing attacks (University of San Diego, 2017). However, Aldawood & Skiner (2019) argued that phishing awareness campaigns and training were not enough for a cyber-security program. The program should also include the identification of end-users at high risk of phishing attacks like new employees (Broadhurst et al, 2018).

Computer networks were at risk of data breaches from end-users who were not aware of these breaches. Therefore, cyber awareness programs play a crucial role in shaping the online behaviour of end-users. These programs included cybersecurity training that can help in addressing the level of user awareness in cyberattacks. The study showed that user awareness was high after cybersecurity training compared to the state before the training. This study included many surveys among the various organization. The purpose of this study was to check the level of cybersecurity awareness before and after the training. The findings of this study proved that only 38 percent of users complied with information security policy and rules before the training while 70 percent of users complied after the training (Stefaniuk, 2020).

Phishers exploit the behaviour of end-users that makes them vulnerable to attack. Some of these behaviours included clicking on the link without checking its authenticity. Other end-users displayed irresponsible behaviour by responding to suspicious emails due to curiosity. This behaviour led many end-users to become victims of phishing attacks through emails and websites. Thus, the lack of awareness programs led to an increase in the number of victims (Gardner & Thomas, 2014). Even though some organizations launched phishing awareness campaigns, many end-users were still unwilling to change the behaviours that exposed them to cyber-attacks. These end-users ignored the company’s policies and procedures that contained various countermeasures and risks of phishing attacks (Hadlington et al., 2019).

2.10 Types of Phishing Awareness Programs

2.10.1 Cybersecurity education

Gardner & Thomas (2014) defined cybersecurity awareness as a program that enables an organization to inform end-users about potential cyber threats. End-user awareness could lead to responsible online behaviour. Similarly, other cybersecurity experts defined cybersecurity awareness as a program that guides the use of IT systems and electronic information to the end-users. The end-users are also informed about the punishment for not following the rules for the proper use of IT systems and information (Wilson & Hash, 2003).

The awareness program equipped end-users with cybersecurity knowledge and training that made them less susceptible to phishing attacks. A phishing attack experiment within an educational institute showed that students who have cybersecurity courses and participated in cybersecurity activities were less prone to phishing attacks, while students who did not participate in any cybersecurity activities had a high chance of being the victim of phishing attacks (Diaz, Sherman & Joshi, 2018). Phishing attacks were rapidly increasing in many African countries due to the absence of a national awareness program for cybersecurity. The lack of this program left many end-users in these countries prone to phishing attacks with the increase of the usage of internet services (Bada et al, 2019).

2.10.2 Training and Skills

The training of users is needed in the fight against cybercrime, and some cybersecurity courses focused on phishing attacks. Citizens of some developing countries benefited from these courses. In these countries, much of the population uses the internet in their daily activities. The excess usage of cyberspace could make people prone to phishing attacks. Furthermore, cybersecurity professionals offered these courses as seminars and training. They were designed to equip people to deal with phishing attacks. Additionally, phishing attacks had severe consequences among end-users and these countries introduced regulations and legislation. They minimized the number of phishing threats and punished non-compliance, which could address the online behaviour of end-users (Innab, Al-Rashoud, Al-Mahawes & Al-Shehri, 2018).

However, some cyber-security training was ineffective since it was more interesting to one group of users within a particular organization and led to a low participation rate from other groups. A study in an IT organization focused on the participation rate of users in awareness training. The findings showed a high participation rate from developers and low participation

from other users. Developers showed interest in the awareness training because the trainer used a game application. Additionally, the lack of engagement from users can lead to irresponsible online behaviour (Butgereit, 2018).

The lack of interest among employees in the compliance of cybersecurity policies was because many organizations did not invest in phishing training the same way they invested in phishing detection technologies such as intrusion detection, firewalls, and more. A study demonstrated that Technology was not enough to counter phishing attacks. The digital certificate was one of the technologies used to check the authenticity of websites. A study found that the use of digital certificates was not enough to prevent phishing attacks. Security experts investigated 10000 phishing websites, and they revealed the use of valid digital certificates. While on the other side, they also analysed 40000 genuine websites which also had valid certificates. (Drury & Meyer, 2019: 211-222).

Besides policies, a study proposed using phishing awareness training to shape users' behaviours. The organization training needed to focus on the identified behaviours: management of passwords, regular security and software updates, exposing of sensitive information online, links and attachment (Kuraku, Kalla, Smith & Samaah, 2023). However, an investigation demonstrated that gender plays a role in phishing awareness training among Thai users. The findings showed that females were more aware of phishing attacks than males (Daengsi, Pornpongtechavanich and Wuttidittachotti, 2022).

2.11 Phishing attacks at Institution of higher education

In Africa, educational institutions were also affected by phishing attacks. The investigator surveyed technical staff who worked with IT resources at the institutions. The survey showed that 335 over 1164 participants were victims of phishing attacks (Sinan, Nwoacha, Ukhurebor, Degila & Onashoga, Enoyoze & Emmanuel, 2024). Moreover, phishing attacks affected universities outside Africa. A phishing experiment within a student community in the USA showed that new users, such as first-year and international students, were more susceptible to phishing attacks on the computer network (Broadhurst et al, 2018). Another experiment of phishing attacks took place at universities in Nigeria among 480 students. It showed that the hackers deceived 92 students with links shared via social media, whereas phishers also tricked 132 students with other links distributed via email to collect users' data (Akazue, Ojugo, Yoro, Malasowe & Nwankwo, 2022).

Phishers at the universities deployed phishing attacks using different strategies to trick users into revealing their personal information or installing malware within the computer's infrastructure. A case study at a leading university in Nigeria showed that hackers deceived students using phishing emails embedded with malicious links to redirect users to cloned websites of school websites (Okokpujie, Kennedy, Nnodu & Noma-Osagha, 2023). Moreover, interviews at the University of the Western Cape in South Africa demonstrated that phishers distributed phishing emails. These emails contained promises of rewards by clicking links, and other users received malicious links through online adverts (Nyasvisvo and Chigada, 2023). Additionally, an investigation at several universities in Nigeria showed that phishers used generic, tailored, and spear phishing. The phishers used no personal information in the generic emails sent to users, and they sent them to many users. In the tailored phishing, the hackers impersonated the institution of education. Lastly, phishers sent spear phishing to users with their personal information (Yoro et al., 2023).

In the effort to counter phishing attacks within the universities, awareness was introduced as part of the cybersecurity education. However, cybersecurity education was also a challenge in some developing countries due to the lack of highly qualified professionals in the cybersecurity field. Many higher education systems in these countries did not produce enough cybersecurity professionals. Furthermore, these institutions did not possess courses to train and educate cybersecurity professionals. Cybersecurity professionals were high in demand due to the increasing cyber-attacks. Researchers conducted a study in higher education institutions. Their study involved a series of interviews among 28 universities. The findings of this study showed that only four institutions out of twenty-eight could deliver training and education for cybersecurity professionals (Catota, Granger & Sticker, 2019).

Additionally, cybersecurity research within universities in countries such as Finland remained low at the national level. Low research output at the national level can lead to a low level of cyber-attack awareness among end-users in the country (Letho, 2015). Furthermore, in African countries such as South Africa, where cyber awareness was deficient, end-users were at high risk of falling victim to phishing attacks. Especially the universities where students were always on the internet. Non-IT students were more vulnerable because their courses did not include cybersecurity (Venter, Blignaut, Renaud & Venter, 2019).

2.12 Summary

The advances in computer networks have allowed the interconnection of computer resources from anywhere with internet access. This innovation has also brought some security

challenges. These challenges are cyberattacks ranging from man-in-the-middle to phishing attacks. To counter these attacks, cyber security experts have implemented security technologies. Phishing attacks can bypass security technologies by tricking users into disclosing confidential information or installing malware. The attackers launched phishing attacks in different ways, such as email, vishing, etc. The number of phishing attacks remained high since cyber security experts detected them for the first time. The experts introduced phishing awareness to mitigate attacks by educating and training users. However, there were some challenges to the effectiveness of this program among many institutes of higher education.

3 CHAPTER THREE: RESEARCH METHODOLOGY & UNDERPINNING THEORY

Society has new challenges every day. Many of these challenges arise in the field of cybersecurity. Researchers can address these challenges by using specific research questions. These questions can lead to understanding or provision of solutions to those problems (Davidaviciene, 2018). Similarly, research is about asking the right questions to find answers to challenges that arise in society. Answers to the challenges are usually a product of well-defined steps in research methodology (Du Plooy-Cilliers, Davis & Bezuidenhout, 2014).

This chapter comprises the following sections: research paradigm (3.1) research approach (research approach), research strategy (3.3), sampling (3.4), data collection methods (3.5), data analysis (3.6) and ethical considerations (3.7). Furthermore, is addresses the need for ethical approval (3.8) and concludes with underpinning theory (3.9). This content of these sections enabled the author to meet research objectives and answer the research questions set out in Chapter 1 (1.5 and 1.6).

3.1 Research Paradigm

The production of scientific knowledge consists of the following elements: theories, methods, and techniques. These elements are the basis of scientific knowledge as they are a series of rigorous procedures that the researcher needs to follow to get to an acceptable conclusion about a problem in a particular field of study. Research paradigms enable the researcher to think about the theories, methods, and techniques to solve a problem in the world. Different types of research paradigms lead to specific interpretations of the problem in a particular field of study. These research paradigms are a set of techniques. The techniques are universally accepted to address a problem in the world (Richards, 2003).

Furthermore, the researcher can use paradigms to understand the problems in the world. Paradigms can also lead to the understanding of individuals and their relationships in the world. An understanding of the world, individuals, and relationships could lead to a potential solution to the problems in the world (Richards, 2003). There are types of paradigms such as positivism, interpretivism, critical theory, constructivism and pragmatism, and epistemology and ontology are element to consider when selecting a research paradigm.

Epistemology consists of acquiring knowledge about problems in the world. The researchers that use this paradigm have their own way of interpreting the results of an issue under investigation (Moon & Blackman, 2014). This paradigm enables the researcher to choose research methods that lead to the production of scientific knowledge to solve problems in the world (Moon & Blackman, 2014). The following research methods: questionnaires, attitude scale, participant observation, and random samples are an example of epistemology choices taken by a researcher (Moon & Blackman, 2014). These methods produce empirical evidence that helps positivist researchers control and predict world issues (Plooy-Cilliers et al., 2014).

On the other hand, ontology seeks to look at the existence or the reality of things from which the research can draw knowledge (Moon & Blackman, 2014). Knowing the reality of the problems in the world can assist researchers with certain assumptions. The assumptions can help the investigation of a problem. (Plooy-Cilliers et al., 2014).

In this study, the researcher used interpretivism because the researcher sought to understand phishing awareness through qualitative research methods to develop a framework for it.

3.2 Research Approach

A particular research approach can influence the type of research strategies chosen. A qualitative approach would lead to a case study, while quantitative research can result in a survey. Furthermore, the research approach dictates the type of sampling and data collection instruments (Bryman & Bell, 2011).

3.2.1 Qualitative approach

The following are two types of research: qualitative and quantitative research. Each type of research has its advantages and disadvantages. This study uses the qualitative research approach because its benefits supports the meeting of the research objectives. The objective of this research is to investigate phishing attacks and develop a phishing awareness program. A qualitative study allows the study to gather in-depth information from the participants to examine the phishing attacks on the University of Technology's computer network. Furthermore, phishing attacks involve the manipulation of human attributes such as relationships, fear, curiosity, and so on; a qualitative study enables efforts to understand these human attributes in phishing attacks. On the other hand, a qualitative study is a subjective research approach, and this kind of approach looks at intangible things such as

perceptions, values, and attitudes (Neville, 2005). Furthermore, qualitative research is used in non-statistical studies (Marczyk, DeMatteo & Festinger, 2005).
The investigation of phishing attacks requires a qualitative approach because a qualitative study produces rich data that enables the understanding of a phenomenon, even though the results cannot be validated in a precise manner (Bernard, 2013). Rich data in the qualitative approach are mainly due to the nature of research questions. These questions are flexible to give the researcher the ability to collect more data. This flexibility could be crucial to the understanding of other issues that the researcher was not aware them (Bryman & bell, 2011).

3.2.2 Quantitative approach

A quantitative approach is an approach that produces enough data through repeatable techniques, and the results can be validated in an accurate way (Bernard, 2013). Additionally, in the quantitative approach, data is collected using statistical tools that does not lead to thick and rich, in-depth information which addresses the phishing awareness among the network users. A quantitative approach makes it difficult to analyse the human attributes (Kumar, 2011). Furthermore, a quantitative study is suitable for research that aims to measure scale, range, and frequency data. This result leads to a lack of flexibility that can prevent the researcher from understanding perceptions and attitudes about problem in depth (Kumar, 2011).

3.3 Research Strategy: Case study

A survey is a research strategy that involves a large population which could be time-consuming and require more resources. However, there are no resources or time to conduct a study on a large scale (Alan, 2016). Additionally, surveys were used in quantitative research where closed-ended questionnaires were developed to collect data from participants. Closed-end questions were not flexible and may have prevented this study from getting the desired results (Bernard, 2013). Surveys are also considered superficial because their structures do not allow the investigator to dig deep into the problem (Mouton, 2001). There is also another research strategy called experimental design. An experimental design is used to conduct a study in laboratory settings where the results of the experiment are compared to other results and measure repeatable. This type of research is not convenient for the development and investigation of phishing awareness attacks (Mouton, 2001). However, a case study is a research strategy that is often made of the following: individuals, a group, a community, an instance, an episode, an event, a subgroup of a population, a

town, or a city that enabled the researcher to collect in-depth information for qualitative studies (Neuman, 2014). This study used a case study research strategy because it is often associated with qualitative studies (Kumar, 2011). This research focused on the users within the University of Technology to gather information necessary to combat phishing attacks.

3.4 Target Population, Sampling Techniques and the Sample

3.4.1 Target Population

The population in this study consisted of university academics, first-year and third-year students and industry experts in the Western Cape, South Africa. Of this large population, a small but representative group of people was selected (Neuman, 2014). The sample group of people in the study provided rich and relevant information that enabled the study to answer the research questions to some extent (Ritchie & Lewis, 2003). In this study, the population comprised users within the University of Technology. This group of users intensively used the computer network for various activities that included the sharing of confidential information. Confidential information is sought after by phishers.

This study's population comprised all universities in the Western Cape province of the Republic of South Africa. Due to time constraints, the study focused on one University of Technology in the province.

3.4.2 Sampling Techniques

Non-probability sampling is a sampling technique that involves the selection of a small group within a large population. The small group represents the entire population under the investigation. A group of users at the University of Technology represented the population of all users who belong to the University’s computer networks (Neuman, 2014). In contrast, probability sampling consisted of giving each person within a large population a chance of being part of an inquiry. Giving every individual a chance to participate in the study is not feasible due to the time frame of this research (Kothari, 2004). There are various non-probability sampling types, which are as follows: quota, convenience, purposive, self-selection, and snowball (Greener, 2008).

Convenience sampling is selecting participants who are easy to find and willing to take part in the inquiry without clear criteria. These participants may lack knowledge of the problem under investigation, hindering the researcher from meeting the research's objective (Ritchie & Lewis, 2003). However, a purposive sampling method involved selecting a group of informants

representing a large population. These informants know the problem under investigation (Kothari, 2004). Furthermore, the purposive sampling method aligned with the research strategy selected in this study (Greener, 2008).

In this study, the University of Technology was selected because it uses the following platforms in its daily activities: emails, SMSes, phones, and websites. Phishers use these platforms to launch their attacks against users. These users were the participants in this investigation as they were the target of the attacks and were made up of IT technical, academic staff, and students.

3.4.3 The Sample

The sample in this study comprised a small group of participants, studied and chosen according to their background and experience on the matter being investigated. This study involved users on the computer network of the University of Technology within the Department of Information Technology. The number of participants selected depended on the data collected.

In this study, there were three categories of participants: 28 first-year (n=8) and third-year students (n=20), 15 academics and two IT technical. Experts. The selected third-year students were studying either an Advanced Diploma in ICT: Application Development (n=12) or an Advanced Diploma in Communications Networks (n=8). The total number of participants was 45. The students reported studying at the case study university for periods ranging between one and seven years. The eight first-year students were enrolled in a Diploma in Information Technology: Application Development stream. Selected academics comprised one professor, one senior lecturer, two academic leaders, ten IT lecturers and one IT technician. Academic experience reportedly ranged between 4 months and 27 years. Two IT technical experts participated in the study. They respectively filled industry positions in management (2 years in the role) and IT strategic services (4 years of company service). Their selection contributed acumen and experience in the cybersecurity discipline and, hence, the phishing domain.

3.5 Data Collection Methods

This study used surveys via questionnaires as a data collection method. Questionnaires are used mostly in quantitative studies. However, previous studies demonstrated that a well-designed questionnaire could help informers to provide memories, opinions, and experiences about the subject investigation. It also gives the respondents the ability to go back to the

previous answers to modify them before sending them to the investigator (Byström, Ruthven and Heinström, 2017). This method of data collection was crucial in addressing the phishing awareness attacks on the university computer network. Furthermore, the questionnaire consisted of a list of questions that addressed a group of participants. This group was a representation of a targeted population (Nicholas, French & Valentine, 2010). This group was responsible for interpreting the meaning of the questions without the intervention of the researcher. The researcher ensured that the questions were easy to understand and in the correct order (Kumar, 2011). Prior to the administration of the questionnaires, the researcher sent a request to the organisation where the participants were selected. The request explained the purpose, importance of the research, and ethical issues to be addressed during the collection of data. The ethical approval letter can be found in the appendices of this study. Once the request was approved, the researcher selected a small sample purposively and conveniently to represent the large group to respond to the questionnaire.

The researcher collected data from the following groups: students, academics, and IT technical. The student category was made up of first-year students who are 8 and 20 years old and third-year. These students were part of the IT department within the Informatics design faculty. The academics were 15 lecturers in the Department of IT within the Faculty of Informatics and Design. The IT technical category was made up of 1 manager of IT strategic services and one information security officer. These agents were responsible for the IT services for the entire university. These services included network services, hardware and software, printing, admin systems, emails, and telephony.

This study used the questionnaire built around open-ended questions as a data collection tool because it allowed the informant to provide qualitative information that they considered essential in their views without being constrained by sensitive questions (Nicholas, French & Valentine, 2010). Furthermore, the questionnaires enabled the respondents to answer the questions anonymously, which led to more accurate answers; This collection method was convenient as, in some instances, the participants were located at remote locations. Lastly, the questionnaire enabled the researcher to save time and finances since the questionnaires could be sent using online tools to collect data (Kumar, 2011).

Table 3.1 Research Objectives, Sample and Data Collection

Research Objectives	Sample	Data Collection Tools
1. To identify the frequency of phishing attacks at a University of Technology	IT technical, academic staff and students	Questionnaire

2. To determine the strategies used to deploy phishing attacks on a University of Technology network	IT technical, academic staff and students	Questionnaire
3. To establish the awareness level of phishing attacks among end-users at a University of Technology	IT technical, academic staff and students	Questionnaire
4. 4. To investigate the nature of a phishing attack awareness program at a University of Technology?	IT technical, academic staff and students	Questionnaire

In this inquiry, the researcher used online survey questionnaires for the respondents. The researcher aimed to have broader and contextual information from participants about phishing attack awareness within the institution. Before answering the online questionnaires, the researcher provided a research brief to participants. The research brief contained the rationale of the study. The researcher guaranteed the confidentiality of participant responses.

The researcher collected data from the following groups: students, academics, the Manager of IT Strategic Services, and the Information Security Officer. Students and academics are ordinary users who use the computer network to do their daily activities. The manager of IT Strategic Services and Information Security Officer users are experts who manage the computer network and develop phishing attack awareness for users.

The study involved 8 first-year and 20 third-year students, 15 academics within the department of ICT, one manager of IT Strategic Services, and one Information Security Officer.

Y Educational Institution is one of the biggest tertiary institutions in the Western Cape Province. It is internationally recognized and can accommodate more than 30,000 students. The institution comprises six faculties offering undergraduate and postgraduate studies in the following fields: Applied Sciences, Business, Education and Social Sciences, Engineering, Informatics and Design, and Health and Wellness Sciences.

The institution uses the computer network to facilitate students' learning and assist staff in their daily activities.

3.6 Data Analysis

Thematic analysis is a data analysis method that identifies, analyses, and reports patterns on rich data. The data is analysed based on the problem under investigation to get the research outcome (Braun & Clarke, 2006). Additionally, thematic analysis is used in the qualitative study, where data is collected and analysed from the participants' perspectives and experiences (Aronson, 1995). Qualitative data in this study was analysed in six main steps to identify major themes and patterns in the data set. The section below details these steps (Marguire & Dlahunt, 2017).

The researcher used thematic analysis as a data analysis method. This method consisted of recording the raw data from the participants. The researcher organised the data according to the research questions and developed codes based on the main elements emanating from the data. The researcher created themes based on patterns emerging from the codes.

The six steps are as follows:

Step 1: Familiarity with data

The researcher is required to know in-depth data obtained from interviews. The data collected should be written in Word format. The word structure would enable the researcher to read through the data several times to become familiar with it.

Step 2: Generating codes

Data from interviews are usually raw, which is difficult to understand. Therefore, the researcher should organize it in a form that makes it easier to understand. The researcher should arrange data in line with the research questions. This arrangement would allow the researcher to capture any element of the research questions. The study referred to those elements as code because they are crucial to the analysis of data.

Step 3: Seeking themes

The codes that the researcher has identified in step two support the creation of themes. The initial themes emerge from codes that overlap. The other themes result from codes that are related to each other. These themes are being developed regarding the research questions.

Step 4: Reviewing of themes

In this step, the researcher reviews themes developed in the previous phase. This revision ensures that themes align with research questions and are meaningful. Additionally, these themes should be representative of the data from which the researcher drew them. There are several tools for reviewing themes, such as an Excel sheet.

Step 5: Define themes

After identifying the themes, the researcher needs to define them by examining their meaning, relation to the primary theme, and relationship to each other.

Step 6: Report

In the last step, a report needs to be written about the analysis of data.

This analysis method is suitable for qualitative studies as textual data is categorized under a theme. The themes are then used to create patterns and relationships that enable this study's data to analyse qualitative data.

In this study, the researcher obtained data from Google Forms and converted it into a Word document. The researcher read the data multiple times. The investigator moved the data to an Excel spreadsheet and organized it in a manner that was easy to understand. The researcher aligned the arrangement of this data according to the study research questions. The researcher drew some key terms emerging from the data and reviewed the patterns and relationships among them, and they were also defined. The investigator reported on the analysis of the data in the study.

3.7 Ethical Considerations

3.7.1 Privacy

All participants in this investigation received assurance from the researcher that their information would remain strictly confidential.

3.7.2 Confidentiality

The participants provided written approval before recording the interview. Interview audio files were kept securely by encrypting the folder with a complex password.

3.7.3 Consent

Before collecting data from the participants, the researcher explained the purpose of the investigation to the participants. The participants received assurance from the researcher that the information shared would remain confidential and only be used for the study.

3.8 Ethical Approval

The investigator applied for an ethical approval letter from the Research Ethics Committee of the University of Technology. In the application, the researcher described the ethical protocols and the research process for data collection. The ethical protocols and research process were as follows:

- The researcher provided the title and description of the research. In this section, the researcher included a research brief, the aims of the study, the research questions, and the research methodologies.
- In this part, the investigator explained to the ethics committee that the study would not harm any participants.
- The investigator kept the participants' identities anonymous when collecting data, and the researcher treated them equally.
- No harm to the environment would occur since the study aimed to develop a phishing awareness program.
- The researcher selected participants who are end-users of the University's computer network. These users are staff members and students.
- The researcher did not provide any incentive to the participants, and their participation would be voluntary.
- The participants were not obliged to answer all the questions, and no collection of personal data would occur.
- The investigator collected responses after conducting the questionnaires. The researcher stored responses on online storage, which required access passwords.
- The researcher ensured confidentiality, privacy, and anonymity by not collecting personal information since the study aims to develop a phishing awareness program.
- The researcher guaranteed that the study would not result in a conflict of interest since only one organization was involved, and no financial involvement was needed as the study aims to develop a phishing awareness program.

The Research Ethics Committee approved the above research procedure and ethics of the study as per APPENDIX A.

3.9 Underpinning Theory

3.9.1 Theoretical framework

The theoretical framework enabled the researcher to set the parameters for the literature review. The settings allowed the researcher to focus the literature on the topic under investigation. The theoretical framework is a valuable tool to guide the researcher through relevant literature. The researcher may try to deviate from the topic because the research problem has roots in various theories. The framework can also help the researcher organize the literature review according to the main theories or themes (Kumar, 2011). Table 3.3 illustrates the common frameworks used in the prevention of phishing attacks.

Table 3.2 Common Frameworks Applied in the Prevention of Phishing Attacks

Technology Threats Avoidance Theory (TTAT)	Perceived Behavioural Control (PBC)	General Deterrence Theory (GDT)
"Technology Threats Avoidance Theory: A Theoretical Perspective" (Liang & Xue, 2009: 71-90).	"Modelling anti-malware use intention of university students in a developing country using the theory of planned behaviour" (Vafaei-Zadeh, Thurasamy & Hanifah, 2019)	"User awareness of security countermeasures and its impact on Information Systems misuse: a deterrence approach" (D'Arcy, Hovav and Galletta, 2009)
Technology Threats Avoidance Theory (TTAT````) framework enabled individual IT users to avoid malicious IT threats. To prevent IT threats, TTAT introduced two processes. The first process is called threat appraisal, which consists of methods to convince the IT users of IT threats and severe consequences of IT threats. The second process is referred to as coping appraisal. After the persuasion of IT threats, the IT users used the available safeguard measures to defend against malicious IT attacks.	PBC was used in a study investigating the attitude of students towards the use of anti-malware software. The PBC was used to check the impact of the perceived price level of anti-malware software and information security awareness on the students' attitude use of anti-malware software. The findings showed that the perceived price level harmed the student's attitude. In contrast, information security awareness had a positive effect on the student's perspective on anti-malware software.	GDT was used to reduce intentional insider security threats to information systems (IS) resources. GDT enabled the researcher to create deterrent practices that reduce the amount of intentional insider security threats. A study was conducted using three practices to deter the misuse of IS. The three practices were user awareness of security policies, security education, training and awareness programs, and computer monitoring. These practices were tested on 269 computer users from eight different companies. The results showed that these practices reduced the insider security threats and the perceived severity of punishment also showed the reduction of insider security threats on IS within companies.

The table above discusses and provides attributes of the theoretical frameworks used in cybersecurity studies.

The section below presents the Technology Threats Avoidance Theory (TTAT), the theoretical framework that the researcher uses to scaffold the study.

3.9.2 Adoption of the Technology Threats Avoidance Theory Framework

The Technology Threats Avoidance Theory (TTAT) framework is the proposed framework for this study as it could enable the IT users within the University's network to avoid malicious phishing attacks. To minimize these cyberattacks, users were made aware of phishing attacks and their severe sequences. Lastly, users were educated about various

countermeasures to defend against phishing attacks (Liang & Xue, 2009). TTAT has also been used in several studies, such as the two studies mentioned in Table 3.3 below.
In this study, after analysing the phishing attack awareness among the end-users, TTAT supported the development of the awareness program. The TTAT ensured that the awareness program included the elements of threat appraisal. The threats appraisal was included by ensuring that end-users on the University‘s computer network are presented with information about the occurrence and the negative impact of phishing attacks. The provision of this information may lead users to change their irresponsible behaviour while on the computer network. Additionally, TTAT ensured the awareness program has various mechanisms or tools against phishing attacks. The end-users should also be familiar with various mitigation techniques to minimize the impact of phishing attacks on the University’s computer networks.

3.9.3 Related Work

Table 3.3 A Selection of TTAT Studies

Authors	Country	Paper Title	Methods	Findings
Arachchilage & Love (2013)	United Kingdom	A game design framework for avoiding phishing attacks	Surveys Questionnaires	The finding of this study revealed that a game designed to educate IT users should have the following elements: perceived threat, safeguard effectiveness, safeguard cost, self-efficacy, perceived severity, and susceptibility to being successful in educating users to become more responsible online.
Rakhra & Kaur (2018)	India	Studying User’s Computer Security Behaviour in Developing an Effective Anti-phishing Educational Framework	Literature	The study focused on guiding the design of the educational security framework that enabled users to identify phishing attacks they encounter on various online platforms such as websites, email, and so on.

The TTAT framework was used in many types of information technology research, including studies on phishing attacks. Table 3.3 above illustrates two such studies.

4 CHAPTER FOUR: RESULTS AND DISCUSSION OF FINDINGS

Research questions were addressed by mapping them to questionnaire items. This process produced a code book showing emergent themes and associated codes. APPENDIX B concretises and illustrates the relationships between research questions, questionnaire items, emergent codes and associated themes. However, this chapter reports the major findings gleaned from student, academic and IT expert questionnaires, acquired via digital distribution. Whilst students and academics were exposed to identical questionnaire items (APPENDIX C), specific industry-related items comprised the IT expert questionnaires (APPENDIX D).

4.1 Introduction

The previous chapter discussed the research method used to carry out this study which included the research paradigm, research approach, research strategy, sampling and data collection methods, data analysis, ethical considerations, ethical approval, and underpinning theory.

This chapter presents, analyses, and interprets the collected results of the study and discusses the findings.

The main question of this study is how to develop a phishing attack awareness framework for educating users about phishing attacks at the University of Technology in the Western Cape. To answer this question, the study gathered data from the different sets of research participants which include students, academics, and IT experts. So, this section presents the collected results that bring answers to the proposed research questions posed in Chapter 1. These results inform the development of the phishing awareness framework for users in the University of Technology in the Western Cape. This model had the goal of educating users about phishing attacks.

4.2 Results – Demographic Information

Section 3.4.3 in Chapter 3 provides a summary of the demographic information associated with the sample of participants who contributed to this research report's results.

4.3 Results – Students and Academics

The results presented in this section are based on the responses from students and academics. The researcher surveyed students and academics within the Department of IT at the University of Technology in the Western Cape.

4.3.1 Have you ever received a phishing attack while working at this organisation?

Student perspective

Thirty-nine (39%) per cent of the students received phishing attacks, while 61 % did not (Figure 4.1).

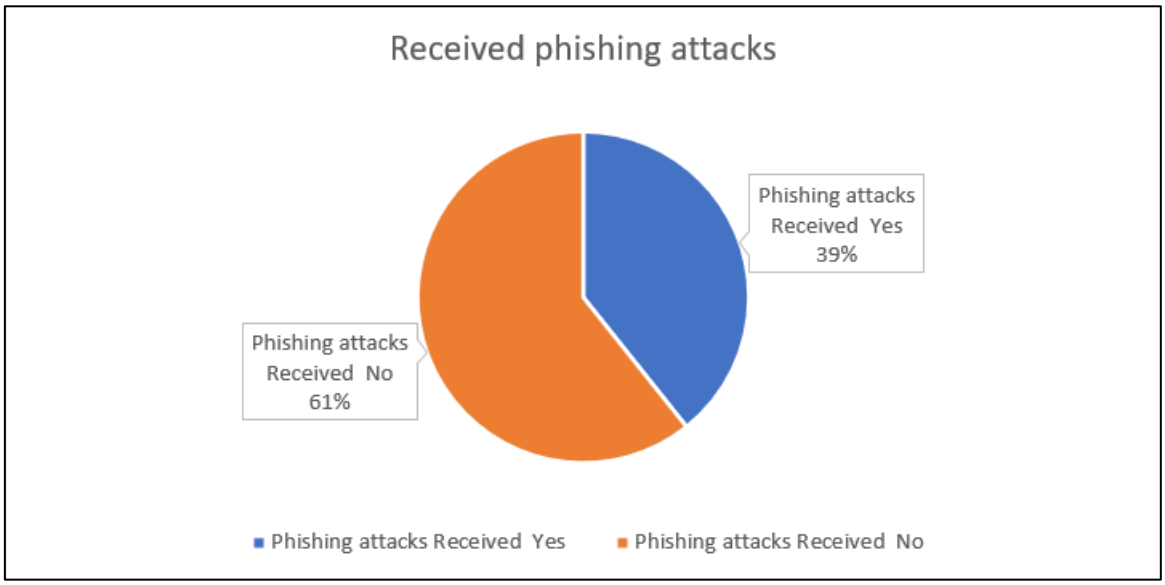


Figure 4.1 Phishing attacks: 2023 - student data

Academic perspective

The researcher led a survey among academics, where 64% confirmed they had received phishing attacks, while 36% did not receive them (Figure 4.2).

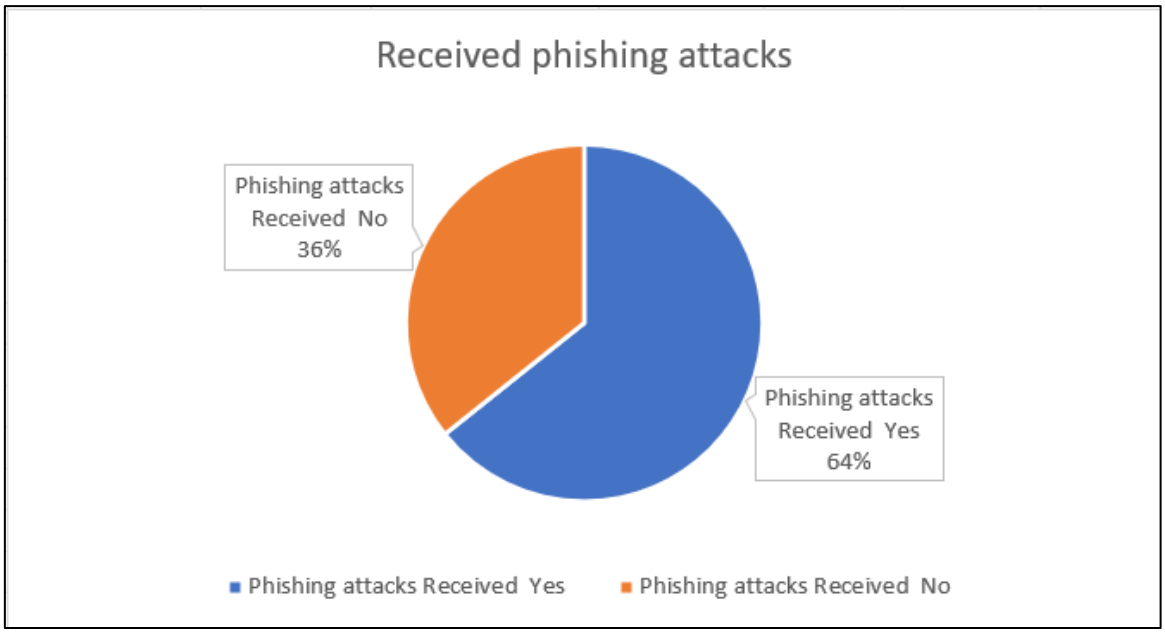


Figure 4.2 Phishing attacks: 2023 – Academics Data

4.3.2 Do you know of any users who have been victims of a phishing attack on the university's computer network?

Student perspective

The results revealed that 21 % of students knew victims of phishing attacks who were network users; on the other hand, 79 % did not know (Figure 4.3).

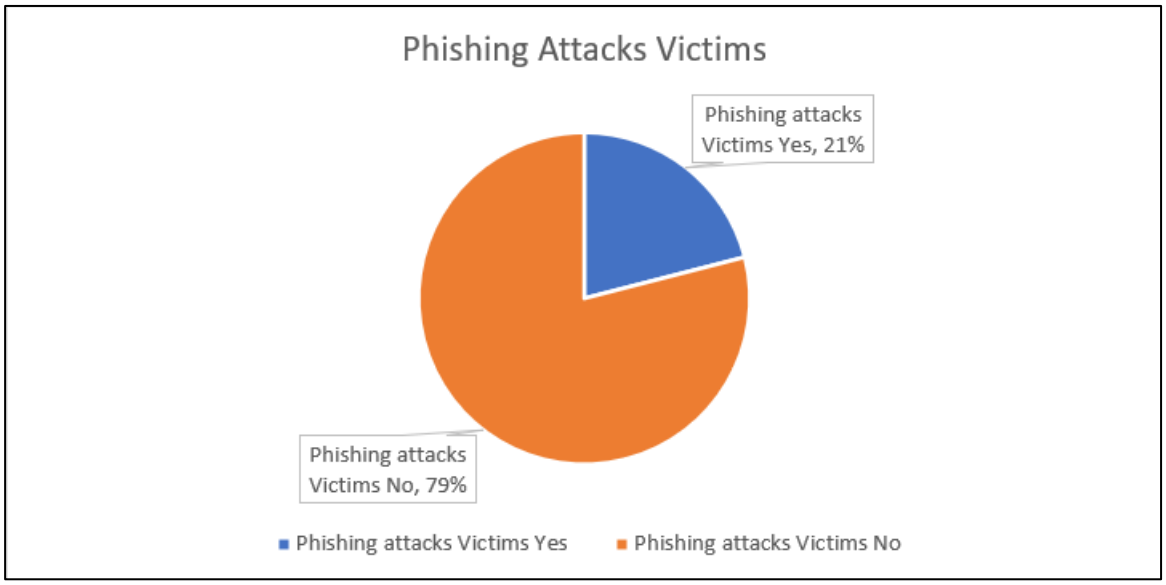


Figure 4.3 Students - Phishing attacks victims: (student perspective)

Academic perspective

Furthermore, 33% of academics in the department revealed that they knew many victims of phishing attacks on the university, and 67% did not know (Figure 4.4).

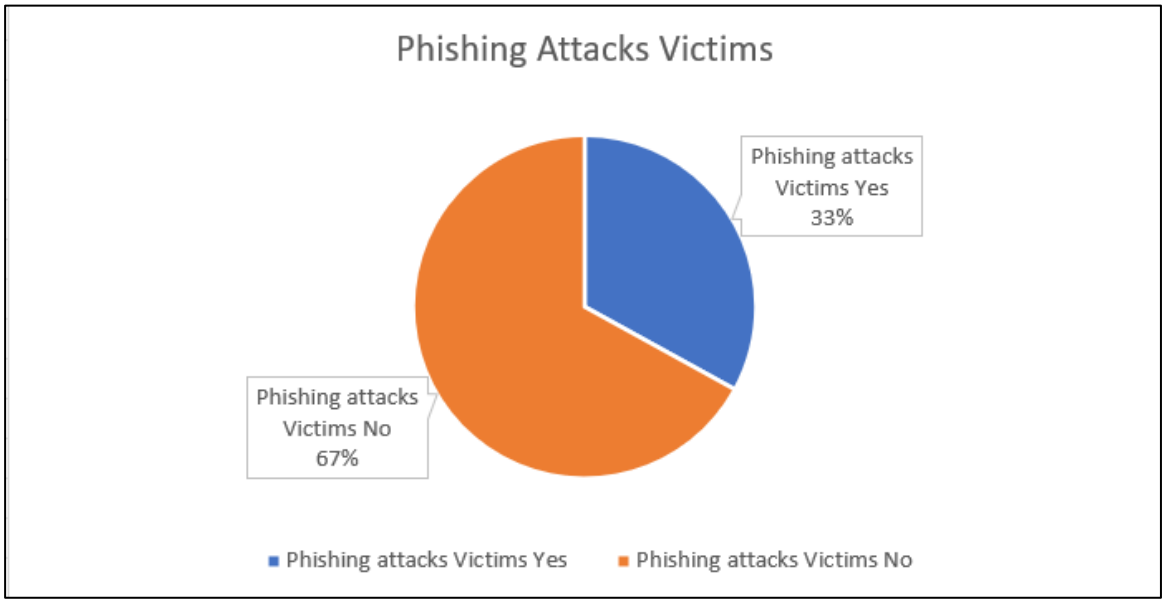


Figure 4.4 Phishing attacks victims: (academics perspective)

4.3.3 Please elaborate on how you received a phishing attack

The researcher sent a questionnaire to students to discover the phishing techniques. The students responded with the following answers: “Received via email, they posed as a legitimate announcement or email from the CTS desk or Newsflash. Asked for users and so on to change one's password and they would say something urgent like due to new security rollouts or protocols have changed or updated or something similar on those grounds. But once I saw some obvious hints of this being a phishing email, I flagged it and deleted it and after that warned my fellow students about this suspicious email.”

“Received an email stating that my account was hacked and that I need to respond to them to get my account back. Also received an email stating sensitive information was leaked off of my phone. Both of which were fake.”

Phishers use the following platforms for phishing activities: SMS, Email, social media, and telephone. Below are the students' percentages and their respective platforms: “79 % of emails, 14 % SMSs, and 7 % social media.”

Student perspective

The researcher sent a questionnaire to students to discover the phishing techniques. The students responded with the following answers: “Received via email, they posed as a legitimate announcement or email from the CTS desk or Newsflash. Asked for users and so on to change one's password and they would say something urgent like due to new security rollouts or protocols have changed or updated or something similar on those grounds. But once I saw some obvious hints of this being a phishing email, I flagged it and deleted it and thereafter warned my fellow students about this suspicious email.”

“Received an email stating that my account was hacked and that I need to respond to them to get my account back. Also received an email stating sensitive information was leaked off of my phone. Both of which were fake.”

Phishers use the following platforms for phishing activities: SMS, Email, social media, and telephone. Below are the students' percentages and their respective platforms: “79 % of emails, 14 % SMSs, and 7 % social media.”

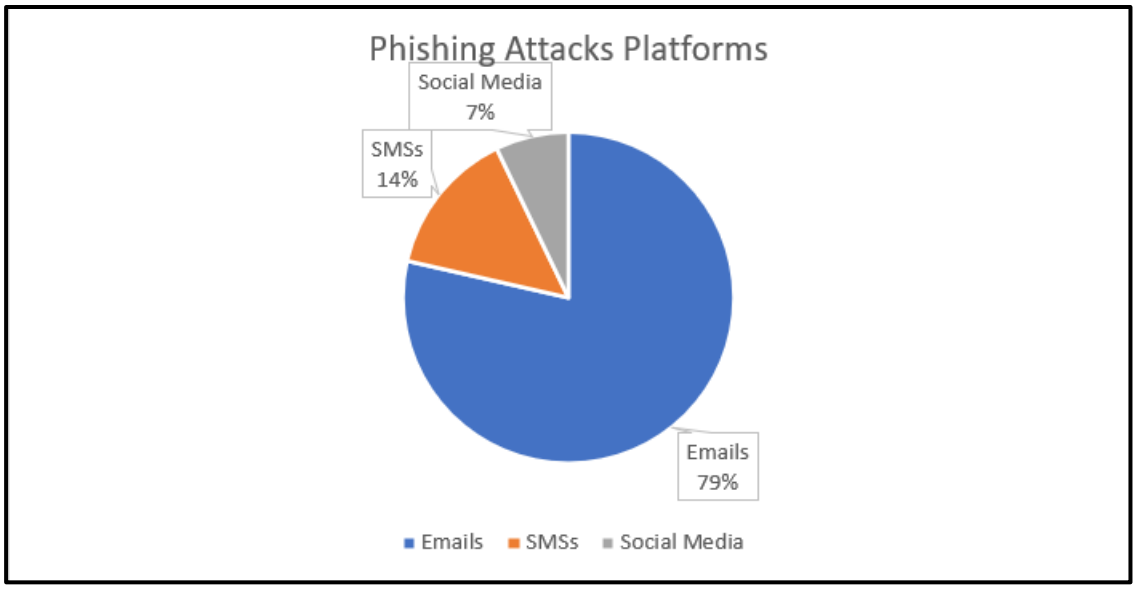


Figure 4.5 Phishing attacks platforms (student perspective)

Academic perspective

The academics reported the following techniques in the questionnaire: “Email was received from an address similar to the institution address but with a slight difference. The email came as across as official communication by the CTS department, but it wasn’t.”

“Was about some aspect where they wanted my login and password to finalize admin processes”.

4.3.4 How often do you receive phishing awareness reminders from the university?

Student perspective

The researcher conducted a survey about phishing awareness reminders. Figure 4.6 illustrates the percentages of the students and their respective periods for reminders: 8 once a month, 4 once a week; 4 once a semester, 4 once a year, 3 once a term, and 3 none”.

Figure 4.6 Students Phishing Reminders

Academic perspective

The academics received phishing awareness reminders in the following manner: 33.3% once a month, 26.7% once a term, 26.7% once a week, 6.7% once a week, and 6.7% none (Figure 4.7).

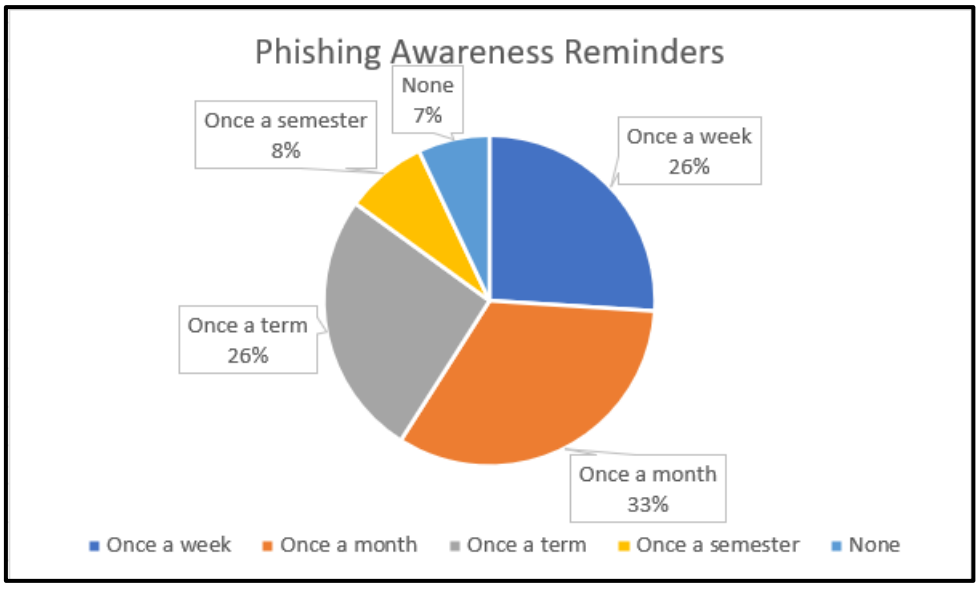


Figure 4.7 Academics phishing reminders

4.3.5 Could you provide some details about your understanding of the phishing attack awareness programme?

A phishing attack awareness program informs end-users about phishing attacks and mitigation techniques. The users are educated by the IT department, as per the responses below from academics: “The CTS department sends out links to videos playing out different scenarios that might occur in the university environment. These videos come up right through the year to help educate end users.” and “It attempts to educate us about aspects of phishing attacks.”

4.4 Results – IT Experts

4.4.1 What is the trend concerning the strategies used by phishing attackers to deploy phishing attacks?

The IT Expert revealed the following techniques in response to the question: “Display name spoofing, especially for business email compromise (BEC) attempts”, and

“It would be the targeting of the user's personal cell phones via SMS and/or WhatsApp.”

4.4.2 Is it true that there is a high number of phishing attacks that impersonate people of authority? If yes, can you elaborate?

The investigator conducted a survey among IT experts within the University of Technology. One of the IT experts gave the following response:

“Yes. We see a spike in this type of attack at the beginning of the year, and at the end, a high number of cases are being reported.” they estimated the percentage of reported phishing attacks at 50. Figure 4.8 outlines feedback received from IT Experts.

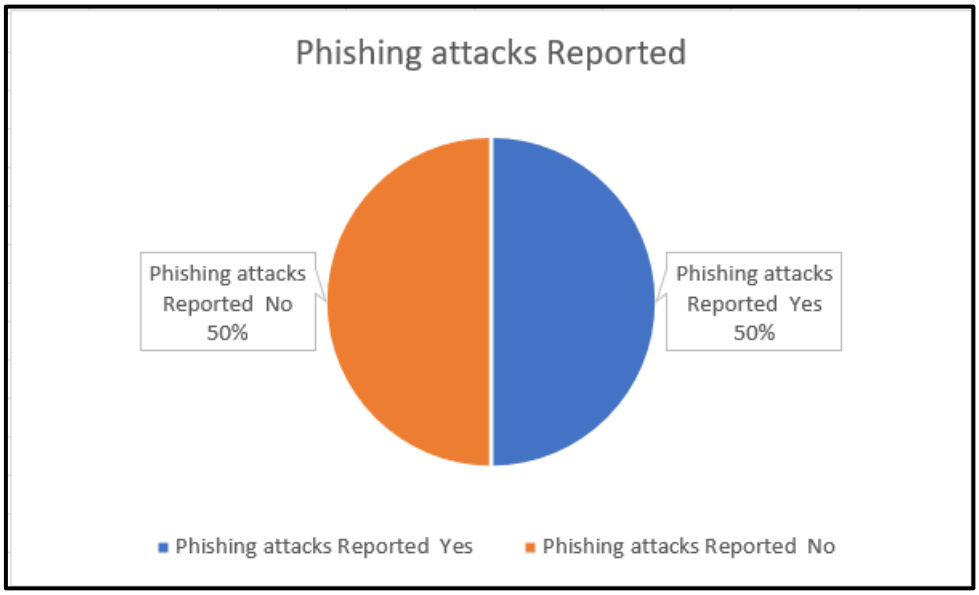


Figure 4.8 Phishing Attacks Reported by IT Experts

4.4.3 What are, on average, the percentages of phishing attacks with links that mimic the legitimate website?

“Those that are coming through to the user, probably 10% - the rest is blocked by our mail security software before reaching the user.” Figure 4.9 summarises feedback from IT Experts.

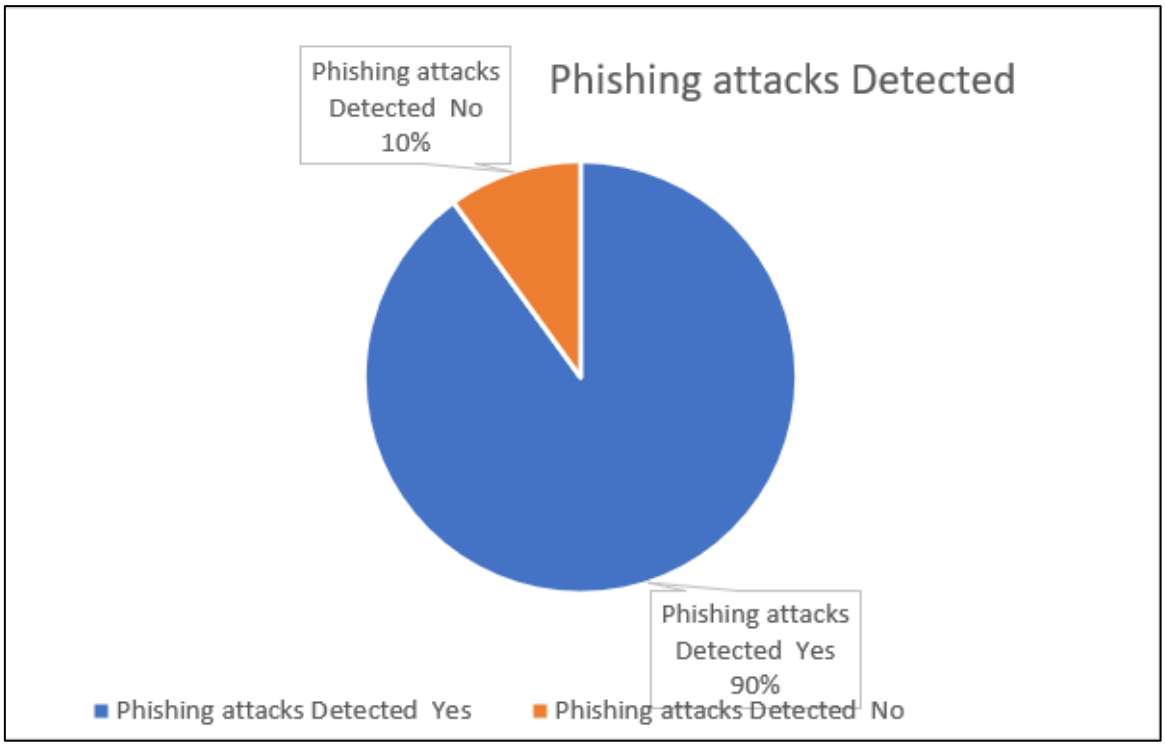


Figure 4.9 Phishing attacks detected and reported by IT Experts

4.4.4 What is the phishing awareness programme made of within the organisation?

The IT experts reported that “Quarterly cyber security awareness modules that include a short video supplemented by a quiz to test knowledge gained as well as quarterly phishing simulation exercises.” (P.4.3.1) and “Cyber Security Awareness Education, different modules and the phishing campaigns. The content includes Phishing, Info Protection, Passwords, and Data in Motion, among other things.”

4.4.5 What do you believe are the key elements that should not be omitted from any phishing awareness programme?

Moreover, the IT experts within the university informed the end users about rules for using computers and related technologies in the following statements: “Constant communication, expressing the impact of cyber risks in a way that resonates with the user base”, and “I believe all three are important for our users at the moment. Our strategy reaches everyone, and they can choose to participate in their time. The Phishing campaigns then test that knowledge. They are not communicated prior; the purpose is to see the user’s first reaction to a phishing email they receive.”

4.5 Discussion and Interpretation of Findings

4.5.1 Frequencies of phishing attacks

The phishing attack is a cyber-attack that is on the rise as per the research conducted within the University of Technology, where a survey of students within the Department of IT revealed that Thirty-nine percent of the students received phishing attacks. Another survey among academics showed 64% received phishing attacks. Similarly, the researcher sent a series of questions to the IT experts, and they responded with the following answers: “Yes. We see a spike at this type of attack at the beginning of the year and at the end, a high number of cases are being reported”, they estimated the percentages of phishing attacks at 50%”, and “Those that are coming through to the user, probably 10% - the rest is blocked by our mail security software before reaching the user.” Moreover, the survey revealed that twenty-one per cent of students knew victims of phishing attacks who were users on the network, and 33% of academics in the department indicated there were many victims of phishing attacks at the university.

On the other hand, many studies demonstrated increased phishing attacks over the years. IT experts discovered phishing attacks for the first time in 1990. It resulted in the creation of fake accounts on America Online (AOL) network systems (Jakobsson & Myers, 2006), and in the year 2018, F5 reported that phishers targeted 71 per cent of users on Google through phishing emails (F5, 2018). Moreover, a study of email phishing at the University of West in England showed that ten thousand email users were victims of phishing attacks in September 2018. These victims were among 4,000 Staff, and 28790 students had email addresses issued by the University (Legg & Blackman, 2019). Additionally, the Kaspersky report of 2022 showed that the number of victims of phishing attacks at the individual and corporate level in Africa has risen to 8.7% (Kaspersky, 2022).

4.5.2 Awareness of phishing attacks

The researcher conducted a survey about phishing awareness within the university, where students were participants. The survey showed the following percentages of students and periods of phishing awareness reminders: 8 % once a month, 4 % once a week, 4 % once a semester, 4 % once a year, 3 % once a term, and 3 % none”. While the academics received phishing awareness reminders in the following manner: 33.3% once a month, 26.7% once a term, 26.7% once a week, 6.7% once a week, and 6.7% none.” On the other hand, IT experts responded with the following statement: “Quarterly cyber security awareness modules that include a short video supplemented by a quiz to test knowledge gained as well as quarterly

phishing simulation exercises." On the other hand, studies demonstrated that phishing awareness consisted of periodic campaigns. The IT experts conducted these campaigns to raise phishing awareness by simulating phishing attacks among users (University of San Diego, 2017).

Additionally, Aldawood & Skiner (2019) argued that when the cybersecurity experts did not conduct phishing awareness campaigns and training timely, the end-users were at substantial risk of phishing attacks on the corporate computer network. Phishing attacks affected more inexperienced users on the computer network. Additionally, a phishing experiment within a student community showed that inexperienced users were more susceptible to phishing attacks than other users on the computer network. These users were first-year and international students (Broadhurst et al, 2018). Furthermore, Stefaniuk (2020) demonstrated that cybersecurity awareness increased the level of awareness among users. The cybersecurity experts conducted an awareness survey that showed 38 per cent of users complied with information security policy and rules before the cybersecurity training, and 70 per cent complied after the training (Stefaniuk, 2020).

4.5.3 Strategies of phishing attacks

The researcher sent a questionnaire to students to discover the phishing techniques. The students responded with the following answers: "Received via email, they posed as a legitimate announcement or email from the CTS desk or Newsflash. Asked for users and so on to change one's password and they would say something urgent like due to new security rollouts or protocols have changed or updated or something similar on those grounds. But once I saw some obvious hints of this being a phishing email, I flagged it and deleted it and thereafter warned my fellow students about this suspicious email." Likewise, the studies conducted in the past revealed that attackers embed a malicious link into the phishing email, which mimicked popular websites by creating copies of the original website from reputable organizations. These links are designed with the aim of collecting sensitive information such as usernames and passwords from victims (Wu et al., 2006).

Besides the malicious links sent by phishers, there are many phishing techniques to get confidential information. The phishing survey among students revealed these responses: "Received an email stating that my account was hacked and that I need to respond to them in order to get my account back. Also received an email stating sensitive information was leaked off of my phone. Both of which were fake." On the other hand, the academics responded with these techniques "Email was received from an address similar to the institution address but with a slight difference. The email came as across as official communication by the CTS

department, but it wasn't." Moreover, research demonstrated that hackers designed malicious mobile applications. These applications mimicked legitimate applications. Hackers use them to obtain confidential information from users. These applications affected most users who did not have the knowledge to authenticate applications using security indicators (Marforio et al., 2015).

On top of the mobile applications, attackers used other platforms such as website login pages, emails, and others to launch their phishing attacks. The researcher investigated these platforms by collecting responses from students, academics, and IT experts. The responses from the students were as follows: "Was about some aspect where they wanted my login and password to finalize admin processes", whereas the IT Experts said, "Display name spoofing, especially for business email compromise (BEC) attempts", and "It would be the targeting of the user's personal cell phones, via SMS and/or WhatsApp.". Furthermore, IT experts' responses showed that the phishers are using these platforms for phishing activities: SMSs, Email, social media, and telephone. Moreover, below are the students' percentages about the platforms where they received phishing attacks: 79 % of emails, 14 % SMSs, and 7 % social media that were used by phishers for attacks". On the other hand, studies by Ferreira & Teles (2019) demonstrated that attackers manipulate emails to infiltrate computer systems. Additionally, other studies showed that phishers designed websites that offered rewards to the user to obtain unauthorized access to victims' accounts (Maimon et al., 2021).

4.5.4 Summary

This chapter presented the results of data obtained from the questionnaire at the University of Technology in the Western Cape province. The objectives of this study were as follows: to identify the frequency of phishing attacks at a University of Technology, to determine the strategies used to deploy phishing attacks on a University of Technology network, to establish the awareness level of phishing attacks among end-users at a University of Technology and to investigate the nature of a phishing attack awareness program at a University of Technology. The results showed some challenges faced by the University of Technology: many users received phishing attacks and victims of phishing attacks, phishers used different strategies to deceive users through various platforms such as email, social media, etc., some users did not receive constant reminders about phishing attacks from IT technical team, and few users participated in training about phishing attacks through learning materials such as video recordings.

5 CHAPTER FIVE: CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

The previous chapter discussed the findings from participants, discussion, and interpretation of the study, and this chapter presents the revision of the research objectives, a summary of findings, and recommendations. Table 5.1 summarises the research findings. The table below provides a summary of the findings, explanation, and recommendation based on the research objective of the study. The section below provides details about the recommendations.

Table 5.1 Summary of Research Findings

Research Objectives (1,2,3,4)	Students		Academics		IT Experts		
	Summary of findings	Explanation	Summary of findings	Explanation	Summary of findings	Explanation	Recommendations
To identify the frequency of phishing attacks at a University of Technology	39% of phishing attacks 21% of victims of phishing attacks	Many phishing attacks Many victims of phishing attacks	64% of phishing attacks 33% of Victims of phishing attacks	Many phishing attacks Many victims of phishing attacks	50% phishing attacks More phishing attacks at the beginning and end of the year	Many phishing attacks	Phishing awareness program: To inform users about the number of phishing attacks
To determine the strategies used to deploy phishing attacks on a University of Technology network	Email mimicking message Emails with fake rewards Malicious links Targeted platforms: Emails, SMSs, social media	Phishing attacks deployed through various techniques Phishing attacks are used on various platforms	Emails mimicking message Malicious links for credentials	Phishing attacks deployed through various techniques	Spoofing BEC Targeted platforms: SMSs & WhatsApp	Phishing attacks deployed through techniques Phishing attacks are used on various platforms	Phishing awareness program: To Educate users about various malicious techniques used by phishers

Research Objectives (1,2,3,4)	Students		Academics		IT Experts		
	Summary of findings	Explanation	Summary of findings	Explanation	Summary of findings	Explanation	Recommendations
To establish the awareness level of phishing attacks among end-users at a University of Technology	Phishing reminders from none to one a year vary between 12% to 31%	Lack of consistency in the awareness of phishing attacks Low level of phishing awareness	Phishing reminders from none to one a year vary between 7% to 33%	Lack of consistency in the awareness of phishing attacks Low level of phishing awareness	Quarterly phishing reminders	Planned phishing awareness reminders	Phishing awareness program: Constant reminders to the user about phishing attacks
To investigate the nature of a phishing attack awareness program at a University of Technology	None	None	Educational videos on Phishing attacks	Educational content about phishing attacks	Educational videos on Phishing attacks Tests of phishing attack knowledge Phishing attack Simulation Educating risk of phishing attacks	Educational content about phishing attacks	Phishing awareness program which consists of educating users about phishing attacks and mitigation

5.2 Towards A Phishing Attack Awareness Framework

Figure 5.1 below provides a synthesized visualisation of the research findings outlined in Table 5.1. It maps the four cornerstone research objectives of the study to emergent outcomes derived from empirical data sources underpinning the research. It specifically provides a taxonomical overview offering theoretical body of knowledge significance associated with phishing in higher education contexts. Furthermore, this provisional framework offers decision-makers and policy-designers with practical and proactive implementation guidelines.

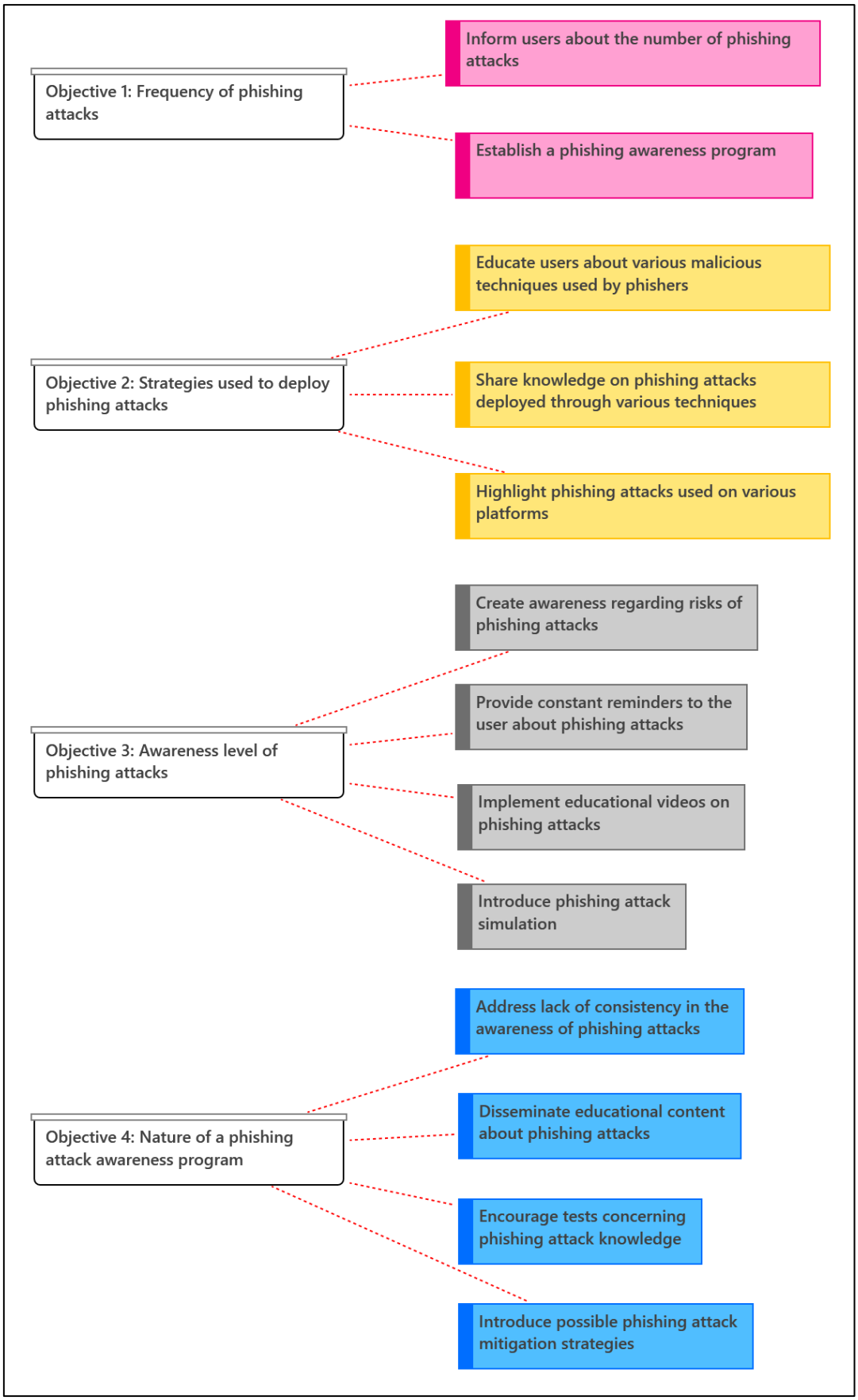


Figure 5.1 Proposed Phishing Attack Awareness Framework

5.3 Recommendations

In section 5.2, the researcher presented a Phishing Attack Awareness framework based on the TTAT framework for educating users about phishing attacks. The framework has two processes: threats and coping appraisals. The first process is to convince the users of the phishing attacks, and the second provides the users with mechanisms to combat phishing attacks. The researcher categorizes these processes into four elements: frequencies of phishing attacks, awareness of phishing attacks, and strategies of phishing attacks that the researcher drew from the findings.

The first and the second elements are the frequencies of phishing attacks and awareness of phishing attacks. These two are part of the threat appraisal process, while the third and fourth elements are strategies for phishing attacks and the nature of phishing awareness programs. The sections below discuss these elements further:

1. Frequencies of phishing attacks

The findings showed many phishing attacks and victims of phishing attacks among users at the University of Technology in the Western Cape. In the university's awareness program, the IT experts inform users about the number of phishing attacks and victims, and this section of the program forms the threat appraisal for motivating users to avoid phishing threats.

2. Strategies for phishing attacks

The findings of the university's investigation showed that phishers use different techniques in phishing attacks. In the university's phishing awareness program, IT experts provide users with information about the malicious techniques and platforms that phishers use in phishing attacks. This coping appraisal could help users with the tools to avoid phishing attacks.

3. Awareness of phishing attacks

The findings of a study on phishing attacks at the University demonstrated that IT users need constant reminders about the danger of phishing attacks. In the university awareness program, the IT experts send timely reminders of phishing attacks. The reminder process raised awareness of phishing attacks against the ever-evolving phishing attack among users.

4. Nature of phishing attack program:

The university's research findings showed the importance of educating users about phishing attacks. In the university's phishing awareness program, IT experts provide users with information to employ mitigation techniques against phishing attacks. This process enables the users to fight phishing attacks on the university's computer network.

5.4 Research Limitations

The research has reached its objective of developing recommendations for a phishing awareness framework. However, the study was limited by having students and academic participants from one department only due to time constraints. The section below presents the concluding remarks and suggestions for further research.

5.5 Concluding Remarks

The study is about developing a phishing attack awareness framework for users at the University of Technology in the Western Cape to educate users about phishing attacks, and the literature review and the results in the study demonstrated that phishers are targeting universities and other organisations. Moreover, the literature and results showed the importance of phishing awareness in defending against phishing attacks.

This study used a TTAT theoretical framework to guide the review of the relevant literature about phishing attacks and the choice of the research methodology. The TTAT allowed the researcher to achieve the study's objective. Furthermore, the researcher used the TTAT in this study to develop a framework. This framework supported the education of users about phishing attacks within the University of Technology.

The framework included four elements: the frequencies of phishing attacks, their strategies, and their nature.

5.6 Future Work

Due to the time constraint, this study focused on the Department of IT in the Faculty of Informatics and Design at one University in the Western Cape, and future work should include other departments and universities in the province.

REFERENCES

Akazue, M. I. *et al.* (2022) 'Empirical evidence of phishing menace among undergraduate smartphone users in selected universities in Nigeria', *Indonesian Journal of Electrical Engineering and Computer Science*, 28(3), pp. 1756–1765. doi: 10.11591/ijeecs.v28.i3.pp1756-1765.

Alan, B. 2016. *Social Research Methods*. Fifth ed. Oxford: Oxford University Press.

Aldawood, H. and Skinner, G. (2019) 'Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues', Future Internet, 11(3). doi: 10.3390/fi11030073.

Alkhalil, Z. *et al.* (2021) 'Phishing Attacks: A Recent Comprehensive Study and a New Anatomy', *Frontiers in Computer Science*, 3(March), pp. 1–23. doi: 10.3389/fcomp.2021.563060.

Al-Qahtani, A. F. and Cresci, S. (2022) 'The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19', IET Information Security, 16(5), pp. 324–345. doi: 10.1049/ise2.12073.

Andreasson, K. 2012. *Cybersecurity: Public sector threats and responses*. New York: Taylor & Francis group.

Anti-Phishing Working Group (2020) 'Phishing Activity Trends Report 3rd Quarter 2020', Apwg, (November), pp. 1–12.

Arachchilage, N. A. G. and Love, S. (2013) 'A game design framework for avoiding phishing attacks', *Computers in Human Behavior*. Elsevier Ltd, 29(3), pp. 706–714. doi: 10.1016/j.chb.2012.12.018.

Aronson, J. (1995) 'A pragmatic view of thematic analysis', The qualitative report, 2(1), pp. 1–3.

Bada, M., Solms, B. Von and Agrafiotis, I. (2019) 'Reviewing national cybersecurity awareness for users and executives in Africa', *arXiv*, 12(1), pp. 108–118.

Benenson, Z. B., Gassmann, F. and Landwirth, R. (2017) 'Unpacking Spear Phishing Susceptibility', 1, pp. 610–627. doi: 10.1007/978-3-319-70278-0.

Bernard, H., 2013. *Social Research Methods: Qualitative and Quantitative Approach*. Second ed. Los Angeles: Sage Publications.

Bidgoli, H. 2021. MIS: Management Information Systems. 10th edition. Boston, MA: Cengage Learning, Inc.

Bidgoli, H. 2012. Management Information Systems. Third Edition. Mason, Cengage Learning, Inc.

Bosworth, S, Michel, K & Whyne, E. 2014. *Computer security handbook*. Sixth edition. New Jersey: Wiley.

Broadhurst, R., Skinner, K., Sifniotis, N., Matamoros-Macias, B., & Ipsen, Y. (2018) 'Cybercrime Risks in a University Student Community', SSRN Electronic Journal, (March 2019). doi: 10.2139/ssrn.3176319.

Butgereit, L. (2018) 'CyberSecurity Education and Training in a Corporate Environment in South Africa Using Gamified Treasure Hunts', Springer International Publishing AG, 558(October 2017), pp. 113–117. doi: 10.1007/978-3-319-54978-1.

Byström, K., Ruthven, I. and Heinström, J. (2017) 'Proceedings of the Ninth International Conference on Conceptions of Library and Information Science , Uppsala , Sweden , June 27-29 ', *Information Research*, 22(1), pp. 1–9. Available at: http://informationr.net/ir/22-1/colis/colis1651.html.

Calder, A. and Watkins, S. (2012) IT Governance. fifth. london: Kogan Page.

Canham, M., Posey, C. and Constantino, M. (2022) 'Phish Derby: Shoring the Human Shield Through Gamified Phishing Attacks', Frontiers in Education, 6(January), pp. 1–10. doi: 10.3389/feduc.2021.807277.

Catota, F. E., Granger Morgan, M. and Sicker, D. C. (2019) 'Cybersecurity education in a developing nation: The Ecuadorian environment', Journal of Cybersecurity, 5(1), pp. 1–19. doi: 10.1093/cybsec/tyz001.

Chigada, J. and Madzinga, R. (2020) 'Cyberattacks and threats during COVID-19 : A systematic literature review Coronavirus Disease-2019', South African Journal of Information Management, pp. 1–11.

Cleary, M., Hayter, M. and Horsfall, J. (2012) ‘Data collection and sampling in qualitative research: does size matter?’, Journal of Advanced Nursing, pp. 473–475.

Costello, E., Corcoran, M., Barnett, J., Birkmeier, M. & Cohn, R. (2014) ‘Information and communication technology to facilitate learning for students in the health professions: Current uses, gaps, and future directions’, Journal of Asynchronous Learning Network, 18(4). doi: 10.24059/olj.v18i4.512.

Daengsi, T., Pornpongtechavanich, P. and Wuttidittachotti, P. (2022) ‘Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks’, *Education and Information Technologies*. Springer US, 27(4), pp. 4729–4752. doi: 10.1007/s10639-021-10806-7.

Diaz, A., Sherman, A. T. and Joshi, A. (2018) ‘Phishing in an academic community: A study of user susceptibility and behavior’, arXiv. doi: 10.1080/01611194.2019.1623343.

Drury, V. and Meyer, U. (2019) ‘Certified phishing: Taking a look at public key certificates of phishing websites’, Proceedings of the 15th Symposium on Usable Privacy and Security, SOUPS 2019, pp. 211–223.

Du Plooy-Cilliers, F., Davis, C. and Bezuidenhout, R. 2014. Research Matters. Paarl Media Paarl, South Africa.

Erl, T., Mahmood, Z. & Puttini, R. 2013. Cloud Computing: Concepts, Technology, Security, and Architecture. First edition. New Jersey: Pearson.

Gardner, B & Thomas, V. 2014. *Building an information security awareness program: defending against social engineering and technical threats*. First edition. Waltham: Elsevier.

Greener, S., 2008. *Business research methods.* London: Ventus publishing.

Gutierrez, C. N., Kim, T., Corte, R. D., Avery, J., Goldwasser, D., Cinque, M. & Bagchi, S. (2018). ‘Learning from the ones that got away: Detecting new forms of phishing attacks’, IEEE Transactions on Dependable and Secure Computing. IEEE, 15(6), pp. 988–1001. doi: 10.1109/TDSC.2018.2864993.

Hadnagy, C & Fincher, M. 2015. *Phishing dark waters: the offensive and defensive sides of malicious emails*. First Edition. Somerset: Wiley.

Hadlington, L., Popovac, M., Janicke, H., Yevseyeva, I. & Jones, K. (2019) 'Exploring the role of work identity and work locus of control in information security awareness', Computers and Security. Elsevier Ltd, 81, pp. 41–48. doi: 10.1016/j.cose.2018.10.006.

Hasudunganlubis, A., Idrus, S. Z. S. and Sarji, A. (2018) 'ICT usage amongst lecturers and its impact towards learning process quality', Jurnal Komunikasi: Malaysian Journal of Communication, 34(1), pp. 284–299. doi: 10.17576/JKMJC-2018-3401-17.

Innab, N., Al-Rashoud, H., Al-Mahawes, R. & Al-Shehri, W. (2018) 'Evaluation of the Effective Anti-Phishing Awareness and Training in Governmental and Private Organizations in Riyadh', 21st Saudi Computer Society National Computer Conference, NCC 2018, (February). doi: 10.1109/NCG.2018.8593144.

Jakobsson, M & Myers, S. 2006. *Phishing and countermeasures: Understanding the Increasing Problem of Electronic Identity theft*. Bloomington: John Wiley & Sons.

D'Arcy, J., Hovav, A. and Galletta, D. (2009) 'User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach', Information Systems Research, 20(1), pp. 79–98. doi: 10.1287/isre.1070.0160.

Kaspersky. 2022. *8.7% of users encountered phishing attacks in Africa in 2022, global number of attacks exceeds 500 million.* Retrieved from https://kaspersky.africa-newsroom.com/press/87-of-users-encountered-phishing-attacks-in-africa-in-2022-global-number-of-attacks-exceeds-500-million?lang=en .[23 March 2023].

Kothari, C., 2004. *Research methodology: methods and techniques.* 2 ed. New Delhi: New age international limited.

Kritzinger, E., Da Veiga, A. and van Staden, W. (2023) 'Measuring organizational information security awareness in South Africa', Information Security Journal, 32(2), pp. 120–133. doi: 10.1080/19393555.2022.2077265.

Krombholz, K., Hobel, H., Huber, M. & Weippl, E. (2015) 'Advanced social engineering attacks', Journal of Information Security and Applications, 22(October 2017), pp. 113–122. doi: 10.1016/j.jisa.2014.09.005.

Kumar, R., 2011. *Research methodology: a step-by-step guide for beginners.* 3rd ed. Los angeles: Sage Publications.

Kuraku, S. *et al.* (2023) 'Exploring How User Behavior Shapes Cybersecurity Awareness in the Face of Phishing Attacks', *International Journal of Computer Trends and Technology*, 71(11), pp. 74–79. Available at: https://doi.org/10.14445/22312803/IJCTT-V71I11P111.

Liang, H & Xue, Y. 2009. *Avoidance of Information Technology Threats: a theoretical perspective*. MIS Quarterly, 33(1): 71-90.

Legg, P. and Blackman, T. (2019) 'Tools and techniques for improving cyber situational awareness of targeted phishing attacks', 2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2019. IEEE, pp. 1–4. doi: 10.1109/CyberSA.2019.8899406.

Maimon, D., Howell, C.J, Perkins, R.C, Muniz, C.N & Berenblum, T. 2021. 'A Routine Activities Approach to Evidence-Based Risk Assessment: Findings From Two Simulated Phishing Attacks', Social Science Computer Review, pp. 1–19. doi: 10.1177/08944393211046339.

Marczyk, G., DeMatteo, D. & Festinger, D. 2005. *Essentials of research design and methodology.* New Jersey: John Wiley & Sons.

Marforio, C, Masti, C, Soriente, C, Kostiainen, K & Capkun, S. (2015) 'Personalized Security Indicators to Detect Application Phishing Attacks in Mobile Platforms'. Available at: http://arxiv.org/abs/1502.06824.

Mimecast. 2019. *The State of Email Security Report 2019* – South Africa. Retrieved from https://info.mimecast.com/sa-the-state-of-email-security.html?utm_medium=SEMPPC&utm_source=GooglePPC&utm_campaign=7011N000001UvqJQAS&utm_term=mimecast%20phishing&gclid=Cj0KCQiAtf_tBRDtARIsAIbAKe0IAe2v2XBX-nAJ9XsDIYBzGU2Ja-reytuPph3X_l54VsdY07TSkUgaAuf6EALw_wcB [28 September 2020]

Mouton, F., Teixeira, M. and Meyer, T. (2017) 'Benchmarking a mobile implementation of the social engineering prevention training tool', 2017 Information Security for South Africa - Proceedings of the 2017 ISSA Conference, 2018-Janua(February), pp. 106–116. doi: 10.1109/ISSA.2017.8251782.

Mouton, J., 2001. *How to succeed in your Master's and Doctoral Studies: A South African guide and resource book.* Pretoria, Van Schaik.

Navas, R.E., Cuppensb, F., Cuppens, N.B., Toutain, L. & Papadopoulos, G.Z. 2021. 'Physical resilience to insider attacks in IoT networks: Independent cryptographically secure sequences for DSSS anti-jamming', Computer Networks, 187. doi: 10.1016/j.comnet.2020.107751.

Neuman, L., 2014. *Social research methods: qualitative and quantitative approaches.* 7 ed. Harlow: Pearson Education.

Neville, C. 2005. *Introduction to research and research methods.* Bradford: Effective learning service.

Nicholas, C., French, S. & Valentine, G. 2010. *Key methods in geography.* 2 ed. London: Sage Publications.

Nyasvisvo, B. and Chigada, J. M. (2023) 'Phishing Attacks : A Security Challenge for University Students Studying Remotely', *The African Journal of Information Systems*, 15(2), pp. 1–27. Available at: https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=2250&context=ajis.

Okokpujie, K. *et al.* (2023) 'Cybersecurity Awareness: Investigating Students' Susceptibility to Phishing Attacks for Sustainable Safe Email Usage in Academic Environment (A Case Study of a Nigerian Leading University)', *International Journal of Sustainable Development and Planning*, 18(1), pp. 255–263. doi: 10.18280/ijsdp.180127.

Ooko, O. S. & Shadrack, M. .2019. 'Securing Wireless Networks in African Universities: A Case Study of Universities in Kenya', Researchgate.Net, (December). Available at: https://www.researchgate.net/profile/Samson-Ooko/publication/337707066_Securing_Wireless_Networks_in_African_Universities_A_Case_Study_of_Universities_in_Kenya/links/5de6396092851c83645d5e84/Securing- Wireless-Networks-in-African-Universities-A-Case-Study-.

Proofpoint. 2019. *State of the phish: 2019 Report*. Available at https://www.proofpoint.com/us/products/security-awareness-training/phishing-simulations accessed on 04/05/2020.

Rajkumar, K. and Njenga, K. (2022) 'Make personal information security great again: A case of users' perspectives on personal identifiable information in South Africa', SA Journal of Information Management, 24(1), pp. 1–9. doi: 10.4102/sajim.v24i1.1526.

Rakhra, M & Kaur, D. 2018. *Studying user's computer security behavior in developing an effective anti-phishing educational framework*. The Proceedings of the Second International Conference on Inventive Systems and Control.

Ritchie, J. & Lewis, J. 2003. *Qualitative research practice: a guide for social science students and researchers.* London: Sage Publications. The proceedings of the second international conference on inventive systems and control.

Shimonski, R. 2014. *Cyber Reconnaissance Surveillance and Defence*. Rockland: Elsevier Science & Technology.

Sinan, I. I. et al. (2024) 'Data architectures and the prevalent cyberattacks encountered by West African higher educational institutions in the COVID-19 era', Journal of Infrastructure, Policy and Development, 8(8), pp. 1–17. doi: 10.24294/jipd.v8i8.3736.

Stefaniuk, T. (2020) 'Training in shaping employee information security awareness', Entrepreneurship and Sustainability Issues, 7(3), pp. 1832–1846. doi: 10.9770/jesi.2020.7.3(26).

Thomas, K, Li, F, Zand, A, Barrett, J, Invernizzi, L, Markov, Y, Comanescu, O, Eranti, V, Moscicki, A, Margolis, D, Paxson, V & Bursztein, E. (2017) 'Data Breaches, phishing, or malware? understanding the risks of stolen credentials', Proceedings of the ACM Conference on Computer and Communications Security, pp. 1421–1434. doi: 10.1145/3133956.3134067.

Vafaei-Zadeh, A., Thurasamy, R. and Hanifah, H. (2019) 'Modeling anti-malware use intention of university students in a developing country using the theory of planned behavior', Kybernetes, 48(8), pp. 1565–1585. doi: 10.1108/K-05-2018-0226.

Venter, I.M., Blignaut, R.J., Renaud, K. & Venter, M.A. 2019. *Cybersecurity education is as essential as the three R's*. Heliyon, 5(12): 1-8.

Wang, J & Kissel, K. 2015. *Introduction to Network Security: Theory and Practice*. 2nd edition. Massachusetts: John Wiley & Sons.

Wannenburg, M. C. et al. (2023) 'South Africans' susceptibility to phishing attacks', Southern African Journal of Accountability and Auditing Research, 25(1), pp. 53–72. doi: 10.54483/sajaar.2023.25.1.4.

West, J., Andrews, J. & Dean, T. 2019. *Network+ Guide to Networks.* Eighth ed. Boston: Cengage Learning.

White, C. 2015. *Data Communication and Computer Networks*. Eighth edition. Mason: Cengage Learning.

Wilson, M & Hash, J. 2003. Computer Security: Building an Information Technology Security Awareness and Training Program. NIST, 1-70.

Wu, M., Miller, R. C. and Garfinkel, S. L. (2006) 'Do security toolbars actually prevent phishing attacks?', Conference on Human Factors in Computing Systems - Proceedings, 1, pp. 601–610. doi: 10.1145/1124772.1124863.

Yoro, R. E., Aghware, F. O., Amaze, M. I., Ibor, A. E. & Ojugo, A. A. (2023) 'Evidence of personality traits on phishing attack menace among selected university undergraduates in Nigerian', *International Journal of Electrical and Computer Engineering*, 13(2), pp. 1943–1953. doi: 10.11591/ijece.v13i2.pp1943-1953.

APPENDICES

APPENDIX A: Ethical Clearance – CPUT

Cape Peninsula University of Technology
creating futures

PO Box 1906, Bellville,7535 Symphony Way, Bellville, Cape Town, South Africa
+ 27 (0)21 959 6767 www.facebook.com/cput.ac.za info@cput.ac.za www.cput.ac.za

Office of the Research Ethics Committee
Faculty of Informatics and Design
Room 2.09
80 Roeland Street
Cape Town
Tel: 021-469 1012
Email: ndedem@cput.ac.za
Secretary: Mziyanda Ndede

12 August 2021

Mutomb Japhet Kayomb
c/o Department of Information Technology
CPUT

Reference no: 217074812/2021/14

Project title: Phishing Attack Awareness Amongst Users in the University of Technology in the Western Cape

Approval period: 12 August 2021 – 31 December 2022

This is to certify that the Faculty of Informatics and Design Research Ethics Committee of the Cape Peninsula University of Technology approved the methodology and ethics of Mutomb Japhet Kayomb (217074812) for the MTech Information and Communication Technology

Any amendments, extension or other modifications to the protocol must be submitted to the Research Ethics Committee for approval.

The Committee must be informed of any serious adverse event and/or termination of the study.

A/Prof I van Zyl
Chair: Research Ethics Committee
Faculty of Informatics and Design
Cape Peninsula University of Technology

APPENDIX B: Research questions, Questionnaire items, Emergent Codes and Themes – Students and Academics

The researcher used thematic analysis as a data analysis method. This method consisted of recording the raw data from the participants. The researcher organised the data according to the research questions and developed codes based on the main elements emanating from the data. The researcher created themes based on the patterns from the codes.

	Questionnaire items	Codes	Themes
Part A: Demographics information	Q.1.1 What qualification are currently registered at the university for ?	Stream of study	
	Q.1.2 For how many years have you studied at this university?	Year of study	
RQ1.What is the frequency of phishing attacks at a University of Technology?	If we accept that phishing occurs when an attacker, posing as a trusted person, tricks a victim into opening an email, instant message, or text message. Now with this in mind:		
	Q.2.1 Have you ever received a phishing attack while working at this organisation? Yes or No: ○ Yes ○ No	Phishing attacks	Frequencies of phishing attack
RQ 2. What are the strategies used to deploy phishing attacks at on a University of Technology network?	Q.2.2 If the answer is yes, please elaborate on how you received a phishing attack.	Mimicking Urgent request Malicious link Rewards Credentials	Strategies of phishing attacks
	Q.2.3 Do you know of any user who has been a victim of a phishing attack on the university's computer network?	Victim	Frequencies of phishing attack

<table>
<tr><th></th><th>Questionnaire items</th><th>Codes</th><th>Themes</th></tr>
<tr><td></td><td>Q.2.4 If the answer is yes, please elaborate on how the user became a victim of a phishing attack</td><td>Clicking links
Request
Logins details
Invitation
Ransom
Personal information</td><td>Strategies of phishing attacks</td></tr>
<tr><td rowspan="4">RQ 2. What are the strategies used to deploy phishing attacks at on a University of Technology network?</td><td>Q.3.1 If you HAVE been a victim of a phishing attack while working at this organisation, please select the platforms through which you received phishing attacks:
☐ Emails
☐ SMSs
☐ Social media</td><td>SMSs, Emails, Telephone & social media</td><td>Strategies of Phishing attacks</td></tr>
<tr><td>Q.3.2 If NOT on any of the above platforms, please elaborate.</td><td>Links</td><td></td></tr>
<tr><td>Q.3.3 If you have NOT been a victim of a phishing attack while working at this organisation, please select and rate the platforms through which you believe you are most likely to receive phishing attacks. Use the following scale:
5-very likely, 4-likely, 3-neutral, 2-unlikely,1-very unlikely
<table>
<tr><th></th><th>5</th><th>4</th><th>3</th><th>2</th><th>1</th></tr>
<tr><td>SMSs</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Emails</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Telephone</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Social media</td><td></td><td></td><td></td><td></td><td></td></tr>
</table>
</td><td>SMSs
Emails
Telephone
Social media</td><td></td></tr>
<tr><td>Q.3.4 If NOT on any of the above platforms, please elaborate.</td><td></td><td></td></tr>
</table>

	Questionnaire items	Codes	Themes
	Q.3.5 In a case where you HAVE received a phishing email, please select one or more of the following strategies that might have been used in that email: ☐ Phishing email with a link replicating a legitimate website of an organization ☐ A phishing email that replicates legitimate business logs ☐ Phishing through advertisement ☐ Impersonating a person of authority ☐ Phishing attack that the hacker personalized to you ☐ Phishing email with a reward offered	Links Business logo Advertisement Impersonating Personalized Reward	Strategies of Phishing attacks
	Q.3.6 If NOT on any of the above strategies, please elaborate.		

RQ 2. What are the strategies used to deploy phishing attacks at on a University of Technology network?	Q.3.7 If you have NOT received a phishing email, please indicate which strategy is likely to be used from one or more of the strategies below: ☐ Phishing email with a link replicating a legitimate website of an organization ☐ A phishing email that replicates legitimate business logs ☐ Phishing through advertisement ☐ Impersonating a person of authority ☐ Phishing attack that the hacker personalized to you ☐ Phishing email with a reward offered	Links Business logs Advertisement Impersonating Impersonating Reward	
	Q.3.8 If NOT on any of the above strategies, please elaborate…		
	Q.3.9 What do you believe would be the impact if you were to respond to a phishing email?	Confidential information Financial loss Access to resources Malfunctioning Unauthorized access Personal information Malware	Awareness of phishing attacks

	Q.3.10 Which mitigation techniques would you use to protect yourself against phishing attacks from the list below? (You may choose more than one option) ☐ The use of technologies such as email filtering tools, anti-malware software, firewall, etc. ☐ I will never click on a website link without knowing its source ☐ I am not sure what technique to make use of	Website link Filtering Anti-malware Firewall	Strategies of Phishing attacks
	Q.3.11 If NOT on any of the above mitigation techniques, please elaborate…		
RQ.3. What is the awareness level of phishing attacks among end-users at a University of Technology?	Q.4.1 How often do you receive phishing awareness reminders from the university? ☐ Once a week ☐ Once a month ☐ Once a term ☐ Once a semester ☐ Once a year ☐ None	Week Month Term Semester Year	Awareness of phishing attacks
	Q.4.2 Do you believe that a phishing awareness programme reduces the chances of becoming victims of phishing attacks? Yes or No	Victim Awareness	
	Q.4.3 Please elaborate on your answer above	Awareness Education Cyber tools Test	Awareness of phishing attacks
	Q.4.4 How do you rate your phishing attack awareness using the scale below? 5. Excellent 4. Good 3. Average 2. Fair 1. Poor	Awareness	
RQ.4.What is the nature of a phishing attack awareness program at a	Q.5.1 Are you aware of any phishing attack awareness programme for users at the University?	Awareness	Awareness of phishing attacks
	Q.5.2 If your answer is yes, could you provide some details about your understanding of the phishing attack awareness programme?		

APPENDIX C: Survey Questionnaire – Students and Academics

Phishing Attack Awareness Questionnaire

Dear participant,

I am conducting a research project which aims to develop a phishing attack awareness framework, which could help reduce the number of attacks on a University of Technology's computer network. Furthermore, it investigates the nature of a phishing attack awareness program at a university of Technology.
I kindly request your participation in a survey which will take 5-10 minutes. To ensure confidentiality of information, no attempt will be made to identify you with the responses you make. Please note that you are free to respond with no fear of victimization. Recommendations will be used only to inform the design and development of the phishing attack awareness framework for the University of Technology. There will be no reference to the identity of sources.
Your participation in this research project is voluntary and you may withdraw from the survey at any stage.
Yours Sincerely
Mr. Japhet Mutomb
mutombk@cput.ac.za
Supervisor contact details:
Dr. Errol Francke
franckee@cput.ac.za

* Indicates required question

Section A

1. Q.1 What qualification are you currently registered at the university for ? *

2. Q.2 For how many years have you studied at this university ? *

Section B

3. If we accept that phishing occurs when an attacker, posing as a trusted person, tricks a victim into opening an email, instant message, or text message… Now with this in mind… Q.1.1 Have you ever received a phishing attack while studying at this university?

   Mark only one oval.

   - ◯ Yes
   - ◯ No

4. Q1.2 If the answer is yes, please elaborate on how you received a phishing attack.

5. Q.1.3 Do you know of any user who has been a victim of a phishing attack on the university's computer network?

   Mark only one oval.

   - ◯ Yes
   - ◯ No

6. Q.1.4 If the answer is yes, please elaborate on how the user became a victim of a phishing attack

7. Q.2.1 If you HAVE been a victim of a phishing attack while studying at this university, please select the platforms through which you received phishing attacks

Tick all that apply.

- [ ] SMSs
- [ ] Emails
- [ ] Telephone
- [ ] Social media

8. Q.2.2 If NOT on any of the above platforms, please elaborate…

9. Q.2.3 If you have NOT been a victim of a phishing attack while studying at this university, please select and rate the platforms through which you believe you are most likely to receive phishing attacks. Use the following scale: 5-very likely 4-likely 3-neutral 2-unlikely 1-very unlikely

Tick all that apply.

	5	4	3	2	1
SMSs	☐	☐	☐	☐	☐
Emails	☐	☐	☐	☐	☐
Telephone	☐	☐	☐	☐	☐
Social media	☐	☐	☐	☐	☐

10. Q.2.4 If NOT on any of the above platforms, please elaborate…

11. Q.2.5 In a case where you HAVE received a phishing email, please select one or more of the following strategies that might have been used in that email:

Tick all that apply.

- ☐ Phishing email with a link replicating a legitimate website of an organization
- ☐ A phishing email that replicates legitimate business logos
- ☐ Phishing through advertisement
- ☐ Impersonating a person of authority
- ☐ Phishing attack that the hacker personalized to you
- ☐ Phishing email with a reward offered

12. Q.2.6 If NOT on any of the above strategies, please elaborate…

13. Q.2.7 If you have NOT received a phishing email, please indicate which strategy is likely to be used from one or more of the strategies below:

Tick all that apply.

- [ ] Phishing email with a link replicating a legitimate website of an organization
- [ ] A phishing email that replicates legitimate business logs
- [ ] Phishing through advertisement
- [ ] Impersonating a person of authority
- [ ] Phishing attack that the hacker personalized to you
- [ ] Phishing email with a reward offered

14. Q.2.8 If NOT on any of the above strategies, please elaborate…

15. Q.2.9 What do you believe would be the impact if you were to respond to a phishing email?

16. Q.2.10 Which mitigation techniques would you use to protect yourself against phishing attacks from the list below? (You may choose more than one option)

Tick all that apply.

- [ ] The use of technologies such as email filtering tools, anti-malware software, firewall, etc.
- [ ] I will never click on a website link without knowing its source
- [ ] I am not sure what technique to make use of

17. Q.2.11 If NOT on any of the above mitigation techniques, please elaborate…

18. Q.3.1 How often do you receive phishing awareness reminders from the university?

Mark only one oval.

- Once a week
- Once a month
- Once a term
- Once a semester
- Once a year
- None

19. Q.3.2 Do you believe that a phishing awareness programme reduces the chances of becoming victims of phishing attacks?

Mark only one oval.

- Yes
- No

20. Q.3.3 Please elaborate on your answer above

21. Q.3.4 How do you rate your phishing attack awareness using the scale below?

5. Excellent 4. Good 3. Average 2. Fair 1. Poor

Mark only one oval per row.

	5	4	3	2	1
Scale	◯	◯	◯	◯	◯

22. Q.4.1 Are you aware of any phishing attack awareness programme for users at the University?

Mark only one oval.

◯ Yes
◯ No

23. Q.4.2 If your answer is yes, could you provide some details about your understanding of the phishing attack awareness programme?

This is the end of the survey. Thank you for participating in it. Your participation is greatly appreciated.

APPENDIX D: Survey Questionnaire – IT Experts

Phishing Attack Awareness Questionnaire

Dear participant,

I am conducting a research project which aims to develop a phishing attack awareness framework, which could help reduce the number of attacks on a University of Technology's computer network. Furthermore, it investigates the nature of a phishing attack awareness program at a university of Technology.
I kindly request your participation in a survey which will take 5-10 minutes. To ensure confidentiality of information, no attempt will be made to identify you with the responses you make. Please note that you are free to respond with no fear of victimization. Recommendations will be used only to inform the design and development of the phishing attack awareness framework for the University of Technology. There will be no reference to the identity of sources.
Your participation in this research project is voluntary and you may withdraw from the survey at any stage.
Yours Sincerely
Mr. Japhet Mutomb
mutombk@cput.ac.za
Supervisor contact details:
Dr. Errol Francke
franckee@cput.ac.za

* Indicates required question

Section A

This expert interview follows a survey conducted within the Department of Information Technology among academics about phishing attacks.

1. Q.1.1 What is your job title or position in the organisation? *

2. Q.1.2 How many years have you been working in this position in the organisation? *

3. 2.1 The survey revealed users received phishing attacks on the following platforms: emails, SMSs, social media and telephone. The phishing attackers target users according to this rank: 70% of attacks through emails, 60% on SMSs, 30% through social media and 10% on phone calls.
   Now with that in mind

   2.1.1. In your opinion, what are the cybersecurity techniques available to users to minimize these attacks received through emails?

4. 2.1.2 What are the security mechanisms for users to minimize phishing attacks received via SMSs?

5. 2.1.3. What are the security measures to reduce these attacks through social media?

6. 2.1.4 What is the trend in the measures used to defend against phishing attacks?

Section B

7. 2.2 The survey also showed that 80% of phishing attacks were impersonating people of authority within the computer network. What security measures can the users take to minimize these attacks?

8. 2.3. With question 2.2 in mind, is it true that there is a high number of phishing attacks that impersonate people of authority? If yes, can you elaborate?

9. 2.4 The investigation showed that users received attacks with embedded links that mimic legitimate websites. What is the mitigation technique in place to prevent such a phishing attack?

10. 2.5 With question 2.4 in mind, what are, on average, the percentages of phishing attacks with links that mimic the legitimate website?

11. 2.6 What is the trend concerning the strategies used by phishing attackers to deploy phishing attacks?

Section C

12. 3.1 The survey also revealed users received phishing awareness reminders at different times, some users once a week, once a month and once a semester. Based on the above statement, how often are phishing awareness reminders sent?

13. 3.2 Based on question 3.1, what is the effectiveness of reminders in minimizing phishing attacks?

14. 3.3 The survey also revealed that the phishing awareness programme is the combination of awareness of mitigation techniques and types of phishing attacks, education, and reminders. What is the phishing awareness programme made of within the organization?

15. 3.4 What do you believe are the key elements that should not be omitted from any phishing awareness programme?

This is the end of the survey. Thank you for participating in it. Your participation is greatly appreciated.

APPENDIX E: Editing Certificate

DR PATRICIA HARPUR

B.Sc Information Systems Software Engineering, B.Sc Information Systems (Hons)
M.Sc Information Systems, D.Technology Information Technology

Editing Certificate

---

19 Keerweder Street
Vredelust
Bellville
7945

083 730 8540
doc@getthatresearchdone.com

To Whom It May Concern

This document certifies I have copy-edited the following thesis by Mutomb Japhet Kayomb:

A PHISHING ATTACK AWARENESS FRAMEWORK FOR USERS IN A UNIVERSITY OF TECHNOLOGY IN THE WESTERN CAPE

Please note this does not cover any content, conceptual organisation, or textual changes made after the editing process.

Best regards

Dr Patricia Harpur

5 January 2024
