




A phishing attack awareness framework for a South African University of Technology

**Authors:**Japhet M. Kayomb¹ Errol R. Francke¹ Tabisa Ncubukezi¹ **Affiliations:**

¹Department of Information Technology, Faculty of Informatics and Design, Cape Peninsula University of Technology, Cape Town, South Africa

Corresponding author:

Errol Roland Francke,
franckee@cput.ac.za

Dates:

Received: 07 Oct. 2024

Accepted: 26 Feb. 2025

Published: 15 July 2025

How to cite this article:

Kayomb, J.M., Francke, E.R. & Ncubukezi, T., 2025, 'A phishing attack awareness framework for a South African University of Technology', *South African Journal of Information Management* 27(1), a1949. <https://doi.org/10.4102/sajim.v27i1.1949>

Copyright:

© 2025. The Authors.
Licensee: AOSIS. This work is licensed under the Creative Commons Attribution License.

Background: Phishing is a deceptive tactic in which an attacker impersonates a trusted entity to steal sensitive information from Internet users. This creates significant risks for university end-users who depend on computer networks, underscoring the critical need for enhanced phishing awareness.

Objectives: This study aims to develop a phishing awareness framework among the University of Technology users and, in so doing, help reduce the number of phishing attacks.

Method: A qualitative method based on a case study was adopted. Data were collected from students, academics and technical staff in the information technology (IT) department with ethical considerations in mind. Data were analysed using thematic analysis with the Technology Threats Avoidance Theory as the theoretical lens for the study.

Results: The findings showed many phishing attacks and victims at the university. Furthermore, phishers use different techniques in phishing attacks, and IT users need constant reminders about the danger of phishing attacks. Lastly, it is important to educate users about phishing attacks.

Conclusion: The study recommended a framework for educating users about phishing attacks within the university. The framework included four elements: the frequencies of phishing attacks, strategies of phishing attacks, awareness of phishing attacks, and the nature of a phishing attack programme.

Contribution: This study has the potential to help protect university data and could reduce 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.

Keywords: cyber-attacks; cyberspace; network security; phishing attack; security awareness.

Introduction

Social value

According to Li, Chen and Wang (2024:1), phishing attacks are one of the most widespread and harmful cyber threats affecting individuals and organisations today. A phishing attack is a practice in which the attacker lures an online user into revealing personal information about themselves. Phishers obtain authentication information through deceptive techniques such as email spoofing, fake login pages, malware-infected links and social engineering tactics that trick users into revealing their credentials. The attacker obtains this information by posing as a trusted individual or organisation (Hussan & Mangi 2025:417).

Phishers often employ tactics to deceive victims into clicking on URLs (uniform resource locators) that direct them to malicious websites, resulting in the daily loss of credentials and digital assets for numerous individuals (Ejaz, Mian & Manzoor 2023:1). To avoid becoming victims, Internet users should, therefore, be aware of the various techniques employed in phishing attacks. While many organisations, including university networks around the globe, are suffering from phishing attacks, some of these cyber-attacks cause indirect financial loss. Mimecast published a report that showed that 67% of organisations had experienced phishing attacks and 73% of victims had experienced a direct financial loss (Mimecast 2019). Mimecast then reports in 'The State of Email & Collaboration Security Report 2024' that the World Economic Forum currently ranks cybercrime as the eighth most significant global risk. In today's interconnected digital economy, all companies, regardless of size, are increasingly vulnerable to cyber threats. The potential for data breaches or system incursions poses a substantial risk to the operations, reputation and revenue of businesses

Read online:

Scan this QR code with your smart phone or mobile device to read online.

worldwide — a fact that has gained widespread recognition. Cybercrime is projected to grow by 15% annually over the next 2 years, escalating from \$8.0 trillion globally in 2023 to \$10.5 trillion by 2025, up from \$3.0 trillion in 2015 – marking the largest wealth transfer in human history. In 2023, business email compromise (BEC), a specifically destructive form of phishing, nearly doubled in incidence. Phishing, along with stolen credentials and the exploitation of network vulnerabilities, continues to be the primary methods through which companies are compromised (Mimecast 2024b).

Educational institutions are void of effective anti-phishing programmes. Benenson, Gassmann and Landwirth (2017) conducted a study that indicates that a phishing attack experiment was conducted in a university with 1200 students. Emails and Facebook messages were sent to the students, and only 10% of them acted according to the university's anti-phishing policy. The lack of anti-phishing awareness programmes can increase the impact of phishing attacks among end-users on the university's network. This is because of the fact that the users on the university's network are not informed about the threats and the techniques associated with phishing attacks and do not fully understand the impact of cyber-attacks.

The techniques used in these reported attacks mainly impersonated emails from trusted business partners and vendors. Email is an essential communication tool that transmits information assets between different parties. According to Mimecast (2019) the breach of information stored on email systems can harm businesses. In a follow-up report, Mimecast (2024a) indicates that it is essential to understand how data breaches occur, identify their most common causes and implement strategies that enable an organisation to take proactive and responsive measures for their mitigation and elimination. Educational institutions are not spared, as they rely heavily on emails for communication.

Scientific value

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 organisation'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 et al. 2019).

Thomas et al. (2017) demonstrate that hackers stole millions of usernames and passwords from various online services between 2016 and 2017. Specops (2025) extend the view of Thomas et al. (2017) by stating that researchers have

confirmed that malware has compromised over 1 billion passwords, prompting a new security alert. The report analysed a total of 1 089 342 532 stolen passwords collected over 12 months. The cybercriminals sold those online credentials on the black market for a large amount of money, and according to Winder (2025), certain stolen passwords from cybersecurity vendors are available for purchase on the dark web at a price of \$10 each. These criminals are also able to log onto some of the victim's 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 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. The attackers create malicious mobile applications such as malicious websites that give unauthorised access to personal information such as passwords, credit card numbers, among others. Human errors such as failure to check the authenticity of the mobile application before installation on the mobile phone play a role in data breaches. 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 et al. 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 countries, such as South Africa (SA), do not possess adequate awareness campaigns, which explains why there is a high number of victims (Bada, Solms & Agrafiotis 2019). Furthermore, more studies show that SA is lagging in terms of cybersecurity awareness and education among Internet users. Many Internet users within the universities lack a basic understanding of phishing attacks (Kortjan & Solms 2014).

South African organisations face significant risks as cyber threats grow in both frequency and complexity. Recent research highlights a sharp rise in security incidents in 2024, with experts attributing this trend to a shortage of awareness and skilled professionals. The Fortinet in-depth study for the 2024 Cybersecurity Skills Gap Global Research Report indicates that their research surveyed 1850 information technology (IT) and cybersecurity decision-makers across 29 countries, including SA. While the report presents global trends, the findings from South African respondents paint a concerning picture of the country's cybersecurity readiness and resilience.

The data show that only 4% of South African organisations avoided cyber-attacks in the past 12 months. Half of the respondents reported experiencing up to four attacks, while 10% faced nine or more. The financial consequences have been significant, with 39% of South African organisations reporting losses exceeding \$1 million and at least one entity suffering a loss greater than \$6m. Julie Noizeux, Channel Manager at Fortinet SA, emphasises the gravity of the situation: 'South Africa is clearly a prime target for attacks, yet we remain behind in cybersecurity investments on a global scale' (SA Business Integrator 2024).

Educational institutions are lagging in the deployment of phishing attack awareness for users. In a study conducted by Benenson et al. (2017) within the university, 1200 users received phishing messages on emails and Facebook that required them to click on a malicious link. The number of users who were aware of the university's anti-phishing policy was mere 10%.

Nadeem et al. (2023) suggest that to mitigate phishing attacks, a range of detection and prevention techniques have been developed. User education and awareness training are essential for empowering individuals to identify and report phishing attempts. Technological measures, including email filtering, two-factor authentication, website certificate verification, anti-phishing toolbars and the application of machine learning (ML) and artificial intelligence (AI), are employed to enhance detection and prevention efforts. Ongoing research and innovation, alongside the implementation of these strategies, are vital in reducing the risks associated with phishing threats.

This study responds to Tatipatri and Arun's (2024:18163) call to establish a framework and develop cybersecurity measures to counter data manipulation and cyber-attacks, along with the research of Nadeem et al. (2023) to mitigate phishing attacks.

Conceptual framework

The theoretical framework enables the researcher to set the parameters for the literature review in relation to the topic under investigation. The framework can also help the researcher organise the literature review according to the main theories or themes (Kumar 2011). Table 1 discusses and provides attributes of the theoretical frameworks used in cybersecurity studies.

Adoption of the technology threats avoidance theory framework

The Technology Threats Avoidance Theory (TTAT) framework serves as the foundation for this study, as it enables IT users within the university's network to avoid malicious phishing attacks. Technology Threats Avoidance Theory is particularly well-suited for phishing awareness programmes because it incorporates threat appraisal (assessing the severity and susceptibility to cyber threats) and coping appraisal (evaluating users' ability to mitigate phishing risks). Unlike general cybersecurity awareness models, TTAT focusses on individual users' responses to cybersecurity threats, making it especially relevant in a university setting where awareness and behaviour modification are critical.

To minimise cyber-attacks, users were made aware of phishing threats and their potential consequences, and they were educated on various countermeasures to defend against phishing attacks (Liang & Xue 2009). Technology Threats Avoidance Theory has been successfully applied in multiple studies.

In this study, TTAT played a key role in developing the phishing awareness programme. The framework ensured that the programme incorporated threat appraisal, which involved presenting end-users with information on the frequency, methods and negative impacts of phishing attacks. By increasing awareness of these risks, users may be encouraged to change unsafe online behaviours while using the university's

TABLE 1: 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' (Zadeh, Thurasamy & Hanifah 2019)	'User awareness of security countermeasures and its impact on Information Systems misuse: a deterrence approach' (John, Hovav & Galletta 2009)
The 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 IT users of IT threats and the 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.	Perceived Behavioural Control 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' attitudes towards the use of anti-malware software. The findings showed that the perceived price level harmed the students' attitude. In contrast, information security awareness had a positive effect on the students' perspective on anti-malware software.	The GDT was used to reduce intentional insider security threats to IS resources. It 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 programmes, and computer monitoring. The results showed that these practices reduced insider security threats, and the perceived severity of punishment also reduced insider security threats to IS within companies.

Note: Please see the full reference list of this article, Kayomb, J.M., Francke, E.R. & Ncubukezi, T., 2025, 'A phishing attack awareness framework for a South African University of Technology', *South African Journal of Information Management* 27(1), a1949. <https://doi.org/10.4102/sajim.v27i1.1949> for more information.
IT, information technology; IS, information systems.

network. Furthermore, TTAT guided the inclusion of various security mechanisms and mitigation techniques, equipping end-users with the necessary tools to reduce the impact of phishing attacks on the university's IT infrastructure.

Aim and objectives

The study aims to develop a Phishing Attack Awareness Framework for users at a university of technology in the Western Cape province.

Objectives

- 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.
- To investigate the nature of a phishing attack awareness programme at a university of technology.

Research methods and design

Study design

This study uses the qualitative research approach because its benefits support the achievement of the research objectives. The objective of this research is to investigate phishing attacks and develop a Phishing Attack Awareness Framework. A qualitative study design allows the researcher 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, among others. A qualitative study enables efforts to understand these human attributes in phishing attacks. A qualitative study is a subjective research approach, and such an approach looks at intangible things such as perceptions, values and attitudes (Neville 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 from the qualitative approach are mainly because of the nature of the research questions. This is crucial to the understanding of other issues that the researcher was not aware of (Bryman & Bell 2011).

Setting

This study used a case study research strategy because it is often associated with qualitative studies (Kumar 2011). Luthfiandana (2024:29) argues that a case study is an in-depth research method that examines one or more examples to understand a specific phenomenon within a particular and complex context. This research focussed on the users within a university of technology to gather information necessary to combat phishing attacks.

Study population and sampling strategy

This study's population consisted of university academics, first-year and fourth-year students and industry experts in the Western Cape, South Africa. Of this large population, a small but representative group was selected (Neuman 2014). The sample group provided rich and relevant information that enabled the study to answer the research questions to some extent (Ritchie & Lewis 2003). Because of time constraints, the study focussed on one university of technology in the province.

A purposive sampling method involves selecting a group of informants representing a large population who know the problem under investigation. This study included users who were likely to encounter phishing attacks on the network because of the value of the information they have access to on the computer network (Kothari 2004). Furthermore, the purposive sampling method aligned with the research strategy selected in this study (Greener 2008).

The sample of 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 (Cleary, Horsfall & Hayter 2014).

Data collection

The researcher collected data from the following groups: students, academics and IT technical staff. The student category was made up of 8 first-year students and 20 third-year students. These students were part of the Department of IT within the Faculty of Informatics and Design. 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 2 staff members in total, consisting of 1 manager of IT strategic services and 1 information security officer. These technical staff were responsible for the IT services for the entire university. These services included network services, hardware and software, printing, admin systems, emails and telephony.

Questionnaires were used as a data collection method because they are suitable for qualitative research. The questionnaire allowed the participants to provide information about the characteristics of a topic of interest, behaviour or attitudes towards the topic under investigation (Nicholas, French & Valentine 2010). 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 et al. 2010). Prior to the administration of the questionnaires, the researcher sent a request to the participants explaining the purpose, importance of the research and ethical issues to be addressed during the collection of data. Once the request was approved, the researcher selected a small sample purposively and conveniently to represent the large group to respond to the questionnaire.

Data analysis

Thematic analysis is used in the qualitative study, where data are collected and analysed from the participants' perspectives and experiences (Aronson 1995). Qualitative data in this study were analysed in six main steps to identify major themes and patterns in the data set, as proposed by Maguire and Delahunt (2017).

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.

Ethical considerations

The investigator applied for an ethical approval certificate 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. Ethical approval to conduct this study was obtained from Cape Peninsula University of Technology and Faculty of Informatics and Design Research Ethics Committee (No. 217074812/2021/14).

All participants provided informed consent before participating in the study, and their confidentiality and anonymity were maintained throughout the research process. The study adhered to ethical guidelines, ensuring that the participant's rights and well-being were protected at all stages of the research.

Results

Students and academics

The results presented in this section are based on the responses from students and academics at the University of Technology.

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

Student perspective: The survey among students revealed that 39% of the students received phishing attacks, while 61% did not receive phishing attacks.

Academic perspective: The survey among academics revealed that 64% confirmed that they had received phishing attacks, while 36% did not.

Please elaborate on how you received a phishing attack

Student perspective: The students revealed the following phishing techniques in the questionnaire which align with the manner in which sensitive information such as usernames and passwords are typically collected from victims (Wu, Miller & Garfinkel 2006):

'Received via email, they posed as a legitimate announcement or email from the Computer and Telecommunications Services [CTS] desk or Newsflash. I asked users and so on to change their

passwords, and they would say something urgent, like due to new security rollouts or protocols that 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.' (S2, Student)

'I received an email stating that my account was hacked and that I needed 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.' (S9, Student)

It appears that phishers use the following platforms for phishing activities: SMS, Email, social media and telephone. Majority (79%) of the phishing attacks take place via emails, 14% via SMS and 7% via social media.

Academic perspective: The academics reported the following techniques in the questionnaire where they deemed it important to respond as it appeared to come from official institutional sources:

'Email was received from an address similar to the institution address but with a slight difference. The email came across as official communication by the CTS department, but it wasn't.' (I5, Academic)

'Was about some aspect where they wanted my login and password to finalise admin processes.' (I7, Academic)

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

Student perspective: The students indicated that they had received phishing awareness reminders in the following manner: 15% once a week, 31% once a month, 12% once a term, 15% once a semester, 15% once a year and 12% none.

Academic perspective: The academics indicated that they had received phishing awareness reminders in the following manner: 26% once a week, 33% once a month, 26% once a term, 8% once a semester, and 7% none.

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

The survey suggests that a phishing attack awareness programme informs end-users about phishing attacks and mitigation techniques. The users are educated by the Computer and Telecommunications Services (CTS) department of the university, as per the responses received from the 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.' (I5, Academic)

'CTS attempts to educate us about aspects of phishing attacks.' (I3 Academic)

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

The IT technical staff revealed the following techniques in response to the question:

'Display name spoofing, especially for business email compromise [BEC] attempts.' (I1, Technical Staff)

'It would be the targeting of the user's personal cell phones via SMS and/or WhatsApp.' (I2, Technical Staff)

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

The IT technical staff revealed the following to indicate that it is true that there is a high number of phishing attacks that impersonate people of authority:

'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.' (I2, Technical Staff)

'It is estimated that the percentage of reported phishing attacks is 50.' (I1, Technical Staff)

What are the percentages of phishing attacks with links that mimic the legitimate website?

The IT technical staff revealed the following in response to the question:

'Those that are coming through to the user, probably 10% – the rest is blocked by our mail security software before reaching the user.' (I2, Technical Staff)

What is the nature of the phishing awareness programme within the organisation?

The IT technical staff revealed the following in response to the question:

'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.' (I1, Technical Staff)

'Cyber Security Awareness Education, different modules and the phishing campaigns. The content includes Phishing, Info Protection, Passwords, and Data in Motion, among other things.' (I2, Technical Staff)

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

The IT technical staff revealed the following in response to the importance of communication in a phishing awareness programme:

'Constant communication, expressing the impact of cyber risks in a way that resonates with the user base.' (I1, Technical Staff)

'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.' (I2, Technical Staff)

Discussion

Frequencies of phishing attacks

The findings suggest that phishing attacks are on the rise. Students within the Department of IT revealed that 29% of the students received phishing attacks and academics showed that 64% received phishing attacks. The IT technical staff reported that phishing attacks tend to surge at the beginning and end of the academic year, likely because of increased email activity and administrative communications

during these periods. According to their observations, while the university's security software successfully blocks the majority of phishing attempts, a smaller portion still bypasses the filters, reaching end-users. This trend aligns with global cybersecurity findings, which indicate that phishing attacks frequently target institutions during high-traffic periods (Kaspersky 2022; Mimecast 2024b). Moreover, the survey revealed that 21% 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.

Many studies demonstrated increased phishing attacks over the years. The IT experts discovered phishing attacks for the first time in 1990. This resulted in the creation of fake accounts on America Online network systems (Jakobsson & Myers 2006). Moreover, a study of email phishing at the University of West in England showed that 10000 email users were victims of phishing attacks in September 2018. These victims were among the 4000 staff and 28790 students who had email addresses issued by the university (Legg & Blackman 2019). 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).

Awareness of phishing attacks

The findings reveal the following about students and periods of phishing awareness reminders: 31% once a month, 15% once a week, 15% once a semester, 15% once a year, 12% once a term and 12% none. The academics received phishing awareness reminders in the following manner: 33% once a month, 26% once a term, 8% once a semester, 26% once a week and 7% none. The IT technical staff suggested that users receive 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. 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).

Aldawood and Skiner (2019) further argued that when the cybersecurity experts did not conduct phishing awareness campaigns and training in a timely manner, 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. In addition, 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. An awareness survey showed that 38% of users complied with information security policy and rules before the cybersecurity training and 70% complied after the training (Stefaniuk 2020).

Strategies for phishing attacks

The findings reveal that the phishing techniques among students are via email posing as a legitimate announcement or email from the CTS desk or Newsflash (the institution's official email for announcements). It requested users to change their password via a link urgently because of new security rollouts or protocols that have changed. Likewise, studies conducted in the past revealed that attackers embed a malicious link into phishing emails, mimicking popular websites by creating copies of the original websites of reputable organisations. 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. For example, the survey response from a student revealed the following:

'I 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.' (S9, Student)

An academic responded in the following manner:

'The email was received from an address similar to the institution's address but with a slight difference. The email came across as official communication by the CTS department, but it wasn't.' (I5, Academic)

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).

Other than mobile applications, attackers use other platforms, such as website login pages, emails and other tools, to launch their phishing attacks. The researcher investigated these platforms by collecting responses from students, academics and IT technical staff. The responses from the students were as follows: 'Was about some aspect where they wanted my login and password to finalise admin processes', whereas the IT technical staff indicated, '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 technical staff responses showed that phishers use platforms for phishing activities such as SMS, email, social media and telephones. The percentage of students who use the platforms where they received phishing attacks is 79% for emails, 14% for SMSs and 7% for social media used by phishers for attacks. On the other hand, study done by Ferreira and Teles (2019) demonstrated that attackers manipulate emails to infiltrate computer systems. Other studies also showed that phishers designed websites that offered rewards to the user to obtain unauthorised access to victims' accounts (Maimon et al. 2021).

Nature of phishing attack programme

The CTS department of the university educated users about phishing attacks through the phishing attack programme. The academics indicated the following:

'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.' (I1, Technical Staff)

'It attempts to educate us about aspects of phishing attacks'. (I2, Technical Staff)

The IT technical staff reported that users receive 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. Furthermore, users also receive Cyber Security Awareness Education, which includes different modules and phishing campaigns. The content includes Phishing, Info Protection, Passwords and Data in Motion, among other things.

On the other hand, study done by Gardner and Thomas (2014) demonstrated that IT experts used phishing awareness campaigns to inform end-users about potential cyber threats. These campaigns led to users' responsible online behaviour. Furthermore, Wilson and Hash (2003) argued that cybersecurity campaigns guide users towards responsible use of IT systems and electronic information to the end-users. Cybersecurity experts used these campaigns to inform the end-users about the repercussions of not complying with the cybersecurity rules. These rules contained guidance for using IT systems and protecting confidential information (Wilson & Hash 2003).

The IT technical staff within the university said that one way of raising phishing awareness was to communicate to the end-users about rules for using computers and related technologies as per the following statements:

'(a) Constant communication, (b) expressing the impact of cyber risks in a way that resonates with the user base, and the other method of raising awareness was (c) to simulate phishing attacks.' (I1, Technical Staff)

As per preceding response:

'I believe all three are important for our users at the moment. Our strategy reaches everyone, and they can choose to participate on their own 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.' (I2, Technical Staff)

Moreover, cybersecurity experts have argued in studies that they achieved cybersecurity awareness through the education of users on the computer network. The education had the following contents: the use of IT systems and electronic information and the consequences of non-compliance with the best practices (Wilson & Hash 2003). In addition, other researchers demonstrated that IT experts conducted phishing awareness through the simulation of phishing attacks among users on the network (Bada et al. 2019).

Proposed phishing attack awareness framework

Figure 1 provides a synthesised visualisation of the research findings. 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 the theoretical body of knowledge significance associated with phishing in higher education contexts. Furthermore, this provisional framework offers decision-makers and policy designers practical and proactive implementation guidelines. The Phishing Attack Awareness Framework includes four elements: the frequencies of phishing attacks, strategies of phishing attacks, awareness of phishing attacks and the nature of a phishing attack programme.

Strength and limitations

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 to achieve the study's objective. It was also used to develop a framework to support the education of users about phishing attacks within the University of Technology. Existing frameworks, such as the General Deterrence Theory (GDT), focus on policy enforcement and punishment to deter security violations. The Perceived Behavioural Control (PBC) examines how users' perceived control over cybersecurity influences their actions. Unlike these models, the Phishing Attack Awareness Framework provides a structured psychological approach to influencing user behaviour, making it a more suitable choice for phishing awareness initiatives. While the research achieved its objective of developing recommendations for a phishing awareness framework, the study was limited by having students and

academic participants from one department only because of time constraints.

Recommendations

The study presents a Phishing Attack Awareness 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 categorises these processes into four elements: frequencies of phishing attacks, awareness of phishing attacks, the nature of a phishing attack 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 programmes. These four elements are further discussed as follows:

- Frequencies of phishing attacks: The findings showed many phishing attacks and victims of phishing attacks among users at the University of Technology. In the university's awareness programme, the CTS informs users about the number of phishing attacks and victims, and this section of the programme forms the threat appraisal to motivate users to avoid phishing threats. Highlighting the number of victims personalises the risk, making it more relatable and urgent, which in turn increases motivation for users to engage in phishing training as a proactive measure to protect themselves.

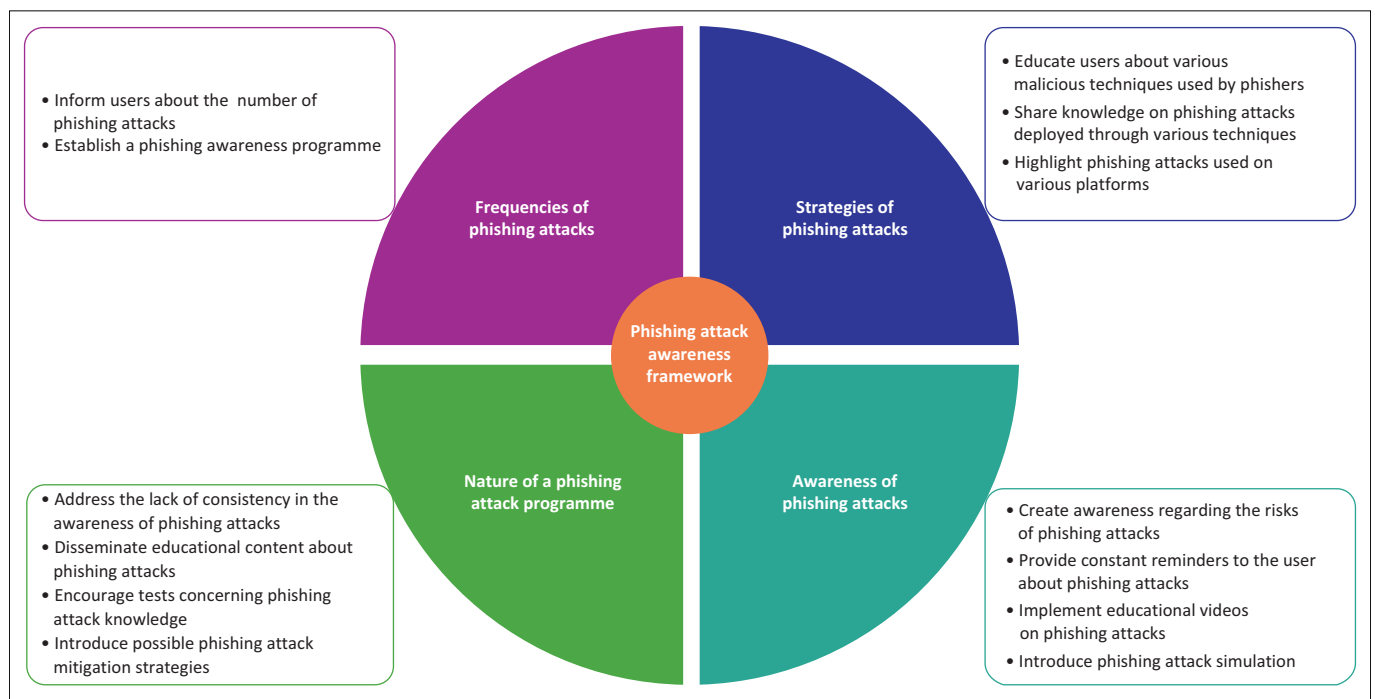


FIGURE 1: Proposed phishing attack awareness framework.

- **Strategies for phishing attacks:** The findings showed that phishers use different techniques in phishing attacks. In the university's phishing awareness programme, 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.
- **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 programme, the IT experts send convenient reminders of phishing attacks. The reminder process raised awareness of phishing attacks against the ever-evolving phishing attack among users.
- **Nature of phishing attack programme:** The university's research findings showed the importance of educating users about phishing attacks. In the university's phishing awareness programme, 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.

Implementation plan of the phishing attack awareness framework

The framework could be implemented through a phased approach within the university, integrating the following activities:

Phase 1: Awareness campaigns

- Conduct quarterly cybersecurity awareness training sessions.
- Disseminate phishing awareness materials via email and campus digital boards.

Phase 2: Simulated phishing exercises

- Send periodic simulated phishing emails to assess user responses.
- Provide real-time feedback to users on their interaction with phishing attempts.

Phase 3: Reporting and monitoring system

- Develop a phishing incident reporting tool for staff and students.
- Analyse reported incidents and identify vulnerabilities in the network.

Phase 4: Policy and enforcement measures

- Strengthen university policies regarding phishing prevention.
- Implement mandatory cybersecurity training for IT-related staff and faculty members.

Conclusion

The study is about developing a Phishing Attack Awareness Framework for users at the University of Technology in the Western Cape province to educate them about phishing

attacks. The literature review and the study's results 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. The implementation of this Phishing Attack Awareness Framework aims to reduce phishing-related security breaches by fostering a culture of awareness. Furthermore, it could improve detection and response time to phishing threats. Lastly, it could enhance cybersecurity resilience by integrating best practices into the university's IT policies.

While phishing awareness frameworks exist, they often do not account for localised phishing threats specific to South African universities. The Phishing Attack Awareness Framework integrates a theoretical behavioural model (TTAT) with practical security measures. It provides a structured, continuous engagement model rather than one-time interventions. It also addresses phishing attack patterns unique to university users, including academic fraud, research data theft and credential hijacking. By addressing these critical gaps, our Phishing Attack Awareness Framework makes a distinct and valuable contribution to the field of cybersecurity in higher education.

Because of the time constraint, this study focussed on the Department of Information Technology at one university in the Western Cape province, and future work should include other departments and universities in the province.

Acknowledgements

This article is partially based on the author, J.M.K.'s Master's dissertation entitled 'Phishing attack awareness amongst users at a university of technology in the Western Cape', towards the degree of Master of Information and Communication Technology in the Faculty of Informatics and Design, Cape Peninsula University of Technology, South Africa, with supervisors Dr E.R. Francke and Dr T. Ncubukezi, received October 2024. It is available here, https://etd.cput.ac.za/bitstream/20.500.11838/4127/1/217074812_Kayomb_Mutomb.pdf.

Competing interests

The authors declare that they have no financial or personal relationships that may have inappropriately influenced them in writing this article.

Authors' contributions

J.M.K. wrote the article under the supervision of E.R.F. and T.N. All authors read and approved the final article.

Funding information

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Data availability

The data that support the findings of this study are available from the corresponding author, E.R.F. upon reasonable request. All empirical data collected for the study will be stored on eSango, the research data repository, powered by Figshare, for the Cape Peninsula University of Technology (CPUT). It is solely meant to make accessible research data as per FAIR principles, that is, Findable, Accessible, Interoperable, and Reusable in support of Open Science <https://esango.cput.ac.za/>.

Disclaimer

The views and opinions expressed in this article are those of the authors and are the product of professional research. The article does not necessarily reflect the official policy or position of any affiliated institution, funder, agency or that of the publisher. The authors are responsible for this article's results, findings and content.

References

- Aldawood, H. & Skinner, G., 2019, 'Review cyber security social engineering training and awareness programs-pitfalls and ongoing issues', *Future Internet* 11(3), 1–16. <https://doi.org/10.3390/fi11030073>
- Aronson, J., 1995, 'A pragmatic view of thematic analysis', *The Qualitative Report* 2(1), 1–3. <https://doi.org/10.46743/2160-3715/1995.2069>
- Bada, M., Solms, B. & Agraftiotis, I., 2019, 'Reviewing national cybersecurity awareness for users and executives in Africa', *arXiv* 12(1), 108–118.
- Benenson, Z., Gassmann, F. & Landwirth, R., 2017, 'Unpacking spear-phishing susceptibility', *International Workshops* 10323, 610–627. https://doi.org/10.1007/978-3-319-70278-0_39
- Bernard, H., 2013, *Social research methods: Qualitative and quantitative approach*, 2nd edn., Sage, Los Angeles, CA.
- Broadhurst, R., Skinner, K., Sifniotis, N. & Matamoros-Macias, B., 2018, 'Cybercrime risks in a university student community', *SSRN Electronic Journal* 1–11. <https://doi.org/10.2139/ssrn.1376319>
- Bryman, A. & Bell, E., 2011, *Business research methods*, 3rd edn., Oxford University Press, Oxford.
- Cleary, M., Horsfall, J. & Hayter, M., 2014, 'Data collection and sampling in qualitative research: Does size matter?', *Journal of Advanced Nursing* 70, 473–475. <https://doi.org/10.1111/jan.12163>
- Ejaz, A., Mian, A.N. & Manzoor, S., 2023, 'Life-long phishing attack detection using continual learning', *Scientific Reports* 13(1), 1–14. <https://doi.org/10.1038/s41598-023-37552-9>
- Ferreira, A. & Teles, S., 2019, 'Persuasion: How phishing emails can influence users and bypass security measures', *International Journal of Human-Computer Studies* 125, 19–31.
- Gardner, B. & Thomas, V., 2014, *Building an information security awareness program: Defending against social engineering and technical threats*, 1st edn., Elsevier, Waltham.
- Greener, S., 2008, *Business research methods*, Ventus Publishing, London.
- Hussan, H. & Mangi, S.M., 2025, 'BERTPHIURL: A Teacher-Student Learning Approach Using DistilRoBERTa and RoBERTa for Detecting Phishing URLs', *Journal of Future Artificial Intelligence and Technologies* 1(4), 417–428. <https://doi.org/10.62411/faith.3048-3719-71>
- Jakobsson, M. & Myers, S., 2006, *Phishing and countermeasures: Understanding the Increasing Problem of Electronic Identity theft*, John Wiley & Sons, Bloomington, IN.
- John, A., Hovav, A. & Galletta, D., 2009, 'User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach', *INFORMS* 20(1), 79–98. <https://doi.org/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*, viewed 23 March 2023, 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>
- Kortjan, N. & Solms, R., 2014, 'A conceptual framework for cyber-security awareness and education in SA', *South African Computer Journal* 52, 29–41. <https://doi.org/10.18489/sacj.v52i0.201>
- Kothari, C., 2004, *Research methodology: Methods and techniques*, 2nd edn., New Age International Limited, New Delhi.
- Kumar, R., 2011, *Research methodology: A step-by-step guide for beginners*, 3rd edn., Sage, Los Angeles, CA.
- Legg, P. & Blackman, T., 2019, 'Tools and techniques for improving cyber situational awareness of targeted phishing attacks', *International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2019, IEEE*, pp. 1–4. <https://doi.org/10.1109/CyberSA.2019.8899406>
- Li, D., Chen, Q. & Wang, L., 2024, 'Phishing attacks: Detection and prevention techniques', *Journal of Industrial Engineering and Applied Science* 2(4), 48–53. <https://doi.org/10.5281/zenodo.12789572>
- Liang, H. & Xue, Y., 2009, 'Avoidance of information technology threats: A theoretical perspective', *MIS Quarterly* 33(1), 71–90. <https://doi.org/10.2307/20650279>
- Luthfiandana, R., Santoso, L., Febrian, W.D., Soehaditama, J.P. & Sani, I., 2024, 'Qualitative research concepts: Phenomenology, grounded theory, ethnography, case study, narrative', *Siber Journal of Advanced Multidisciplinary* 2(1), 26–36. <https://doi.org/10.38035/sjam.v2i1.91>
- Maguire, M. & Delahunt, B., 2017, 'Doing a thematic analysis: a practical, step-by-step guide for learning and teaching scholars', *All Ireland Journal of Higher Education* 9(3), 3351.
- 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* 1–19. <https://doi.org/10.1177/08944393211046339>
- Marforio, C., Masti, C., Soriente, C., Kostianen, K. & Capkun, S., 2015, *Personalised security indicators to detect application phishing attacks in mobile platforms*, viewed 28 September 2020, from <https://arxiv.org/pdf/1502.06824.pdf>
- Mimecast, 2019, *The state of email security report 2019 – South Africa*, viewed 28 September 2020, from https://info.mimecast.com/sa-the-state-of-email-security.html?utm_medium=SEMPPC&utm_source=GooglePPC&utm_campaign=7011N000001Uvq1QAS&utm_term=mimecast%20phishing&gclid=Cj0KCQIAtf_tBRDtARISAlbAKE0IAe2v2XBX-nAJ9XsDIYBzGU2JareyruPph3X_I54VsdY07TSkUgaAuf6EALw_wcB
- Mimecast, 2024a, *Preventing a data breach*, Mimecast, viewed 10 February 2025, from <https://www.mimecast.com/blog/how-to-prevent-a-data-breach-in-todays-cyber-environment/>
- Mimecast, 2024b, *The State of Email and Collaboration Security 2024*, Mimecast, viewed 26 August 2024, from <https://www.mimecast.com/the-state-of-email-and-collaboration-security-2024/>
- Mouton, F., Teixeira, M. & Meyer, T., 2017, *Benchmarking a mobile implementation of the social engineering prevention training tool*, IEEE, Johannesburg.
- Nadeem, M., Zahra, S.W., Abbasi, M.N., Arshad, A., Riaz, S. & Ahmed, W., 2023, 'Phishing attack, its detections and prevention techniques', *International Journal of Wireless Information Networks* 12(2), 13–25. <https://doi.org/10.37591/IJWSN>
- Neuman, L., 2014, *Social research methods: Qualitative and quantitative approaches*, 7th edn., Pearson Education, Harlow.
- Neville, C., 2005, *Introduction to research and research methods*, Effective Learning Service, Bradford.
- Nicholas, C., French, S. & Valentine, G., 2010, *Key methods in geography*, 2nd edn., Sage, London.
- Ritchie, J. & Lewis, J., 2003, 'Qualitative research practice: A guide for social science students and researchers', *The proceedings of the second international conference on inventive systems and control*, Sage, London, p. 757.
- SA Business Integrator, 2024, *South Africa's cybersecurity crisis – new research shows lack of local skills to combat threat-laden landscape*, SA Business Integrator, viewed 10 February 2025, from <https://sabusinessintegrator.co.za/cyber-security/south-africas-cybersecurity-crisis-new-research-shows-lack-of-local-skills-to-combat-threat-laden-landscape/>
- San Diego University, 2017, *Phishing awareness program*, viewed n.d., from <https://www.sandiego.edu/its/security-and-privacy/phishing-awareness-program.php>
- Specops, 2025, *Specops breached password report 2025*, Specops, viewed 10 February 2025, from <https://specopssoft.com/our-resources/most-common-passwords/>
- Stefaniuk, T., 2020, 'Training in shaping employee information security awareness', *Entrepreneurship and Sustainability Issues* 7(3), 1832–1846. [https://doi.org/10.9770/jesi.2020.7.3\(26\)](https://doi.org/10.9770/jesi.2020.7.3(26))
- Tatipatri, N. & Arun, L., 2024, 'A comprehensive review on cyber-attacks in powers: Impact analysis, detection, and cyber security', *IEEE Access* 12, 18147–18167. <https://doi.org/10.1109/ACCESS.2024.3361039>
- Thomas, K., Li, F., Zand, A., Barrett, J., Invernizzi, L., Markov, Y., Comanescu, O. et al., 2017, 'Data Breaches, phishing, or malware? Understanding the risks of stolen credentials', *Proceedings of the ACM Conference on Computer and Communications Security*, Dallas, Texas, USA, October 30, 2017, pp. 1421–1434.
- West, J., Andrews, J. & Dean, T., 2019, *Network + guide to networks*, 8th edn., Cengage Learning, Boston, CA.
- Wilson, M. & Hash, J., 2003, 'Computer security: Building an information technology security awareness and training program', *NIST* 1–70. <https://doi.org/10.6028/NIST.SP.800-50>
- Winder, D., 2025, *New security alert – 1 Billion passwords Stolen by Malware, Act Now*, Forbes, viewed 10 February 2025, from <https://www.forbes.com/sites/daveywinder/2025/01/23/security-alert-issued-as-1-billion-passwords-stolen-by-malware-act-now/>
- Wu, M., Miller, R. & Garfinkel, S., 2006, 'Do security toolbars actually prevent phishing attacks?', *The Proceedings of Conference on Human Factors in Computing Systems* 1, 601–610. <https://doi.org/10.1145/1124772.1124863>
- Zadeh, A., Thurasamy, R. & Hanifah, H., 2019, 'Modelling anti-malware use intention of university students in a developing country using the theory of planned behavior', *Kybernetes* 48(8), 1565–1585. <https://doi.org/10.1108/K-05-2018-0226>