Cybersecurity in the workplace: Factors that influence cybersecurity protective behaviour against phishing in South Africa

A Masters Dissertation presented to the

Department of Information Systems

University of Cape Town

By

KARABO PILANE

In partial fulfilment of the requirements for the Master of Commerce: Information Systems

2023

Supervisor: Zainab Ruhwanya

5 November 2023

Cybersecurity in the workplace: Factors that influence cybersecurity protective behaviour against phishing in South Africa

Declaration

(a) I know that plagiarism is wrong. Plagiarism is to use another's work and pretend that it is one's own.

(b) I have used the APA convention for citation and referencing. Each contribution to, and quotation in, this dissertation from the work(s) of other people has been attributed and has been cited and referenced.

(c) This dissertation is my own work.

(d) I have not allowed and will not allow anyone, to copy my work with the intention of passing it off as his or her own work.

(e) I acknowledge that copying someone else's assignment, essay or dissertation, or part of it, is wrong, and I declare that this is my own work.

Signed by candidate

Signature:

Date: November 2023

Full Name of Student: Karabo Pilane

Student Number: PLNLET001

Acknowledgements

I remain grateful to my Maker for affording me the opportunity and supplying me with the strength to go through the wonderful journey of knowledge acquisition.

I owe this one to my beloved supervisors, Ms Zainab Ruhwanya and Prof Irwin Brown for taking me by the hand to walk the path. What a journey! My research supervisors have made a mark in my life that cannot be erased. They did it one step at a time, with grace, unearthing capabilities within me I never thought existed. One cannot wait to continue working with them in the next research endeavours or other academic projects as they have a lot of academic wealth piled on them.

I also thank the team of UCT researchers who took me through this learning journey together with my supervisors. The program was very enriching, and fun but challenging. In addition, my peers in the Masters class were fun to engage with, never a dull moment with them. Also, I remain thankful to all participants from South African organisations who participated in my survey.

A special thanks to my employer who supported me financially and with other resources to complete this task coupled with work demands. Finally, thanks to my wife, two daughters and my son for their faithful prayers to make this journey a reality and success.

Abstract

In South Africa one of the top cybersecurity threats is phishing. Furthermore, employees' responses to phishing emails can either bolster or weaken an organisation's cyber security. It is estimated that more than 90% of data breaches are due to successful phishing attacks. They bring the maximum benefits with little to no cost for cyber attackers. Hence, this study aims to explain the factors that influence cybersecurity protective behaviour against phishing in South African organisations. A quantitative method was used, and data were collected online through a questionnaire survey. One hundred and twenty respondents from South African organisations participated. The partial least squares-structural equation modelling platform provided in SmartPLS-4 was used to model the data. SmartPLS was used to calculate and analyse reliability, convergent and discriminant validity, path coefficients, and significance of relationships. Factors that were identified as influencing cybersecurity protective behaviour against phishing were remote working, cybersecurity awareness, perceived user self-efficacy, facilitating conditions, perceived vulnerability, perceived severity, response efficacy, response costs, and government cyber laws enforcement.

Table of Contents

Table of Figures

Table of Tables

1. Introduction

1.1 Contextual Background

Although investments in information technology have notable economic and financial benefits, cybersecurity remains a challenge to many organisations (Kabanda et al., 2018). Furthermore, as information technology advances so does the cybersecurity management challenge (Scott & Kyobe, 2021). The goal of cybersecurity in information technology management within organisations is to preserve the confidentiality, integrity, and availability of information, but often these goals are not achieved (Stratton et al., 2017; Dremliuga et al., 2021). Confidentiality means information should be accessed only by authorised users while integrity means that information should be complete, reliable, and unchanged (Bispham et al., 2021). Availability means that information should be accessible timeously when needed by authorised users (Bispham et al., 2021). Cybersecurity management enables organisations to manage cybersecurity risks as part of business risks and to limit them to acceptable levels in line with the organisation's risk appetite (Kwak et al., 2020).

The global spread of internet access has increased organisations' reliance on information technologies, resulting in a slew of new cybersecurity vulnerabilities (Calderaro & Craig, 2020; Berlilana et al., 2021). This was exacerbated by the COVID-19 pandemic as many employees had to work remotely (Khan et al., 2020). Cybersecurity vulnerabilities include exposure to phishing, ransomware, distributed denial of service (DDOS), and supply chain attacks. These vulnerabilities may be related to outdated or legacy systems, security misconfigurations, and third-party risks (outsourced information systems services), but there are many other sources of systemic weaknesses. South Africa has not been spared from cyberattacks. Notable South African organisations that have been successfully attacked include Transnet (where the attack brought its operations to a weeklong halt), the Life Healthcare Group, the Department of Justice and Constitutional Development (DOJCD), and TransUnion South Africa (Pieterse, 2021; South African Banking Risk Information Centre, 2023).

Kara and Aydos (2022) suggest that cybersecurity risks to information systems keep increasing despite efforts by organisations that have implemented cybersecurity solutions. Examples of cybersecurity solutions are next-generation firewalls, next-generation antivirus software (AV),

data loss prevention (DLP), endpoint detection and response (EDR), database activity monitoring (DAM) systems, intrusion detection, and intrusion prevention systems.

A contrasting perspective is that, although cybersecurity threats are a nuisance to management, in many countries they may not pose a major threat to national interests (Kenneth, 2017). Also, according to cyber threat inflation theory, cybersecurity threats may be exaggerated by cybersecurity vendors to gain a profit (Kenneth, 2017). Nevertheless, cybersecurity breaches have been projected to cost the world more than $10 trillion by 2025 (Buckley at al., 2023).

According to the World Economic Forum (WEF) report, cybersecurity failure is ranked the ninth top risk by likelihood (WEF, 2021). In 2017 WEF identified that data fraud or theft ranked by likelihood as a top fifth risk; cyberattacks and data fraud were third and fourth in 2018; and data fraud and cyberattacks were fourth and fifth in 2019 (WEF, 2021). The report of McLennan and Group (2022) ranked cybersecurity failures as seventh in the ranking of top risks that worsened during the COVID-19 pandemic whilst ransomware increased by 435%. During and after the pandemic, the working arrangements of many organisations changed from working from office to working from home or remote working (Khan et al., 2020). Some companies adopted a hybrid work approach, meaning employees could work both from office and remotely (Klein, 2021).

Having conducted a survey Mimecast reported 2021 as the worst year recorded for cybersecurity (State & Security, 2022). Furthermore, Mimecast found that the incidents of email cyberattacks increased more rapidly than before the COVID-19 pandemic. This may be due to employees working from home, as organisations depend on information technology as a business enabler for the new norm of remote working (Khan et al., 2020). Furthermore, cyber attackers identified the COVID-19 pandemic as an opportunity for financial gain (Khan et al., 2020).

A respected community of cybersecurity researchers identified cybersecurity management issues like phishing, as dominant, especially during and after the COVID-19 pandemic (APWG, 2021; Baral & Arachchilage, 2019; Leet, 2020; McLennan & Group, 2022; State & Security, 2022; Us, 2018). Also, according to Us (2018), phishing remains the most frequently used tool in cyber-attacks and the predominant initiator in cybersecurity breaches across the globe.

Phishing is popular amongst cybercriminals because of its effectiveness (*Microsoft-Protect Yourself from Phishing*, n.d.).

Employees' responses to phishing emails can either bolster or weaken organisations' cyber security (Buckley et al., 2023). It was through phishing that the Bangladesh bank was defrauded of $81 million from the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network (SWIFT, 2019). Cyber attackers also attempted to steal $1 billion from financial organisations across the world and during this attack, the Bangladesh Bank became a victim (CISA, 2020). In South Africa, one of the top cybersecurity threats is phishing (Interpol, 2021). The South African Banking Risk Information Centre (2021) report of annual crime statistics emphasized that digital banking fraud was driven mainly by social engineering including phishing.

Cybersecurity protective behaviours are the intersections between humans and the environment in which they operate and can help minimise or maximise cybersecurity risks (Almansoori et al., 2023; Hong et al., 2021; Mou et al., 2023). Cybersecurity protective behaviours can assist in securing information and are regarded as positive cybersecurity behaviours (Almansoori et al., 2023). Lack of cybersecurity protective behaviours, regarded as negative cybersecurity behaviours is the type of behaviour that may result in the success of cybersecurity attacks (Almansoori et al., 2023; Mou et al., 2023).

1.2 Problem Statement

According to research, South Africa is one of the countries most frequently targeted by cyberattacks such as phishing (Kritzinger at al., 2023; Pieterse, 2021; Wannenburg et al., 2023). However, there are not many peer-reviewed publications that analyse cyber-attacks, such as phishing, that occur in South Africa (Pieterse, 2021). Jansen and van Schaik (2019) acknowledged this gap in studying cybersecurity protective behaviour improvements against phishing, but in that study, the technological, organisational, and environmental contexts were not considered. In addition, earlier studies have considered variables such as remote working, which have recently become more common, as influencing cybersecurity protective behaviour against phishing (Khan et al., 2020). It is estimated that 90% of data breaches are linked to successful phishing attacks (Interpol, 2023).

During the pandemic and afterwards, phishing remained the most frequent type of cyber-attack (Al-Qahtani & Cresci, 2022). Phishing-related cybercrime incidents increased by 220% during the period 2019 to 2020 (Kumar et al., 2022). South African organisations face a problem of increasing phishing attacks and many of them do not appear to have acceptable cybersecurity and cyber resilience postures (Interpol, 2021).

The results of this study are expected to explain the factors influencing cybersecurity protective behaviour against phishing in South African organisations post-COVID-19 lockdowns. There is now a new way of work (remote work and hybrid work) which may warrant a change from the old ways of work as they relate to cybersecurity. Furthermore, besides individual perceptions of phishing avoidance, there may be additional factors related to technology, the organisation, and the environment in which an organisation operates, that may influence cybersecurity protective behaviour against phishing.

1.3 Context of Study

According to Malwarebytes (2019, 2023), the problem of phishing impacts all societies and organisations negatively and reduces trust in information technologies. African organisations are regarded as particularly attractive for cyber attackers and phishing is one of the cybersecurity issues faced by those organisations (KPMG, 2022). The African Cyber Threat Assessment report highlighted that more than 90% of African businesses run their operations without proper cybersecurity protective controls and this has the potential to threaten business continuity (Interpol, 2021). In contrast, developed countries have more reliable information and communication technology (ICT) infrastructures than developing economies like South Africa (Matli, 2022). Therefore, organisational cybersecurity protective measures in South African organisations may not be as cyber resilient as in the developed economies. According to KPMG (2022), the top cybersecurity threat in the Southern African region is business email compromise and phishing is a part of business email compromise.

Mcanyana et al. (2020) are of the view that the South African national government has poor cybercrime legislation due to implementation challenges or lack of enforcement of legislation. Similarly, Dlamini and Mbambo (2019) report that the South African government struggles to implement cybersecurity-related laws effectively. This is a concern for South African organisations and possibly discourages cybersecurity protective behaviour against phishing by

employees. South Africa has its own unique set of national challenges including a scheduled load-shedding policy that has threatened business continuity for many organisations. Remote working employees may have little or no control over power outages that affect the availability of the ICT infrastructure and as noted earlier, availability is important for cybersecurity (Mathi, 2022).

Nonetheless, the proposition is that there are factors that can influence cybersecurity protective behaviour against phishing in workplaces for South African organisations post-COVID-19 lockdowns. This proposition is in line with the work done by Jansen and van Schaik (2019). It is worth noting that, according to the Internet Crime report (2021), South Africa ranked fifth out of the top twenty international cybercrime victims. Furthermore, South African organisations suffer significant financial losses caused by phishing, with the public sector the most seriously affected (Butler & Butler, 2020; Pieterse, 2021). South Africa is estimated to have lost up to R2.2 billion rands due to cybersecurity incidents of which phishing may be a significant part (Mzekandaba, 2023).

1.4 Research objective and question

The primary objective in this category of research is:

- To explain the factors that influence cybersecurity protective behaviour against phishing in South African organisations.

The research question is:

- What factors influence cybersecurity protective behaviour against phishing in South African organisations?

1.5 Research Value

This research is anticipated to contribute to the cybersecurity body of knowledge. Cybersecurity practitioners, management, academics, and heads of organisations may benefit by gaining insights as to how to strengthen their cybersecurity capabilities. Remote workers may be sensitised through this study regarding the threats posed by phishing. This study will discuss phishing due to its predominance in cybercrime and ultimately cybersecurity.

1.6 Research Overview

This study is organised as follows. Section 2 starts with a review of the academic literature using recent work from cybersecurity researchers. The scope covered included the definition and understanding of phishing, the types of phishing, the evolution of phishing, and the characteristics of phishing. Section 2 continues with a discussion of the three theories that are relevant to cybersecurity protective behaviour against phishing, namely, the Protection Motivation Theory (PMT), the Theory of Planned behaviour (TPB), and the Technology-Organisation-Environment (TOE) framework. The hypotheses were formulated, and the research model (conceptual framework) emerged from the academic literature review, while Section 3 describes the research methodology and design. Section 4 presents the data analysis, and Section 5 reports the findings and a discussion of those findings to the literature, acknowledges research limitations, and proposes future research.

2 Literature Review

2.1 Introduction

This chapter begins with the definition and understanding of phishing. Furthermore, the chapter discusses the theoretical background that was used by researchers for the cybersecurity protective behaviour against phishing. Afterwards, literature was reviewed on factors that influence cybersecurity protective behaviour against phishing.

2.2 Defining and understanding phishing

Phishing is an attempt by cyber attackers to fraudulently access end-users sensitive information (Qabajeh et al., 2018). Similarly, phishing has been described as a deceptive tactic that makes use of a technical capability and manipulates people's trust (emotions) or psychology to persuade them to provide sensitive information needed for the execution of criminal activities (Sun et al., 2016). The definitions by Qabajeh et al. (2018) and Sun et al. (2016) complement each other, but this study will use the definition by Sun et al. (2016) as it is comprehensive. Phishing is, therefore, primarily centred around people and their emotions and cannot solely be countered by technological measures (Butler & Butler, 2018).

The sensitive information which cyber attackers want to access through phishing may include but is not limited to, personally identifiable information (PII) such as end-users identity document (ID) numbers, names, dates of birth, passwords, and photos (Baral & Arachchilage, 2019). In addition, according to the South African Protection of Personal Information Act 4 of 2013, personally identifiable information includes race, gender, sex, and medical information (Parliament of the Republic of South Africa, 2023). Also, financial information, such as account numbers, personal identification numbers (PINs), payslips, and credit scores is usually sensitive. In the organisational context, sensitive information includes trade secrets and company strategies as these provide companies with a competitive edge in the industry in which they operate. The South African Fraud Prevention Service (2023) provides a platform for reporting identity theft-related incidents to combat identity fraud.

HaveIbeenpwned website reported in 2023 that data obtained from cyber-attacks is subsequently placed on the dark web and is, therefore, available to be used in phishing attacks.

This includes email addresses, IP (internet protocol) addresses, usernames, gender, geographic locations, and passwords. One notable case from the South African context was the Experian data breach, which exposed email addresses, employers, government-issued IDs (identifiers), names, occupations, and phone numbers (HaveIbeenpwned, 2023).

2.2.1 Variations of phishing

There are several forms of phishing, such as spear phishing, whaling, pharming, smshing, and vishing (APWG, 2021; Sun et al., 2016). Spear phishing targets a specific user and appears to be from a legitimate source (Kwak et al., 2020). Whaling is aimed at high-ranking officials in organisations (such as corporate executives or senior management) or senior government officials (such as ministers, and members of parliament) (Qabajeh et al., 2018). Smshing, widely used in digital banking fraud, uses short message services (SMS) while vishing is initiated using a phone call and is often called voice phishing (South African Banking Risk Information Centre, 2021). In pharming users are misdirected to a false website when entering a website name on a browser (Google Chrome, Microsoft Edge, Firefox, and many others) (Sun et al., 2016).

Recently, phishing has started to make use of artificial intelligence-generated deep fake videos to deceive unsuspecting users, as it may not be easy to distinguish real videos from fake ones (Fei et al., 2021). However, in all cases of phishing the objective remains to fraudulently access users' sensitive information for financial gain.

2.2.2 Evolution of phishing

New phishing strategies are created every day as a result of information technology advancements and the growing use of internet-enabled gadgets; this is likely to continue (Baral & Arachchilage, 2019, Kabanda et al., 2018; Leet, 2020). The Internet Crime Report (2020) identified phishing as a leading strategy used by cyber attackers leading to cybersecurity breaches and cybercrime in general. The Anti Phishing Working Group (2021) also identified phishing as a major threat to cybersecurity. Most cybercriminals use phishing as a springboard for the execution of unauthorised activities such as ransomware, identity theft and data fraud.

Mimecast, the global leader in email security solutions, reported that three out of four companies receive email-based threats whilst 96% of companies have been the target of email-

related phishing attempts (State & Security, 2022). Mimecast does not anticipate a reduction in phishing attacks and sees it as mutating. Furthermore, the COVID-19 pandemic provided cybercriminals with an exploitable topic (COVID-related news and statistics) that rendered COVID-19-themed phishing a persistent threat (Akdemir & Yenal, 2021; Rameem Zahra et al., 2021). Before the COVID-19 pandemic, other non-COVID themes were exploitable and this may remain post the COVID-19 pandemic (Abroshan et al., 2021).

Cyber attackers can use artificial intelligence and machine learning to launch phishing attacks. Deep fakes, developed through artificial intelligence and machine learning, have introduced a major threat in curbing cybersecurity attacks (Mustak et al., 2023; Mirsky et al., 2023). Deep fakes involve media information that has been digitally altered, including but not limited to videos, sound, and images (Mustak et al., 2023; Mirsky et al., 2023). Several examples of deep fake voice phishing exist. A high-ranking business executive of a company was tricked through voice phishing to transfer money to an attacker's account (Mustak et al., 2023; Mirsky et al., 2023). Similarly, in what cybersecurity practitioners called an uncommon instance of artificial intelligence being employed in hacking, cybercriminals impersonated a chief executive's voice and demanded a bogus payment of $243,000 which was paid (Stupp, 2019). Another case occurred where deep fake voice phishing was used to transfer money ($35 million) to fraudsters (Brewster, 2021).

Cybercriminals have exacerbated phishing attacks with QR (quick response) codes which embed a malicious site where victims are redirected (Sharevski et al., 2022). This type of phishing attack is called quishing because it is aided by QR code scanning.

2.2.3 Characteristics of phishing

Some of the characteristics of phishing are:

- Creating a sense of urgency to act, such as clicking a link that may contain malicious software such as ransomware, backdoor, rootkits, denial of service, viruses, worms, SQL (Structured Query Language) injection,
- Poor spelling and grammar in the email body; however, artificial intelligence-powered tools solutions (e.g. ChatGPT) aid cyber attackers in crafting emails with correct spelling and grammar,

- Fake email domains (redirecting the user to a cyber attacker's website or server),
- Unusual attachments or suspicious links,
- Persuasion,
- Influence (Falade, 2023; Farkhondeh et al., 2020; Microsoft, 2018)

Artificial intelligence (AI) is anticipated to increase the attack landscape of phishing attacks (Falade, 2023; Guembe et al., 2022). The threat landscape may include unknown patterns different to the known types of characteristics mentioned above such as learning and adapting to launch an attack (Guembe et al., 2022).

Chng et al., (2022) identify various types of attackers that engage in phishing, including internal employees, state-sponsored attackers, and professionals. Phishing attackers' motivations differ but the most common one is financial gain. Organisations can suffer financial losses, reputational damage, and lawsuits because of phishing (Falade, 2023). Furthermore, AI-enhanced phishing may lead to disinformation that could tarnish high-ranking officials such as CEOs (chief executive officers), the organisation's image, and so on (Falade, 2023). Disinformation or misinformation against an organisation through AI-enhanced phishing may sway public perception of that organisation.

2.3 Theoretical Background

Three theories that will be discussed in this study are the Protection Motivation Theory (PMT), the Theory of Planned Behaviour (TPB), and the Technology-Organisation-Environment Framework (TOE). The probability of phishing attacks against individuals and organisations succeeding depends on the quality of human decision-making. Therefore, it remains imperative to survey information systems theories that explain human behaviour. Often, the theories below are used for human behavioural studies in Information Systems research.

2.3.1 Protection Motivation Theory

Protection Motivation Theory posits that, when an individual is confronted with a threat, he or she evaluates the threat as well as any potential remedies (Rogers, 1975). Mou et al. (2022) applied the Protection Motivation Theory (PMT) in the context of Information Systems studies and produced the model in Figure 1.

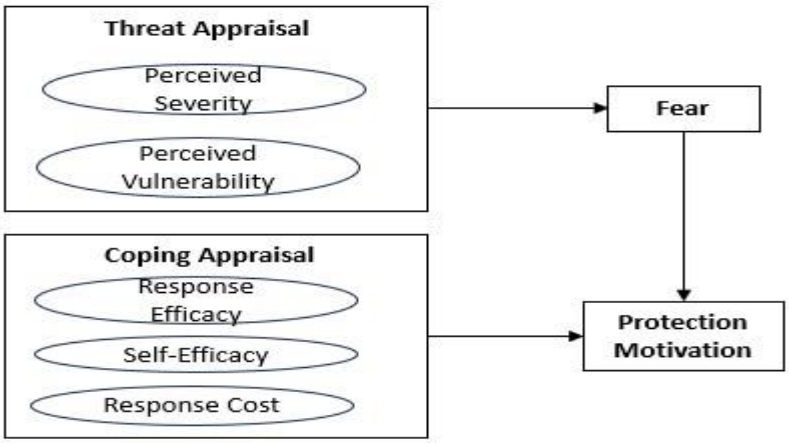

Figure 1: Protection Motivation Theory for Information Systems Research (Mou et al., 2022)

PMT has been widely used in cybersecurity protective behaviour studies (Bax et al., 2021; Bekkers et al., 2023; Jansen & van Schaik, 2019; 2023; Menard et al., 2017; Mou et al., 2022; Ng et al., 2021). In addition, many researchers have used PMT in their studies of phishing (Bayl-Smith et al., 2022; Jansen, 2022) However, not many studies were found to the researcher's knowledge that evaluated the link between threat appraisals and coping appraisals from PMT, but this is part of this study. In this study, coping appraisal is measured through the constructs (factors) of perceived user self-efficacy (see Section 2.4.4), response efficacy (see Section 2.4.8) and response costs (see Section 2.4.9). All three factors or constructs (perceived user self-efficacy, response efficacy, and response costs) have previously been found to influence cybersecurity protective behaviour. Furthermore, in this study, two constructs (perceived vulnerability and perceived severity) make up threat appraisal according to PMT. Perceived vulnerability (see Section 2.4.6) and perceived severity (see Section 2.4.7) are concepts that may have a positive influence on cybersecurity protective behaviour against phishing driving the level of emotional response.

This study discussed and supported the five PMT factors of perceived severity, perceived vulnerability, perceived user self-efficacy, response-efficacy, and response costs as depicted in figure 1. PMT was used as a base framework in this study. Mou et al. (2022) argued that context matters; some PMT constructs or factors (such as perceived severity, perceived vulnerability, and perceived user self-efficacy) may have particularly strong effects in a personal context while others (response cost and response efficacy) may have a more noticeable effects in a

workplace context. Research remains inconclusive on this view of personal versus workplace contexts of PMT (Mou et al., 2022). Some other researchers acknowledged that contexts differ according to nation (Mou et al., 2022).

2.3.2 Theory of Planned Behaviour

The Theory of Planned Behaviour (TPB) has been widely used in behavioural studies of cybersecurity including phishing and is useful in this study of cybersecurity protective behaviour against phishing (Alqahtani & Braun, 2021; Alyahya and Weir, 2021; Arachchilage et al., 2016; Zaman et al., 2021). According to TPM, attitudes (e.g. users' valuation of psychological objects on behaviour), subjective norms (perceived social practices that impact users' behaviour, and perceived behavioural control (PBC) (users' perception of how easy or hard to perform a behaviour).

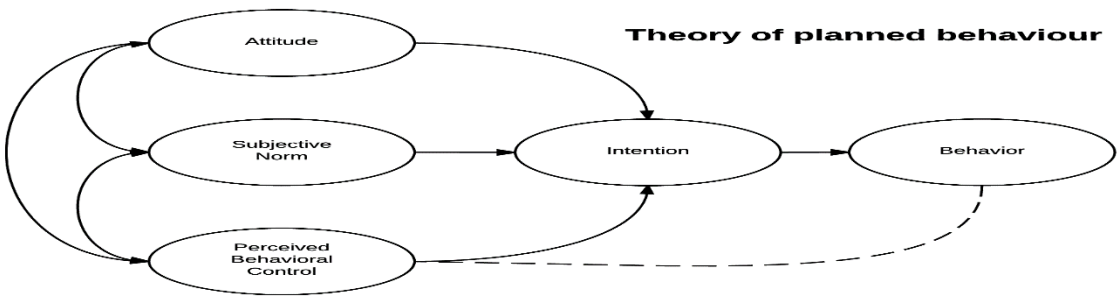

Figure 2: Theory of Planned Behaviour (Azjen, 1991)

TPB can be used to extend PMT since concepts such as user self-efficacy are common to both PMT and TPB. The threat appraisals (perceived vulnerability and perceived severity) from PMT seem to be similar to the attitudes used in TPB. The construct of perceived behavioural control (PBC) reflects the individual's experience and perceived obstacles. The greater the PBC, the more likely the cybersecurity protective behaviour against phishing. PBC can be measured in terms of facilitating conditions. The facilitating conditions in this study refer to facilities needed to ensure that employees engage in the cybersecurity protective behaviour against phishing required of them by their organisations (Humaidi et al., 2018).

Again, in this study, the TPB construct of behaviour is similar to PMT's construct of protection motivation. Hence TPB is acknowledged and recognised as contributing to the construct of cybersecurity protective behaviour against phishing.

2.3.3 Technology-Organisation-Environment Framework

Technology-Organisation-Environment Framework is adopted in this study due to its organisation-centric nature of application. According to the technology-organisation-environment framework, a process by which an organisation adopts and implements technological innovation is influenced by the technological context, organisational context, and environmental context (Depietro et al., 1990). The technological context includes internal and external technologies that are relevant to the organisation. The organisational context refers to the characteristics and resources of the organisation including the cybersecurity culture, cybersecurity policies, and working arrangements (remote working, hybrid working). The environmental (internal and external) context may include factors such as the regulatory environment in which the organisation operates.

In this study, the concepts of cybersecurity awareness, the extent of remote working, and facilitating conditions are organisational factors. The perception of government cyber laws enforcement is regarded as an external environmental factor. PMT, TPB, and TOE have been discussed to predict a desired cybersecurity protective behaviour against phishing. Below are some concepts discovered from the literature review that could influence cybersecurity protective behaviour against phishing in South African organisations.

2.4 Factors that Influence Cybersecurity Protective Behaviour against Phishing

Information systems journals that are peer-reviewed were used to identify factors that influence cybersecurity protective behaviour against phishing in South Africa. The journal period was mostly between 2018 to 2023. Notable journals that were used include but are not limited to IEEE, Computers and Security, Computers in Human Behaviour and MIS Quarterly (Management Information Systems). Furthermore, conference proceedings and vendor surveys supplemented the journals. Keyword searches that were used included “phishing”, “phishing behaviour”, and “cybersecurity”.

2.4.1 Cybersecurity Protective Behaviour against Phishing

User behaviour is based on the notion that human conduct leaves behind detectable patterns, and user behaviour analysis (Mihailescu et al., 2023). In addition, by adopting user behaviour analysis, organizations can switch from a reactive to a proactive cybersecurity approach.

Phishing is a challenge to operational efficiency within organisations and it is important to adopt behaviours that foil it. It was mentioned earlier (section 2.2) that phishing is human-centric and perhaps best practices of human behaviours may be improved. It was highlighted in section 1.1 that cybersecurity protective behaviours can aid in securing information while negative cybersecurity behaviours may result in the successful execution of cyber-attacks (Almansoori et al., 2023).

As an example of cybersecurity protective behaviour against phishing, organizations may closely examine user actions, such as login timings, access patterns, file transfers, deletion of suspicious emails, email filter usage, and application usage, to compile comprehensive profiles of normal user activity (Almansoori et al., 2023; Bax et al., 2021; Mihailescu et al., 2023). This profiling may be used as a baseline to look for any deviations that would indicate attempts at unauthorized access, accounts that have been hacked, or suspicious activities such as opening emails from unknown sources linking back to cybersecurity protective behaviour against phishing. An example of a negative cybersecurity behaviour would be falling victim to a phishing attack (Almansoori et al., 2023).

2.4.2 Remote Working

During the COVID-19 pandemic, many organisations moved to remote or hybrid working environments (Klein, 2021). Remote working is also called working from home or teleworking (Mihailović et al., 2021). It is estimated that 70% of the global workforce works remotely at least once a week (Nyarko & Fong, 2023). Although remote work offers a flexible schedule and a chance for improved work-life balance, it poses cybersecurity risks (Vivekananth, 2022).

Mihailović et al. (2021) emphasise that the greatest danger regarding remote working is cybersecurity. Remote working has introduced an attractive environment for cyber attackers because some employees may be using their own devices and networks that do not exhibit the same cybersecurity properties and configuration policies as when they worked from the office (Škiljić, 2020). Cybersecurity researchers note that when working remotely, individuals or employees sometimes use information systems that are passed the end of life, do not have vendor security patches, or are not updated (Klein, 2021; Nyarko & Fong, 2023). In addition, remote working could increase the probability of risky or negative cybersecurity behaviours by individuals who do not comply with security policies and procedures and may use personal

email accounts which may result in data breaches. Phishing attacks pose a considerable challenge for organisations that allow their staff to work from home (Vrhovec et al., 2023).

Some studies on cyber security-related behaviour incorporate demographic factors (e.g., the extent of remote working), but frequently treat them differently or rarely use demographic factors to influence or predict dependent variables (Gillam and Waite, 2021). Few studies investigate demographic factors for moderating effects or variables (Gillam & Waite, 2021). Nevertheless, remote working is explored as an influential variable on the predictive variable (cybersecurity protective behaviour against phishing). There may be a negative relationship between remote working and cybersecurity protective behaviour against phishing.

H1*: Remote work has a negative influence on cybersecurity protective behaviour against phishing*

2.4.3 Cybersecurity Awareness

Researchers have emphasised awareness as an important factor in cybersecurity protective behaviour against phishing in the workplace (Alqahtani & Braun, 2021; Butler and Butler, 2018; Jansen & van Schaik, 2019; Kabanda et al., 2018). This may also apply when working from home or remotely (Abroshan et al., 2021). Cybersecurity awareness influences users' attitudes against phishing, ransomware, insider threats, third-party risks, and many others. Also, cybersecurity awareness contributes to the organisation's cybersecurity culture (Alshaik, 2020). Butler and Butler (2018) posit that the objective of cybersecurity awareness is to focus users' attention on the phishing challenge while providing them with the knowledge needed to identify and act against phishing. Mimecast found that only 23% of companies offered cybersecurity security awareness training for their staff continuously. Furthermore, employees who were offered regular training were five times more likely to notice and prevent cybersecurity threats (State & Security, 2022).

Phishing awareness can be tailored to different users (for example, technical and non-technical). It can use a variety of media (email messages, phishing simulation tools, social media, website notices, flyers, television, and radio), and gamified approaches depending on the budget available and expected return on investment (Baral & Arachchilage, 2019; Butler & Butler, 2018). For example, technical users may be made aware of and be trained to define and configure anti-phishing controls, such as email filters to remove spam emails and spoofed

emails. Technical users also need to be able to implement sender policy framework (SPF), domain keys identified mail (DKIM), domain-based message authentication, reporting and conformance (DMARC), multi-factor authentication (MFA), strong password management policies, and conditional access policies (Us, 2018). Technical users may also receive targeted awareness training to increase the company website's resilience against phishing by securely configuring it. A website may be securely configured against anti-click jacking, injection attacks (Structured Query Language injection attack, Lightweight Directory Access Protocol injection attack), cross-site scripting, cross-site request forgery, and website defacement, all of which are vulnerabilities used as a launching pad for phishing (Bakalovic, 2020; Leet, 2020). In addition, technical users may install digital certificates on their websites to ensure that traffic is encrypted, and configure web filters, and botnet filters.

For non-technical users, phishing awareness training may focus on topics such as, but not limited to, 'typosquatting' and 'cybersquatting'. 'Typosquatting' is a form of online 'cybersquatting' that results from internet users making mistakes (typos) while typing a website URL (Uniform Resource Locator) or address (Ahmad et al., 2019). Furthermore, users should be taught how to spot a real and secure website from a fake and insecure one, because cyber attackers prefer creating fake websites. The fake websites may appear legitimate, and links to these sites are attached to emails by cyber attackers; hence, unsuspecting users are encouraged to click on them and provide sensitive information (Kara & Aydos, 2022). Groups of non-technical users (such as the Board, Senior Management, Human Resources staff, and Finance staff) may be provided with targeted awareness training sessions covering topics relating to their area of work.

Another dimension to the cybersecurity awareness for phishing is information sharing or knowledge sharing amongst industry peers, other stakeholders, or a cybersecurity community of practice (Alqahtani & Braun, 2021; Leet, 2020). Cybersecurity researchers suggested that this type of collaboration is of value in managing the phishing threat landscape (Alqahtani & Braun, 2021; Leet, 2020).

Qabajeh et al. (2018) note that cybersecurity awareness training is a notable factor influencing information systems users to spot cybersecurity breaches and attempts. However, cybersecurity awareness is a continuous process, it should not stop as users may be forgetful, and this

repetition adds an extra layer of costs (Qabajeh et al., 2018). Furthermore, some companies may not invest in cybersecurity awareness against phishing as they believe it is not necessary (Bakalovic, 2020). Some researchers point out that training alone is insufficient because many users remain susceptible to phishing even after training (Kävrestad et al., 2022). Moreover, employees working remotely may not be aware of cybersecurity threats, especially phishing. Employees may make mistakes when working remotely and dealing with cybersecurity challenges such as phishing (Yang, Jing; Linkeschova, n.d.).

A need to provide cybersecurity awareness training is vital for remote employees (Hijji & Alam, 2022; Nyarko & Fong, 2023). This is because remote workers often lack awareness of the latest cybersecurity risks, especially phishing (Bispham et al., 2021; Salman, 2022). If unaware, these employees may use unsafe and insecurely configured wi-fi networks, personal emails, and weak passwords, and the routers may be launching pads for phishing attacks (Vivekananth, 2021). Therefore, there may be a relationship between cybersecurity awareness and cybersecurity protective behaviour against phishing.

H2*: Cybersecurity awareness has a positive influence on cybersecurity protective behaviour against phishing.*

2.4.4 Perceived User Self-Efficacy

Perceived user self-efficacy is defined as users' confidence in their ability to perform a cybersecurity protective behaviour against phishing (Bax et al., 2021; Sun et al., 2016). Perceived user self-efficacy has been identified as another factor that influences acceptable cybersecurity protective behaviour against phishing (Arachchilage et al., 2016; Chin & Chua, 2021; Jansen & van Schaik, 2019; Kwak et al., 2020; Ng et al., 2021; Sun et al., 2016). Perceived user self-efficacy is enhanced through cybersecurity awareness and knowledge and the relationship between the two appears to be intrinsic (Baral & Arachchilage, 2019). Perceived user self-efficacy is a well-established construct adopted from Protection Motivation Theory (PMT) and may lead to users' better phishing threat perception and avoidance.

Mou et al. (2022) hold a view that extends those of previous researchers, namely that perceived user self-efficacy has a stronger effect in personal contexts than in a workplace setting. People are regarded as the weakest link in phishing, and user self-efficacy is considered to be the most

critical aspect in taking protective measures against phishing (Alahmari et al., 2023; Baral and Arachchilage, 2019).

H3*: Perceived user self-efficacy has a positive influence on cybersecurity protective behaviour against behaviour.*

2.4.5 Facilitating Conditions

Facilitating conditions refer to resources and forms of support that are in place that make it fairly easy for an information systems user to habitually behave in a way that is cybersecurity protective against phishing (Alqahtani & Braun, 2021; Chin & Chua, 2021; McLennan & Group, 2022; Pilane et al., 2022). These resources may be cybersecurity strategies, frameworks such as sender policy framework (SPF), policies such as conditional access policies, standards, guidelines or insurance. Assistance from a computer support incident response team (CSIRT) and security operations centre (SOC) are important facilitating conditions. Technological solutions include automated anti-phishing controls such as multi-factor authentication (MFA), domain keys identified mail (DKIM), cybersecurity awareness platforms (i.e., Mimecast, KnowBe4 etc.), domain-based message authentication, reporting and conformance (DMARC) (Us, 2018). Facilitating conditions need to be aligned with the perceived cybersecurity risk of the type of organisation and can be customised to detect messages with exact-domain spoofing (that is, spoofing that targets a particular group of organisations or sectors).

It is unlikely that employees working remotely will have computers configured as securely as in the office premises (Škiljić, 2020). They might use their own devices, normally called Bring Your Own Device (BYOD) and their own wi-fi networks which may not be secure (Škiljić, 2020).

H4a: *Facilitating conditions have a positive influence on cybersecurity protective behaviour against phishing.*

Employees of organisations who are offered regular cybersecurity training (facilitating condition) were five times more likely to notice and prevent cybersecurity threats, increasing awareness which as discussed in section 2.3.3 bolsters perceived user self-efficacy, and finally improving cybersecurity protective behaviour against phishing (Baral & Arachchilage, 2019; State & Security, 2022).

***H4b**: Facilitating conditions positively moderate the influence of perceived user self-efficacy on cybersecurity protective behaviour against phishing.*

Png et al. (2009) highlighted that facilitating conditions effect end-user precautions (awareness) against cybersecurity attacks (phishing). Facilitating conditions such as security training programmes, rewards (although rewards do not produce a required behaviour all the time), cybersecurity collaboration and information sharing, and information technology skills (Alahmari et al., 2023; Bakalovic, 2020; Leet, 2020; Png et al., 2009)

***H4c:** Facilitating conditions have a positive influence on cybersecurity awareness.*

A facilitating condition through regular training on cybersecurity phishing makes users aware five times more to notice and prevent cyber-attacks, increasing phishing awareness, and bolstering perceived user self-efficacy (Alahmari et al., 2023; Baral & Arachchilage, 2019; State & Security, 2022).

***H4d:** Facilitating conditions have a positive influence on perceived user self-efficacy.*

2.4.6 Perceived Vulnerability

Perceived vulnerability is adopted from Protection Motivation Theory where it is a sub-construct of threat appraisal (Rogers, 1975). Bekkers et al. (2023) described perceived vulnerability as an estimation of the likelihood or probability of being exposed to risk, the risk being phishing in the context of this study. Furthermore, in this case, perceived vulnerability is a person's perception of their susceptibility to email phishing threats (Bax et al., 2021). To engage in a cybersecurity protective behaviour against phishing, individuals need to believe that they are at risk and perceive such risks as serious (Alahmari et al., 2023; Bekkers et al., 2023).

Cybercriminals use phishing ploys, such as fear appeals, to trick employees into revealing sensitive information (see section 2.2) such as user credentials (Škiljić, 2020). Cybersecurity vulnerabilities and risks often affect individuals and organisations negatively (Almansoori et al., 2023; Bodsberg et al., 2021).

The prior experience of individuals and their perceived knowledge regarding phishing threats can make them less susceptible to phishing attacks; conversely, lack of experience may make

individuals more susceptible. Furthermore, experience and perceived knowledge may empower individuals. This enables them to identify vulnerabilities, evaluate them, and choose an action which they are confident will protect them (De Kimpe et al., 2022; Farkhondeh et al., 2020).

***H5a**: Perceived vulnerability has an influence on cybersecurity protective behaviour against phishing.*

There is a close relationship between vulnerability perception and user self-efficacy (Bekkers et al., 2023; Mou et al., 2022). Hence, initially, employees need to perceive the vulnerability (risk) and assess if they are capable of handling (self-efficacy) the risk (Bekker et al., 2023). Only after that can they take action that may thwart the threat (Bekker et al., 2023). Another aspect of perceived vulnerability is that people tend to be optimists (a term known as optimism bias); they are inclined to think that a negative event (phishing attack) is unlikely to happen to them, but that a positive event will occur (Lei et al., 2023). When an employee assesses vulnerability to phishing as high and believes the consequence of being phished is serious, phishing efficacy will increase and will affect the subsequent intention to engage in cybersecurity protective behaviour against phishing attacks (Lei et al., 2023). There may be a relationship between threat appraisals and coping appraisals (e.g., perceived vulnerability and user self-efficacy), although little literature was found that makes this claim. However, in health studies, this was established by Chen and Jackson (2019). Despite their actual limited or no knowledge of phishing, employees of most organisations it has been suggested that they assume that they have the knowledge to manage phishing attacks (Farkhondeh et al., 2020).

***H5b**: Perceived vulnerability has a negative influence on perceived user self-efficacy.*

2.4.7 Perceived Severity

Perceived severity is an estimation of the severity of the possible consequences of exposure to phishing (Alahmari et al., 2023; Bekkers et al., 2023). Alternatively, the perception of the gravity of the effects of succumbing to an email phishing threat is known as perceived severity (Bax et al., 2021). Perceived severity has an intrinsic relationship with perceived vulnerability in the sense that individuals need to be convinced first that they are at risk, perceive the risk (phishing) as significant and then act out a cybersecurity protective behaviour against phishing (Almansoori et al., 2023; Bekkers et al., 2023). Perceived severity is stronger in a personal context than in a workplace setting (Mou et al., 2022).

***H6a**: Perceived severity has an influence on cybersecurity protective behaviour against phishing.*

As noted earlier, Farkhondeht et al. (2020) concluded that individuals' phishing prior experiences may make them less susceptible to phishing attacks. This may be because they can assess phishing attacks' severity based on their own experience and this allows them to behave confidently and counter the threat with increased efficacy. Therefore, the user's perception of this severity affects their evaluation of the extent to which their behaviour can minimize the phishing risk (Bekker et al., 2023; De Kimpe et al., 2022; Farkhondeht et al., 2020). As noted above, many employees are optimists and this influences their perceived severity assessment and therefore their assessment of response efficacy (Lei et al., 2023). When an employee assesses the level of phishing severity to be high and believes the consequence of being phished is serious, fear will increase and this will affect the subsequent intention to engage in protective measures against phishing attacks (Chen and Jackson, 2019; Lei et al., 2023). Despite their lack of expertise regarding various security threats like phishing, employees frequently believe that they can safeguard their devices from cybercriminals (Farkhondeh et al., 2020).

***H6b**: Perceived severity has an influence on response efficacy.*

2.4.8 Response Efficacy

An evaluation of the extent to which a behaviour contributes to minimizing the phishing risk is called response efficacy (Bekkers et al., 2023). Bax et al. (2021) describe response efficacy as the extent of an individual's conviction or confidence that a specific course of action will be successful in fending off a cybersecurity threat. In this study, that course of action is cybersecurity protective behaviour against phishing since there may be a positive effect between response efficacy and cybersecurity protective behaviour against phishing. However, although response efficacy has been found to have a strong effect in some workplace settings, this can differ in different contexts (Bax et al., 2021; Bekkers et al., 2023; Mou et al., 2022; Rogers, 1975). Although response efficacy may contribute to cybersecurity protective behaviour against phishing, it may not be significant in different contextual settings depending on their nature, scale, and complexity (Bekkers et al., 2023).

***H7**: Response efficacy has a positive on influence cybersecurity protective behaviour against phishing.*

2.4.9 Response Costs

Response costs are the contributions, in terms of money, time and effort, expended when taking preventative measures, such as cybersecurity protective behaviour against phishing (Bax et al., 2021; Bekkers et al., 2023; Mou et al., 2022; Rogers, 1975). Individuals need to perceive a behaviour intended to reduce the risk of phishing as being cost-efficient and effective. Hence, the benefits of performing a cybersecurity protective behaviour against phishing should be perceived as outweighing the costs of performing the cybersecurity protective behaviour against phishing. In this study, the preventative measure or action is cybersecurity protective behaviour against phishing. There may be a positive and direct effect between response costs and cybersecurity protective behaviour against phishing. Furthermore, Mou et al. (2022) argued that response costs may influence behaviour in the workplace setting including work from home that is purely personal context. This is in line with this study.

An example of response costs is the case lost by the ENSAfrica law firm. What happened was the potential home buyer paid money to an account after a cybercriminal who used phishing, altered the account number into which the home buyer was supposed to pay money (Chamber, 2023). Due diligence failures by company employees resulted in lawsuits, an example of employees avoiding taking email security seriously as they were not anticipating the costs of failure to do so. The employees, therefore, thought that the cost of due diligence outweighed the penalties. Another example was the administrative fine of five million rands which was issued to the Department of Justice and Constitutional Development (DoJCD) for contravening the Protection of Personal Information Act (Information Regulator, 2023). The Information Regulator had advised DoJCD to renew licenses for its antivirus, security information and event management (SIEM), and intrusion detection system, and submit proof to the Information Regulator within 31 days. However, DoJCD failed to comply with the Information Regulator, presumably because they thought it was too difficult, time-consuming or expensive (that is a high response cost). This estimate that response cost will be too high may apply to South African organisations that do not implement controls to manage cybersecurity protective behaviour against phishing. Lack of due diligence by DoJCD by employees resulted in a legal fine (financial risk) of five million rands. This could also tarnish the reputation of DoJCD.

H8*: Response costs have a positive influence on cybersecurity protective behaviour against phishing.*

2.4.10 Perception of Government Cyber Laws Enforcement.

Some countries in Africa, including South Africa suffer from difficulties in implementing cybersecurity-related laws, particularly in monitoring whether organisations are adhering to the law. Mcanyana et al. (2020) suggested that South Africa had poor cybersecurity-related legislation. However, South Africa has enacted the following cybersecurity-related laws (see Table 1).

Table 1: South African Government Cyber-Related Laws

Law	Source
Cybercrimes Act 19 of 2020	Parliament of South Africa (2023)
Critical Infrastructure Protection Act 8 of 2019	Parliament of South Africa (2023)
Protection of Personal Information Act 4 of 2013	Parliament of South Africa (2023)
Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002	Parliament of South Africa (2023)
Electronic Communications Security Pty Ltd Act 68	Parliament of South Africa (2023)
Electronic Communications and Transactions Act 25 of 2002	Parliament of South Africa (2023)

Chin and Chua (2021) are of the view that governments' effectiveness in implementing cyber laws will be positively related to how employees evaluate their organisations' cybersecurity postures. Individuals who recognise the financial consequences, reputational image, legal and compliance risks, and business continuity risks that come from phishing may consider the costs to be justified and act in a manner that manages phishing challenges. As an example, a violation of the Protection of Personal Information may carry a fine of up to R10 million and jail time depending on the severity of the offence.

In addition to the cyber-related laws discussed above, there is a.za namespace which is managed and regulated by the Domain Name Authority of South Africa (ZADNA) and may be of

assistance if South African organisations' domains are misused for phishing attacks. On its website, ZADNA's mandate is to *"regulate and license registries"*, *"license and regulate registrars for respective registries"*, and *"comply with international best practices in administration and management of the .ZA namespace"* (ZADNA, 2023). It appears that ZADNA's mandate is limited to the .za namespace only, but some South African organisations' domain names may not be under .za. It appears that ZADNA may be of assistance in the event whereby the South African organisations' domain is intentionally misused through 'typosquatting' and 'cybersquatting' for phishing attack purposes.

Also, there is an organisation (Internet Service Providers' Association) that is authorised to take down content from the internet relating to South African organisations if it is proven that the information was shared without authorisation from the organisation. This may improve cybersecurity protective behaviour against phishing (Internet Service Providers' Association, 2023).

To augment its efforts against cybercrime, South Africa is a signatory to the Council of Europe's Budapest Convention on cybercrime (Belli, 2021). Cybercrime, including phishing attacks, is generally transnational or borderless and this treaty strengthens collaborative efforts between member countries and signatories to exchange information to resolve cybercrimes. Phishing attacks cannot be addressed in isolation. The police recorded crime statistics (fourth quarter 2022/2023 report) did not indicate any individual types of cybercrimes such as phishing (South African Police Service, 2022). Furthermore, this study could not establish which reported crimes were computer-dependent and which ones were computer-assisted as envisaged by the Budapest Convention on cybercrime (Šupa et al., 2023).

The role of the government in adding a layer of cybersecurity protective behaviour against phishing cannot be overemphasised. This is regarded as an external environmental factor in which South African organisations operate and is from the Technology-Organisation-Environment framework (see Section 2.3.3).

***H9a**: Enforcement of government cybersecurity laws has a positive influence on cybersecurity protective behaviour against phishing.*

Hypothesis H9b below should be read in conjunction with section 2.4.8.

H9b *Enforcement of government cybersecurity laws has a positive influence on response costs.*

2.5 Conceptual Framework and Hypotheses

The study proposes the model below (Figure 3) with independent variables (facilitating conditions, cybersecurity awareness, perceived user self-efficacy, response efficacy, response costs, perceived severity, perceived vulnerability, and training, government cyber laws enforcement). The dependent variable is cybersecurity protective behaviour against phishing. Table 2 states each hypothesis and lists the major authors supporting the hypothesis.

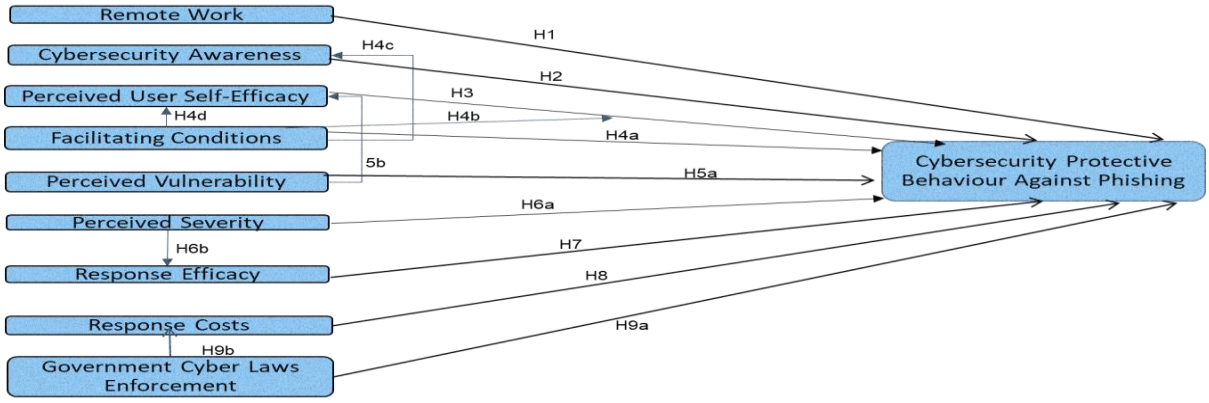

Figure 3: Conceptual Framework for Cybersecurity Protective Behaviour against Phishing in South Africa

Table 2: Hypotheses and their Descriptions

Hypothesis	Supporting literature
H1 Remote work has a negative influence on cybersecurity protective behaviour against phishing.	Remote working impacts and affects cybersecurity protective behaviour against phishing (Klein, 2021; Mihailović et al., 2021; Mou et al., 2022; Nyarko & Fong, 2023; Vivekananth, 2022; Škiljić, 2020).
H2 Cybersecurity awareness has a positive influence on cybersecurity protective behaviour against phishing.	Cybersecurity awareness influences cybersecurity protective behaviour against phishing when (Alshaik, 2021; Hijji & Alam, 2022; Vivekananth, 2021).

Hypothesis	Supporting literature
H3 Perceived user self-efficacy has a positive influence on cybersecurity protective behaviour against behaviour.	Perceived user self-efficacy may be a strong concept that may influence users to act against phishing by performing cybersecurity protective actions when working remotely (Almansoori et al., 2023; Arachchilage et al., 2016; Azjen, 1991; Bax et al., 2021; Chin and Chua, 2021; Jansen and van Schaik, 2019; Kwak et al., 2020; Ng et al., 2021; Rogers, 1975; Škiljić, 2020; Sun et al., 2016).
H4a Facilitating conditions have a positive influence on cybersecurity protective behaviour against phishing.	Facilitating conditions influence cybersecurity protective behaviour against phishing emails at work (Alqahtani and Braun, 2021; Azjen, 1991; Chin and Chua, 2021; McLennan and Group, 2022).
H4b Facilitating conditions positively moderate the influence of perceived user self-efficacy on cybersecurity protective behaviour against phishing.	Facilitating conditions appear to moderate the impact of user self-efficacy on cybersecurity protective behaviour against phishing (Alqahtani and Braun, 2021; Azjen, 1991; Chin and Chua, 2021; De Kimpe at al., 2022; McLennan and Group, 2022).
H4c Facilitating conditions have a positive influence on cybersecurity awareness.	Cybersecurity resources influence cybersecurity awareness (Abroshan et al., 2021; Alqahtani and Braun, 2021; Azjen, 1976; Bispham et al., 2021; Butler and Butler, 2018; Hijji and Alam, 2022; Jansen & van Schaik, 2019; Kabanda et al., 2018; Nyarko & Fong, 2023; Qabajeh et al., 2018).
H4d Facilitating conditions have a positive influence on perceived user self-efficacy.	Facilitating conditions impact perceived user self-efficacy (Alshaik, 2021; Chin and Chua, 2021; De Kimpe et al., 2022; Hijji & Alam, 2022; Vivekananth, 2021).
H5a Perceived vulnerability has an influence on cybersecurity protective behaviour against phishing.	Bax et al. (2021) and Almansoori et al. (2023) claim that perceived vulnerability has a measurable relationship with cybersecurity protective behaviour against phishing attacks.
H5b Perceived vulnerability has a negative influence on perceived user self-efficacy.	Prior user experience or lack of it of phishing threats anchor individuals to perceive vulnerabilities so as not to be exploitable, they then evaluate vulnerabilities and choose an action or behaviour which they believe will make them not to be exploited due to their efficacy (Almansoori et al., 2023; Bekkers et al., 2023; Chen and Jackson, 2019; De Kimpe et al., 2022; Farkhondeht et al., 2023; Lei et al., 2023).

Hypothesis	Supporting literature
H6a Perceived severity has an influence on cybersecurity protective behaviour against phishing.	Perceived severity has a measurable relationship with cybersecurity protective behaviour against phishing attacks (Almansoori et al., 2023; Bax et al., 2021; Chin and Chua, 2021; Rogers, 1975).
H6b: Perceived severity has an influence on response efficacy.	Users' experience or lack of it enables them to perceive phishing attacks' severity which then influences their ability to behave confidently (efficacy) against it. Therefore, after users perceive this severity, they evaluate the extent to which their behaviour can contribute to minimizing the phishing risk (Bekkers et al., 2023; Chen and Jackson, 2019; De Kimpe et al., 2022; Farkhondeht et al., 2023; Lei et al., 2023).
H7 Response efficacy has a positive influence on cybersecurity protective behaviour against phishing.	Response efficacy has a positive measurable relationship with cybersecurity protective behaviour against phishing emails (Almansoori et al., 2023; Bax et al., 2021; Bekkers et al., 2023; Mou et al., 2022, Rogers, 1975).
H8 Response costs have a positive influence on cybersecurity protective behaviour against phishing.	Response cost has a positive measurable relationship with cybersecurity protective behaviour against phishing emails (Bax et al., 2021; Bekkers et al., 2023; Mou et al., 2022; Rogers, 1975).
H9a Enforcement of government cybersecurity laws have a positive influence on cybersecurity protective behaviour against behaviour.	Perceptions of individuals within the organisation regarding the enforcement of government cybersecurity laws influence cybersecurity protective behaviour against phishing (Buckley et al., 2023; Chin and Chua, 2021; Dlamini and Mbambo; 2019; Interpol, 2021; Mcanyana et al., 2020).
H9b Enforcement of government cybersecurity laws has a positive influence on response costs.	Employees assess the consequences of compliance with government cyber laws versus how they respond in their workplaces (Buckley et al., 2023; Chin and Chua, 2021; Dlamini and Mbambo; 2019; Interpol, 2021; Mcanyana et al., 2020)

2.6 Summary of Chapter

The literature review discussed factors that influence cybersecurity protective behaviour against phishing. The factors of remote working, facilitating conditions, cybersecurity awareness, perceived vulnerability, perceived severity, perceived user self-efficacy, response efficacy, response costs, and perceptions of government cyber laws enforcement may influence

cybersecurity protective behaviour against phishing in South African organisations. A summary of authors who identified these factors as influencing cybersecurity protective behaviour against phishing is given in Table 3.

Table 3: Summary of Factors Influencing Cybersecurity Protective Behaviour against Phishing

Factor	Author
Remote Working	Klein (2021); Nyarko and Fong (2023); Škiljić (2020); Vivekananda (2022)
Cybersecurity awareness	Al-Qahtani and Cresci (2022); Butler and Butler (2018); Jansen and van Schaik (2019); Kabanda et al. (2018); Pilane et al. (2022); Qabajeh et al. (2018)
Perceived User self-efficacy	Arachchilage et al. (2016); Bax et al. (2021); Chin and Chua (2021); Jansen and van Schaik (2019); Kwak et al. (2020); Ng et al. (2021); Sun et al. (2016); Triandis (1980).
Facilitating Conditions	Alqahtani and Braun (2021); Azjen (1991); Chin and Chua, 2021; McLennan & Group (2022); Triandis (1980)
Perceived Vulnerability	Bax et al. (2021); Chin and Chua (20 Mou et al. (2022); Rogers (1975)
Perceived Severity	Bax et al. (2021); Chin and Chua (2021); Mou et al. (2022); Rogers (1975)
Response Efficacy	Bax et al. (2021); Bekkers et al. (2023); Mou et al., 2022; Rogers (1975)
Response Costs	Bax et al. (2021); Bekkers et al. (2023); Mou et al., 2022; Rogers (1975)
Perceptions of Government Cybersecurity Laws Enforcement	Chin and Chua (2021); Dlamini and Mbambo (2019); Eboibi (2020); Mcanyana (2020)

The factors were adapted from the literature review and theories, including the Theory of Planned Behaviour (TPB), the Protection Motivation Theory (PMT), and the Technology-Organisation-Environment framework (TOE). However, PMT was the basis that guided this research study to develop a conceptual framework for factors influencing cybersecurity protective behaviour against phishing in South African organisations.

The hypotheses were formulated using literature and will be assessed for confirmation (support) or rejection (refute). There is limited research literature relating to the study of factors influencing cybersecurity protective behaviour against phishing in the workplace within South African organisations' context. Hence, it is anticipated that the contribution provided by the study will enhance the existing body of knowledge to improve cybersecurity protective behaviour against phishing in the workplace context of South African organisations post-COVID-19 pandemic.

3. Research Methodology

3.1 Introduction

This chapter details the steps that were carried out to answer the research question. They include the research philosophy, research purpose, research approach, research strategy, timeframes, ethics, risks, and budget.

3.2 Research Philosophy

3.2.1 Ontology

The ontological stance reflects the view that information and ideas about cybersecurity protective behaviour against phishing can be obtained through observation and learning and is not based on the personal beliefs or convictions of the researchers. Thus, the ontological stance for this research study is objective as this study was done independent of the researcher's views through a questionnaire survey. (Bhattacherjee, 2012; Ryan, 2018, Saunders et al., 2009). This study is based on objectivity, and it is expected to yield reliable facts. The data may be analysed and extrapolated to the population of interest (Saunders et al., 2009).

3.2.2 Epistemology

This study adopts the view of observable social reality and accepts that the impacts identified may not necessarily be conclusive (Saunders et al, 2009). That is, only observable phenomena may provide credible information or facts. This study held the view that experienced events should be the subject of scientific enquiry where independent and dependent variables are quantified and conclusions are drawn from the sample population (Saunders et al., 2009). The focus is on causality and law-like generalisations, reducing phenomena to the simplest elements (Saunders et al., 2009). Hence the researcher's epistemological stance was positivistic.

3.3 Research purpose

The research purpose can be exploratory, descriptive, explanatory or a combination of these (Saunders et al., 2009). The study's knowledge claim is that it makes an explanatory contribution as the researcher explains the concept of cybersecurity protective behaviour against phishing (the phenomenon), having developed the conceptual framework using relations between independent variables and the dependent variable.

3.4 Research approach

This research is based on current literature, guided by Protection Motivation Theory. Following that, a conceptual framework comprising constructs (factors), sub-constructs, and hypotheses was established, as shown in Figure 3, and discussed in Table 2. Hypotheses were examined to see if they could be confirmed (accepted) or disputed (Bhattacherjee, 2012; Ryan, 2018; Saunders et al., 2012). As a result, the research takes a deductive approach because the testing of hypotheses was centred around an established theory (Bhattacherjee, 2012; Saunders et al., 2012).

3.5 Research Strategy

Questionnaire surveys collected data from participants and quantitative methodologies were applied to analyse those data (Ryan, 2018). Questionnaire surveys are commonly utilised for cross-sectional quantitative research and are convenient for participants (Saunders et al., 2009). Participants in questionnaire surveys provided a concise account of their behaviours, beliefs, opinions and situations and this can easily be converted to numerical data. Hence, a quantitative study method could be applied (Saunders et al., 2009).

3.5.1 Target Population

This study was aimed at South African employees from any formal workplace setting with internet access. However, since not all employees have access to the internet and not all use emails, it was challenging to determine how many South African employees had internet access and used emails regularly in their workplaces (that is, to accurately estimate the size of the target population). An element is a single person within the population. Everyone in the target population was subject to the same cyber laws and domestic challenges.

3.5.2 Sampling Frame and Sampling

The sampling frame is a list of all elements (in this case individual people) in the target or statistical population from which the sample size is calculated to gain an understanding of the whole population (Bhattacherjee, 2012; Saunders et al., 2012). Due to the large size of the target population, not all individuals working for the many organisations received an opportunity to be sampled in this study. Hence, sampling everyone within all organisations which were within the population was not statistically reasonable or feasible. Therefore, a non-probability

sampling method was used. Snowball sampling was used in this study. Snowball sampling is a strategy for locating desirable responders in a population when it is difficult to do so. Initial responders contribute information about later respondents for snowball (Saunders et al., 2009). The limitation of snowball sampling is that it is a challenge to reach a representative sample and generalise the analysed results to the target population (Pasikowski, 2023).

The sample size for this study was calculated based on the assumption that the sample size in multivariate research should be ten times the number of variables (Ahmad et al., 2016). Because there are ten constructs (factors) in this study, a minimum sample size of one hundred participants was required. The target population might not be projected accurately but the study adopts a 95% confidence level and a 5% margin of error or confidence interval (Bhattacherjee, 2012; Saunders et al., 2012). A probability value of less than 0.1 can be marginally supported (Li et al., 2018). The error margin for generalizing research findings or results to the population can be reduced if the sample size is larger than the minimum required and is representative (Saunders et al., 2009). To reduce bias, the non-response rate was considered. Participants who do not respond to a survey are said to be non-responsive (Bhattacherjee, 2012; Saunders et al., 2012). To maximise response rates, the questionnaire was not made to be too long, items or statements were as less ambiguous as possible, and feedback was anonymised.

3.5.3 Pilot testing strategy

The research instrument was pilot-tested with ten participants from various organisations. The pilot testing was performed to ensure that the research instrument's (the questionnaire) measurements were reliable and valid before it was sent to the sample of participants (Bhattacherjee, 2012). After pilot testing was performed, a few changes were made to the research instrument based on the responses collected. These changes related to spelling and grammatical errors and were not material to the research instrument.

3.5.4 Data Collection

Questionnaires were used as the main data collection instrument to assess the hypotheses (Bhattacherjee, 2012; Saunders 2009). This is done to obtain objectivity (the researcher is not present when the research participant provides data). An online questionnaire survey was administered through a platform called Qualtrics and connected with research participants through emails and social media channels. The questionnaire included a cover letter (see

Appendix D) and was accessed through a hyperlink. On Qualtrics, features such as forced response can be enabled before allowing a respondent to move to the next question. Participants were only allowed to complete one questionnaire. To maximise the response rate or minimise nonresponse bias, the survey was kept short and targeted to the required and necessary information from participants (Bhattacherjee, 2012). Furthermore, participants' anonymity in their responses was maintained.

3.5.5 Research Instruments

As part of the survey, participants received a questionnaire; this is a research instrument with items (individual questions) (see Appendix D, Table 13). The questionnaire collected data associated with the constructs in the conceptual model (remote working, facilitating conditions, cybersecurity awareness, perceived vulnerability, and perceived severity). The questionnaire also collected data associated with the constructs related to the theories used (perceived user self-efficacy, response efficacy, response costs, government cyber laws enforcement, and cybersecurity protective behaviour against phishing). The questionnaire survey consisted of a total of 73 items. Table 4 shows which constructs each of the items investigated together with associated research studies. In addition, the questionnaire survey had a section in which respondents provided demographic information to determine whether they were a representative sample of the target population (see Appendix D, Table 12).

Table 4: Questionnaire Survey Items

Constructs	Factors/Measures	Number of Items	Source
Remote Working Extent (Organisational Factors)	Percentage of remote work	5	
	Remote working frequency (work from home) frequency	5	Van Zoonen et al. (2021)
	The extent of remote working	5	Min (2022)
	Length of Remote Work (years)	5	Fay (2007)
	The intensity of remote work (Hours spent online per week)	5	Alheneidi et al. (2021)
Organisational Factor	Facilitating Conditions	3	Zaman et al. (2018)

Constructs	Factors/Measures	Number of Items	Source
Cybersecurity Awareness		6	Phillip et al. (2023
Threat Appraisal	Perceived Vulnerability	6	Bax et al. (2021)
	Perceived Severity	6	Bax et al. (2021)
Coping Appraisal	Perceived User Self-efficacy	6	Bax et al. (2023)
	Response Efficacy	4	Bax et al. (2021)
	Response Costs	8	Bax et al. (2021)
Environmental	Government Cyber Laws Enforcement	4	Chin and Chua (2021)
Cybersecurity Protective Behaviour Against Phishing		7	Bax et al. (2021)

3.5.6 Data Analysis

Statistics (Microsoft Excel, PLS-SEM tools), tables, and charts were used to interpret and analyse data collected from respondents to arrive at conclusions from the findings for each research question to be answered (Bhattacherjee, 2012; Saunders, 2009). The data was tested for measurement or item reliability (composite reliability) to determine the consistency of measurement over time (Bhattacherjee, 2012; Venkatesh et al., 2013). Convergent validity was measured as average variance extraction (the amount of variance the latent construct reflected against its indicators) (Chin 1998). For discriminant validity testing of constructs, cross-loading tests, HTMT, and Fornell-Lacker criterion are commonly used and were tested (Chin, 1998; Hair et al., 2011; Fornell and Lacker 1981).

3.6 Timeframes and Project Plan

The study was cross-sectional due to a restricted time frame; it was conducted at a single point in time (Bhattacherjee, 2012; Saunders, 2009). The researcher had to adhere to timelines stipulated to conduct research for a Masters course.

3.7 Ethics

The ethics for and research instrument were approved by the University of Cape Town's Ethics in Research Committee. Participation in this research was voluntary and harmless, A consent form was signed by participants in the event they wanted to withdraw. Information collected from participants remained confidential. Furthermore, the participants' identities were not and will not be disclosed. In addition, the analysis and reporting were not fabricated. Plagiarism offences were not tolerated and would be penalised (Bhattacherjee, 2012).

3.8 Risks

Bias (convenient responses that are not necessarily true) may occur in participants' responses to questionnaires (Bhattacherjee, 2012). The bias may be mitigated by explaining to participants the importance of responding honestly. Also, the bias of the researcher's prior knowledge was guarded against by adhering to a research design that promoted objectivity. A sampling risk was taken into consideration. Sampling risk means that the target sample may not be representative of the whole target population.

3.9 Budget

No costs were incurred because the software license (Smart PLS) required to conduct the research was provided by UCT.

3.10 Summary of Chapter

This chapter discussed research philosophy whose ontological stance was objective and epistemological stance was positivistic. Furthermore, the research purpose was explanatory, and the research approach was deductive. The research strategy used an online questionnaire survey, and the time frame was cross-sectional.

4. Data Analysis

4.1 Introduction

This chapter presents results from data analysis which went through validation. Data that was analysed included demographics from survey participants. Responses from the survey questionnaire and the researcher's findings are interpreted. The data was collected using a questionnaire survey from Qualtrics was downloaded using Microsoft Excel and was imported into Smart PLS (partial least squares equation modelling) Version 4. Before that, data was cleaned through deleting and editing collected data. There were two respondents whose surveys were incomplete, meaning there was no feedback on any items. They were discarded and no missing data was found.

4.2 Demographic Profile

The demographic data results in Figure 4 indicate that most of the respondents were between the ages of 31 and 40 (60,4%), the next biggest group was respondents between the ages of 41 and 50 (20,8%). Furthermore, there was a 9.9% representation of respondents between the ages of 21 and 30 and 7,9% of respondents between the ages of 51 and 60. There were no respondents between the ages of 18 and 20 and only one respondent above the age of 60.

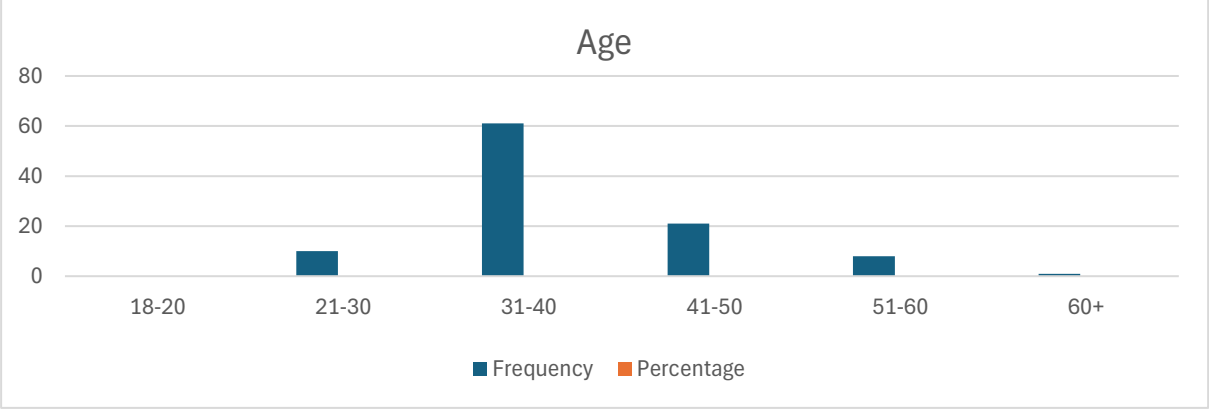

Figure 4: Age

From these results (figure 5), there were more female (58,4%) respondents than male (40,6%) respondents. However, this was a good balance in terms of the genders represented. Although not tested, some researchers highlight that gender may influence cybersecurity protective

behaviour against phishing (Gillam and White, 2021). In addition, there was only one respondent in the non-binary gender group.

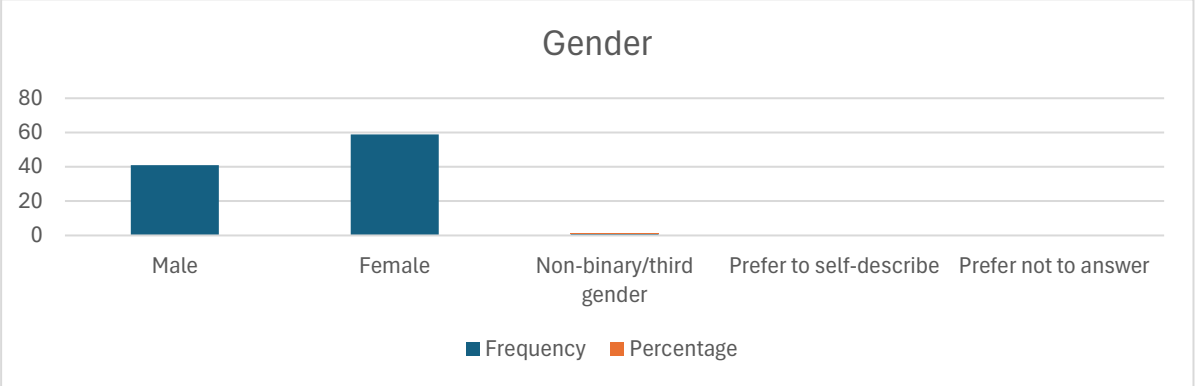

Figure 5: Gender

The results (figure 6) indicate that the majority of respondents had obtained a Postgraduate-Diploma and Honours (39%), the next largest group had Bachelor's Degree or Bachelor of Technology qualifications (21,8%), a smaller group were Master's degree holders (17,8%), Certificate and Diploma holders (17%), Doctoral degree holders (4%) and one respondent at High school level.

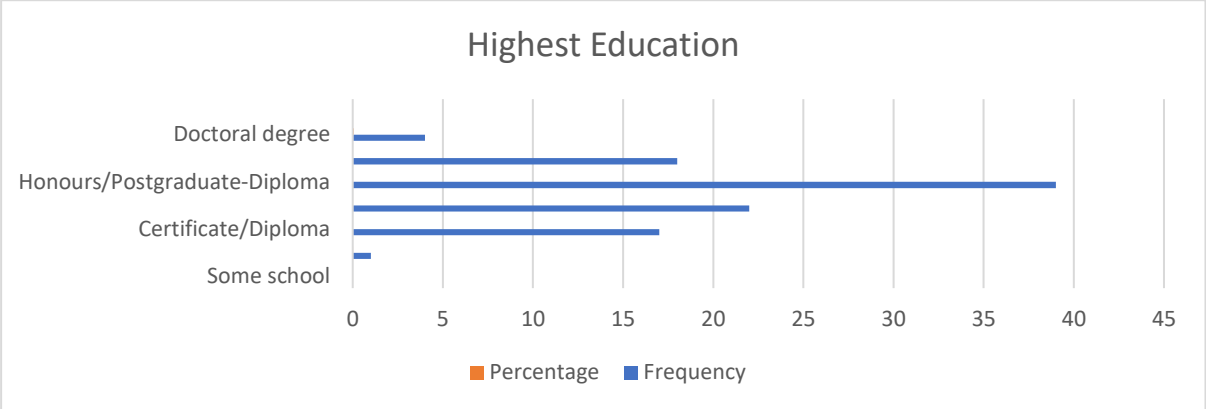

Figure 6: Highest Education

A high number of respondents (see Figure 7) indicated that they were employed in this descending order from Private companies (40%), Government (35,8%), State-Owned Companies (12,5%), and Public Companies (10,8%). Figure 7 shows that most of the respondents worked in industries from Financial and Insurance Activities (32,2%), followed by Information and Communication (17,8%), Other Service Activities (14,4%), Public

Administration and Defence (11%), Education (5%), Manufacturing (4,24%), and Professional, Scientific and Technical services (3,4%). Two industries with a small number of people participating in this research were Agriculture, Forestry and Fishing (2,54%) and Administrative and Support Service Activities (2,54%), followed by Retail (1,7%), Construction and Transportation (0.85%) and Storage industries (0.85%). KPMG (2022) reported that the top targeted industries in the Southern African region were financial services, energy and natural resources, and manufacturing.

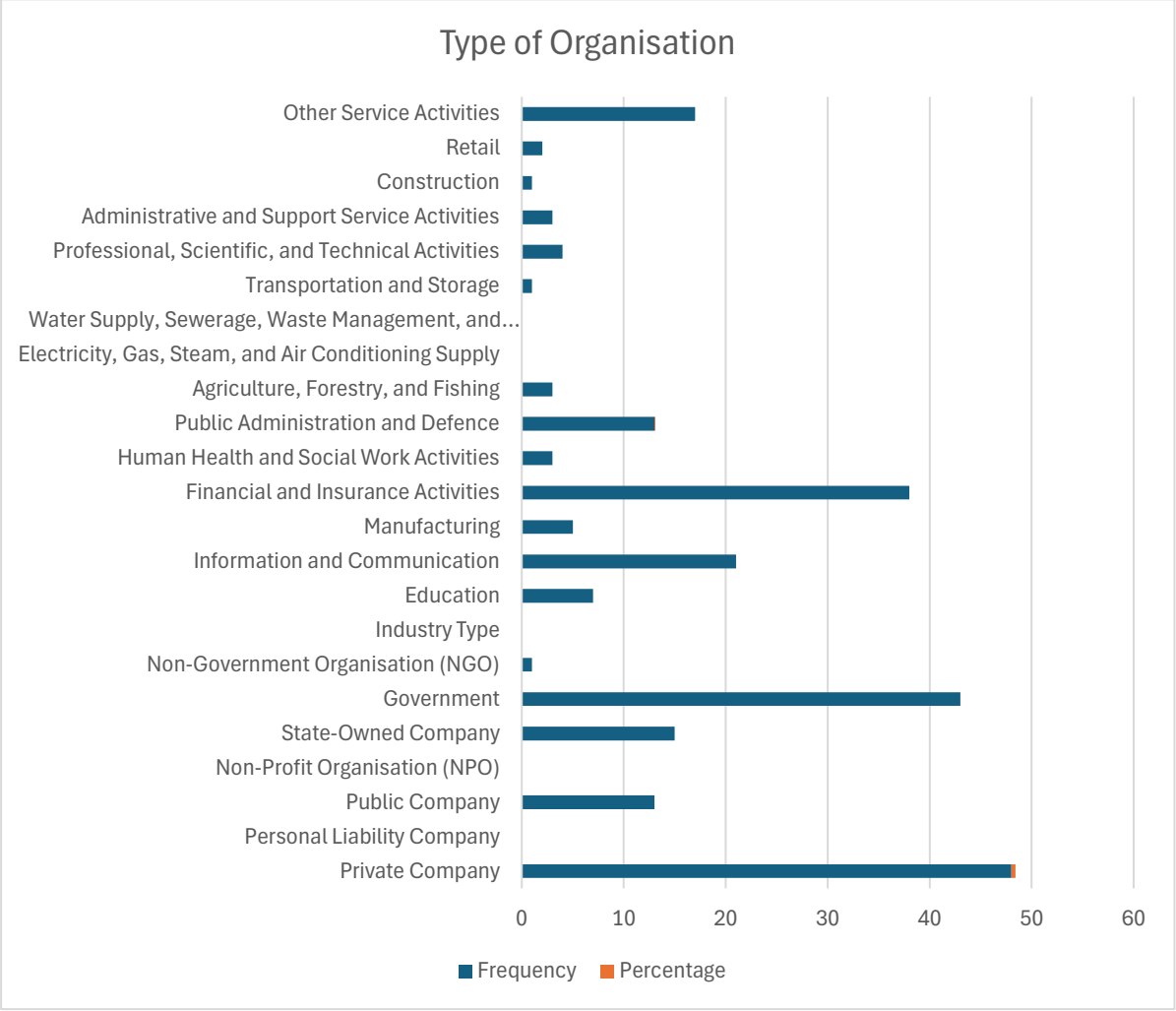

Figure 7: Type of Organisation

It was noted from these results (figure 8) that most respondents worked for large organisations (84,2%), with far fewer in medium-sized organisations (10,8%), small organisations (3,3%), and micro-size organisations (1,7%).

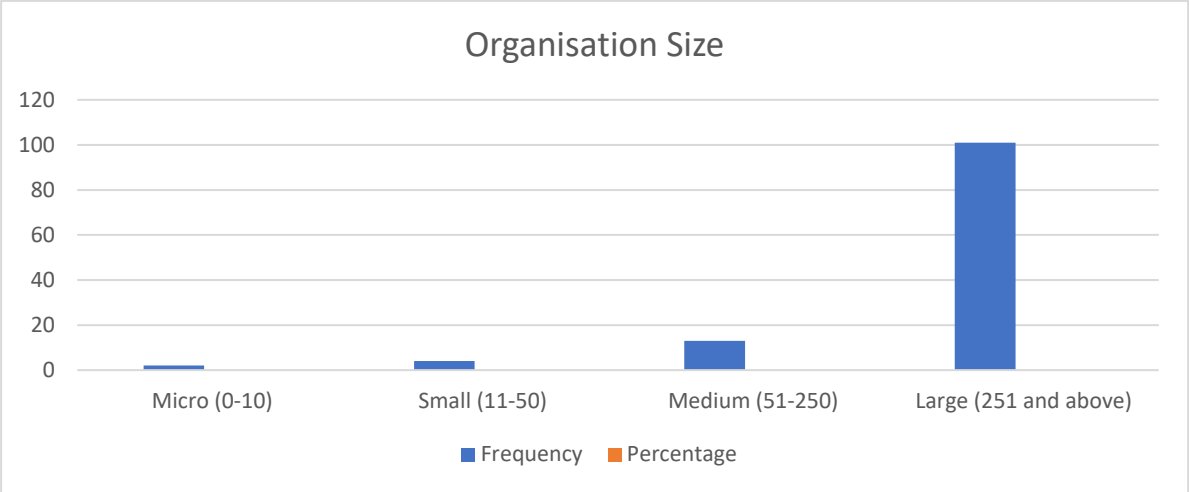

Figure 8: Organisation Size

Furthermore, the occupational levels for respondents were mainly those describing themselves as Professionally Qualified/ Experienced Specialist/ Middle Management at 42,6% followed by Skilled Technical and Academically qualified/ Junior Management/Supervisors/ Foremen /Superintendents at 34,7%, then Senior Management (10,9%), Semi-Skilled (9,9%), and Top Management or Executive (1.9%, which is approximately 2%).

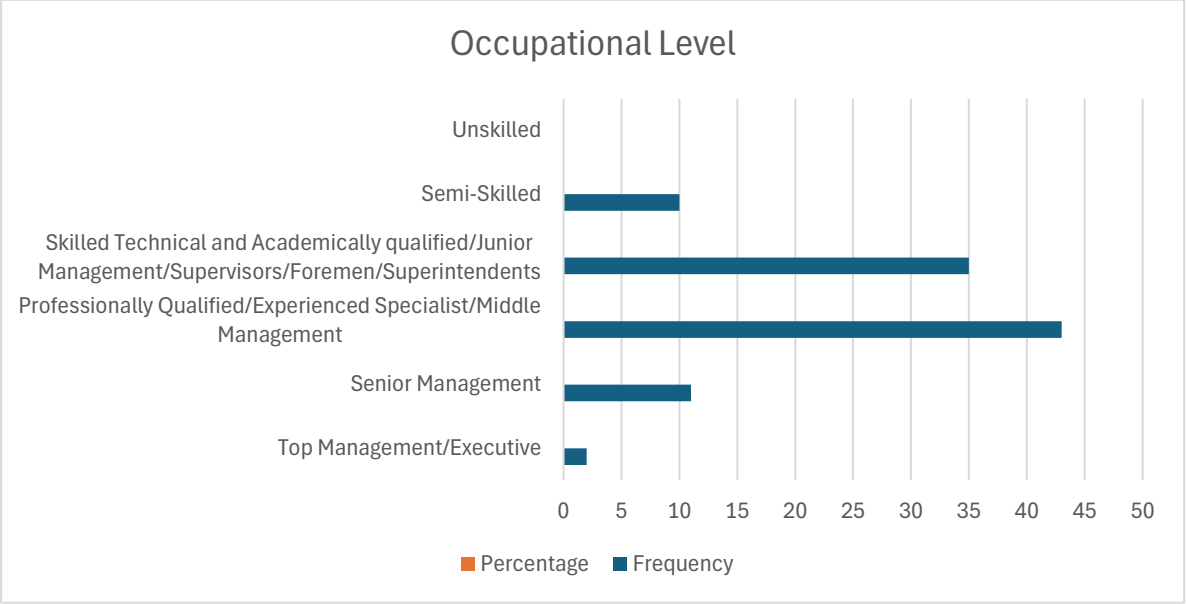

Figure 9: Occupational Level

It was observed (in Figure 10) that most respondents had been working (possibly in different organisations) for more than ten years (30.7%), followed by those who have been working

between two to five years (24,8%), then zero to two years (23,8%), and finally between five to ten years (20,8%), and more than ten years (3,7%). Some researchers argue that new employees may be more susceptible to phishing attacks (Beu et al., 2023).

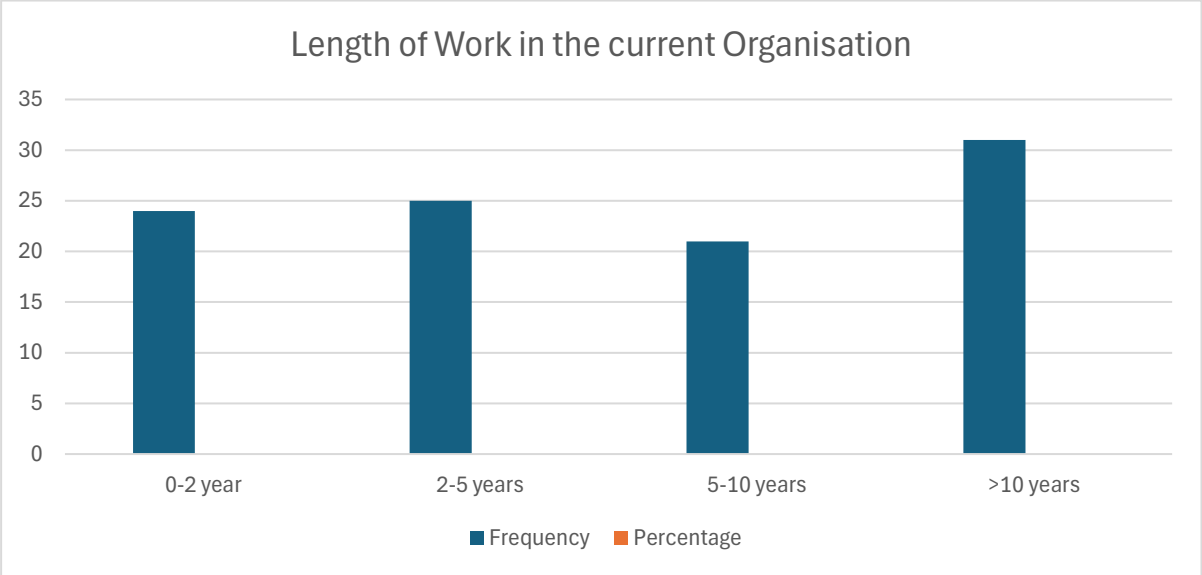

Figure 10: Length of Work in the Current Organisation

Most respondents indicated that they had internet access for work in their organisations for more than ten years (89,1%). Internet access is needed for a phishing attack to be established because phishing is Internet-dependent.

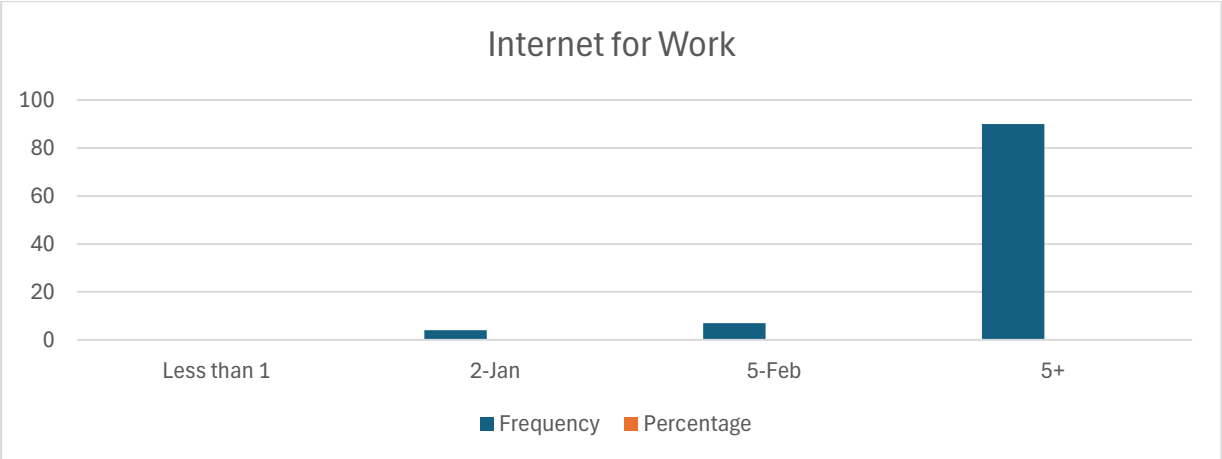

Figure 11: Internet for Work

4.3 Descriptive Statistics

Table 5: Descriptive Statistics

Name	Mean	Median	Min	Max	Standard deviation	Excess kurtosis	Skewness
Consent	1	1	1	1	0	NaN	NaN
FC1	3.89	4	1	5	1.1	0.39	-0.96
FC2	4	4	1	5	1.01	1.48	-1.24
FC3	3.91	4	1	5	1	0.79	-0.98
CAW1	4.29	4	1	5	0.89	4.63	-1.91
CAW2	4.36	4	1	5	0.81	5.62	-1.97
CAW3	4.43	4	1	5	0.6	2.38	-1.02
PV1	3.15	3	1	5	1.18	-1.05	-0.27
PV2	3.2	3	1	5	1.1	-0.87	-0.33
PV3	2.68	3	1	5	0.98	-0.29	0.36
PV4	2.76	3	1	5	1.07	-0.94	0.12
PV5	2.88	3	1	5	1.14	-1.19	0.096
PV6	2.9	3	1	5	1.14	-1.16	0.061
PS1	4.35	4	1	5	0.73	4.35	-1.58
PS2	4.35	4	1	5	0.77	3.62	-1.59
PS3	4.58	5	1	5	0.6	1.95	-1.34
PS4	4.58	5	1.	5	0.7	6.74	-2.24
PS5	4.08	4	1	5	0.89	0.55	-0.88
PS6	3.7	4	1	5	1.03	-0.79	-0.39
PUSE1	3.96	4	1	5	0.89	2.16	-1.29
PUSE2	4.06	4	1	5	0.79	3.3	-1.35
PUSE3	3.94	4	1	5	0.81	2.29	-1.13

Name	Mean	Median	Min	Max	Standard deviation	Excess kurtosis	Skewness
PUSE4	3.84	4	1	5	0.83	0.95	-0.86
PUSE5	3.96	4	1	5	0.77	2.04	-1.05
PUSE6	3.84	4	1	5	0.89	1.4	-1.03
RE1	4.32	4	1	5	0.75	5.6	-1.79
RE2	4.15	4	1	5	0.89	2.74	-1.45
RE3	4.06	4	1	5	0.8	1.65	-1
RE4	4.28	4	1	5	0.7	1.21	-0.89
RC1	2.38	2	1	5	1.18	-0.35	0.76
RC2	2.33	2	1	5	1.23	-0.51	0.79
RC3	2.05	2	1	5	1.03	0.45	1.01
RC4	2.08	2	1	5	1.04	-0.076	0.83
RC5	2.2	2	1	5	1.11	0.004	0.86
RC6	1.86	2	1	5	0.99	2.21	1.51
RC7	2.52	2	1	5	1.1	-0.76	0.44
RC8	2.4	2	1	5	1.14	-0.58	0.65
CPBAP1	3.25	3	1	5	1.11	-0.98	-0.14
CPBAP2	3.52	4	1	5	1.06	-0.38	-0.61
CPBAP3	3.69	4	1	5	1.05	0.16	-0.81
CPBAP4	4.05	4	1	5	0.69	3.47	-1.13
CPBAP5	3.9	4	1	5	0.99	1.33	-1.2
CPBAP6	3.36	4	1	5	1.13	-0.85	-0.29
CPBAP7	3.77	4	1	5	1.01	-0.53	-0.58
GCL1	3.08	3	1	5	1.03	-0.54	-0.03
GCL2	2.84	3	1	5	1.03	-0.55	0.23

Name	Mean	Median	Min	Max	Standard deviation	Excess kurtosis	Skewness
GCL3	2.98	3	1	5	1	-0.57	0.14
GCL4	2.77	3	1	5	1.07	-0.55	0.32

Table 5 provides descriptive statistics including variables' means, median, minimum, and maximum Likert scale ratings, skewness, and kurtosis. These values are commonly used to test for the normality of data. Skewness and Kurtosis are used to check how data deviate from a normal distribution. Positive values of skewness signify that the distribution curve lies to the right while negative values signify that the distribution curve is skewed to the left (Blanca et al., 2013). Furthermore, positive kurtosis values indicate that the curve has a higher peak than normal while negative values highlight that is flatter than normal (Blanca et al., 2013).

4.4 Structural Equation Model

In this study, Partial Least Square-Structural Equation Modelling (PLS-SEM) was utilised to analyse the quantitative set of data that was collected from respondents of South African organisations. Iqbal et al. (2021) say that PLS-SEM assists researchers in analysing sophisticated models with different constructs (including dependent and independent variables). Also, PLS-SEM is regarded as an efficient way to analyse cause-effect relationships between latent constructs. Moreover, PLS-SEM is regarded as the most reliable method to measure direct and indirect paths because it analyses complex latent constructs (Iqbal et al., 2021).

In PLS-SEM, the constructs (factors) are called latent variables and the items that make up a questionnaire are called indicators. Hair et al. (2012) explain that PLS-SEM consists of the structural model (inner model) and the measurement model (outer model). The inner and outer models measure the relationships between independent variables and dependent variables and between latent constructs and observed indicator variables (Hair et al., 2012).

4.5 Measurement Model

The measurement model (outer model) was analysed to assess its reliability by calculating the composite reliability (CR) and average variance extraction (AVE). In addition, Cronbach Alpha

(CA) was calculated; CA is commonly used to calculate internal consistency and was utilised to measure the reliability of the items (Bhattacherjee, 2012; Saunders et al., 2012). CA and CR values should at least be 0.7 and AVE must be 0.5 to measure convergent validity as suggested by researchers (Hair et al., 2012).

For the remote work (RW) construct, four out of five subconstructs were dropped as they failed validity testing due to initial outer loadings being less than 0.4 and therefore only a single item remained that measured the length of remote work (see Table 6). Similarly, for perceived severity, two items (PS5 and PS6) were dropped as they had the lowest outer loading, and AVE (for perceived severity) needed to be at least 0.5 (see Table 6). Similarly, the cybersecurity protective behaviour against phishing items, CPBAP1 and CPBAP2, as AVE must be 0.5 or above (see Table 6). Once these items were excluded, for cybersecurity awareness (CAW), the CA, CR and AVE values were 0.8, 0.88, and 0.709 respectively; for facilitating conditions (FC), the CA, CR, and AVE were 0.91, 0.94, and 0.85; and for government cyber laws (GCL), these same three measures had values of 0.89, 0.92, and 0.8. The CA, CR, and AVE values for cybersecurity protective behaviour against phishing (CPBAP) were 0.79, 0.86, and 0.54; perceived severity (PS) values were 0.84, 0.87, and 0.58; for perceived user self-efficacy (PUSE) the corresponding values were 0.95, 0.96, and 0.79; while the values for perceived vulnerability (PV) were 0.9, 0.92, and 0.67. CA, CR, and AVE values were measured to be 0.91, 0.92, and 0.61 for response costs (RC), 0.76, 0.84, and 0.59 for response efficacy (RE). These were all found to be reliable and valid (see Table 6).

Also, all the AVE values were above 0.5 (see Table 6) for convergent validity assurance purposes, implying that latent constructs accounted for a significant number of variances in their indicators (Henseler et al., 2016; MacKenzie et al., 2011). Similarly, convergent validity determines how correlated the items of a construct are to other items of a latent construct.

Table 6: Measurement Model

Construct	Item Code	Final Loading	Outer Weights	CA	CR	AVE
Cybersecurity Awareness				0.8	0.88	0.709
	CAW1	0.858	0.4			

Construct	Item Code	Final Loading	Outer Weights	CA	CR	AVE
	CAW2	0.84	0.3			
	CAW3	0.84	0.48			
Facilitating Conditions				0.91	0.94	0.85
	FC1	0.95	0.43			
	FC2	0.89	0.29			
	FC3	0.92	0.36			
Government Cyber Laws				0.89	0.92	0.8
	GCL1	0.93	0.54			
	GCL2	0.89	0.35			
	GCL3	0.86	0.16			
	GCL4	0.84	0.067			
Cybersecurity Protective Behaviour Against Phishing				0.79	0.86	0.54
	CPBAP3	0.72	0.26			
	CPBAP4	0.73	0.24			
	CPBAP5	0.71	0.29			
	CPBAP6	0.71	0.27			
	CPBAP7	0.81	0.3			
Perceived Severity				0.84	0.87	0.58
	PS1	0.73	0.24			
	PS2	0.81	0.23			
	PS3	0.85	0.24			
	PS4	0.88	0.52			
Perceived User Self-efficacy				0.95	0.96	0.79
	PUSE1	0.9	0.19			

Construct	Item Code	Final Loading	Outer Weights	CA	CR	AVE
	PUSE2	0.91	0.18			
	PUSE3	0.94	0.2			
	PUSE4	0.85	0.16			
	PUSE5	0.9	0.18			
	PUSE6	0.81	0.21			
Perceived Vulnerability				0.9	0.92	0.67
	PV1	0.77	0.22			
	PV2	0.91	0.31			
	PV3	0.75	0.13			
	PV4	0.81	0.19			
	PV5	0.81	0.14			
	PV6	0.86	0.23			
Response Costs				0.908	0.924	0.608
	RC1	0.76	0.2			
	RC2	0.84	0.19			
	RC3	0.91	0.24			
	RC4	0.88	0.21			
	RC5	0.77	0.11			
	RC6	0.74	0.073			
	RC7	0.56	0.039			
	RC8	0.72	0.18			
Response Efficacy				0.76	0.84	0.58
	RE1	0.79	0.34			
	RE2	0.82	0.35			

Construct	Item Code	Final Loading	Outer Weights	CA	CR	AVE
	RE3	0.78	0.39			
	RE4	0.65	0.23			
Remote Work				-	-	-
	Length of Remote Work	1				
	RW - CPBAP	1	1			

Table 7: Cross Loadings

	CAW	FC	GCL	CPBAP	PS	PUSE	PV	RW	RC	RE	RW-PS	RW-PV	RW-CAW	RW-FC	RW-PUSE
CAW1	0.848	0.266	0.106	0.364	0.114	0.353	-0.288	0.060	-0.129	0.331	0.044	-0.003	0.087	-0.078	0.032
CAW2	0.835	0.145	-0.067	0.276	0.221	0.232	-0.231	-0.131	-0.204	0.317	0.070	-0.142	0.244	-0.062	0.041
CAW3	0.843	0.364	0.196	0.438	0.363	0.261	-0.084	-0.020	-0.280	0.468	0.098	-0.044	0.101	0.048	0.151
FC1	0.310	0.948	0.273	0.279	0.126	0.380	-0.116	0.067	-0.089	0.351	-0.103	-0.090	-0.028	0.077	0.164
FC2	0.223	0.891	0.323	0.191	0.055	0.269	-0.117	0.068	-0.121	0.289	-0.155	-0.072	-0.085	0.092	0.147
FC3	0.356	0.923	0.324	0.234	0.040	0.347	-0.067	0.047	-0.056	0.315	-0.035	-0.119	-0.002	0.110	0.184
GCL1	0.132	0.296	0.931	0.121	0.009	0.061	0.093	-0.082	0.123	0.180	0.048	-0.107	0.008	0.029	0.103
GCL2	0.090	0.308	0.892	0.078	-0.108	0.062	0.099	0.039	0.209	0.229	0.036	-0.125	-0.074	-0.029	0.110
GCL3	0.078	0.279	0.855	0.036	-0.083	0.043	0.097	-0.017	0.200	0.198	0.071	-0.070	-0.069	-0.039	0.069
GCL4	0.032	0.290	0.837	0.015	-0.105	0.052	0.027	-0.005	0.221	0.111	0.077	-0.052	-0.114	-0.080	0.043
LengthWk	-0.025	0.066	-0.034	-0.123	-0.006	0.098	0.013	1.000	0.060	0.070	0.084	-0.107	0.017	-0.204	-0.011
CPBAP3	0.275	0.257	0.199	0.715	0.140	0.407	-0.253	0.017	-0.140	0.364	0.044	0.152	-0.122	0.025	0.021
CPBAP4	0.374	0.084	-0.004	0.729	0.261	0.240	-0.215	0.001	-0.157	0.386	0.061	0.097	0.007	-0.042	-0.001
CPBAP5	0.306	0.132	-0.053	0.711	0.261	0.329	-0.251	-0.293	-0.098	0.361	0.105	0.005	0.076	0.219	0.157
CPBAP6	0.304	0.249	0.196	0.714	-0.042	0.305	-0.311	-0.146	-0.120	0.344	-0.151	0.031	-0.000	0.118	0.064
CPBAP7	0.368	0.229	0.037	0.810	0.101	0.428	-0.375	-0.015	-0.254	0.338	-0.100	0.082	0.065	0.089	0.107
PS1	0.284	0.086	-0.004	0.107	0.730	0.045	0.100	0.005	-0.291	0.256	0.290	0.001	0.140	-0.031	-0.047
PS2	0.294	0.044	-0.020	0.101	0.809	0.094	0.031	0.043	-0.270	0.250	0.287	0.066	0.129	-0.020	0.018
PS3	0.264	0.130	0.012	0.106	0.850	0.039	0.043	0.018	-0.316	0.262	0.226	0.069	-0.003	-0.034	-0.026
PS4	0.175	0.047	-0.088	0.231	0.876	0.126	0.021	-0.041	-0.255	0.225	0.250	0.020	0.039	-0.096	-0.011
PS5	0.005	0.047	0.136	-0.015	0.448	-0.016	0.150	-0.005	-0.046	0.185	0.175	0.091	-0.044	0.044	0.025
PUSE1	0.350	0.322	0.052	0.423	0.209	0.900	-0.237	0.053	-0.166	0.498	0.033	-0.031	0.227	0.161	0.013
PUSE2	0.373	0.381	0.038	0.401	0.232	0.909	-0.218	0.086	-0.127	0.479	0.018	-0.025	0.123	0.162	-0.014
PUSE3	0.289	0.341	0.054	0.441	0.119	0.941	-0.221	0.074	-0.139	0.512	0.017	0.007	0.069	0.159	-0.028
PUSE4	0.280	0.266	0.051	0.344	-0.019	0.850	-0.320	0.095	-0.049	0.361	-0.090	-0.030	0.217	0.148	0.002

PUSE5	0.325	0.366	0.113	0.402	0.089	0.903	-0.288	0.138	-0.156	0.548	-0.084	0.047	0.066	0.167	-0.021
PUSE6	0.189	0.269	0.035	0.455	-0.064	0.807	-0.361	0.077	-0.039	0.422	-0.060	-0.013	0.051	0.161	-0.075
PV1	-0.108	0.007	0.111	-0.320	-0.019	-0.300	0.773	-0.057	0.174	-0.047	0.105	0.070	-0.131	-0.145	-0.116
PV2	-0.210	-0.060	0.080	-0.446	0.034	-0.276	0.905	0.002	0.098	-0.121	0.066	0.046	-0.040	-0.113	-0.005
PV3	-0.134	-0.158	0.083	-0.190	0.046	-0.169	0.749	-0.010	0.138	-0.050	-0.007	0.005	-0.049	0.051	0.061
PV4	-0.209	-0.082	0.090	-0.275	-0.049	-0.244	0.809	0.079	0.210	-0.157	-0.001	0.011	-0.000	0.019	0.074
PV5	-0.216	-0.106	0.095	-0.203	0.165	-0.192	0.808	0.028	0.091	-0.044	0.003	0.059	-0.057	-0.038	0.014
PV6	-0.230	-0.182	0.053	-0.329	0.094	-0.289	0.860	0.034	0.157	-0.180	0.012	0.083	-0.086	-0.094	-0.017
RC1	-0.083	0.028	0.255	-0.182	-0.157	-0.006	0.180	0.091	0.759	-0.137	0.049	-0.069	0.018	0.027	0.002
RC2	-0.111	-0.020	0.205	-0.173	-0.200	-0.070	0.133	0.062	0.839	-0.123	0.109	-0.031	-0.028	-0.103	-0.103
RC3	-0.312	-0.074	0.233	-0.224	-0.358	-0.157	0.180	0.077	0.914	-0.276	-0.024	-0.134	-0.102	-0.061	-0.040
RC4	-0.272	-0.179	0.146	-0.197	-0.326	-0.147	0.137	0.023	0.882	-0.232	-0.068	-0.055	-0.079	0.035	-0.080
RC5	-0.143	-0.072	0.070	-0.099	-0.184	-0.037	0.173	0.037	0.771	-0.170	-0.018	-0.017	-0.012	-0.048	-0.044
RC6	-0.172	0.016	0.079	-0.068	-0.346	-0.071	-0.001	0.087	0.740	-0.191	0.035	-0.123	0.039	0.021	-0.016
RC7	-0.112	-0.237	-0.107	-0.036	-0.291	-0.079	0.028	0.029	0.555	-0.038	-0.024	-0.014	0.002	-0.098	-0.156
RC8	-0.260	-0.134	-0.002	-0.164	-0.318	-0.184	0.117	-0.023	0.720	-0.287	0.025	-0.058	-0.076	-0.084	-0.082
RE1	0.484	0.361	0.096	0.374	0.353	0.516	-0.091	0.104	-0.234	0.786	0.118	0.043	0.118	-0.000	-0.090
RE2	0.354	0.322	0.166	0.381	0.311	0.438	-0.030	0.002	-0.188	0.817	0.076	0.083	0.012	0.019	-0.029
RE3	0.277	0.185	0.187	0.432	0.106	0.373	-0.138	0.048	-0.202	0.775	-0.033	0.122	0.031	0.013	-0.050
RE4	0.264	0.188	0.227	0.254	0.099	0.272	-0.151	0.068	-0.118	0.651	-0.063	0.034	-0.135	-0.047	-0.020
RW-PUSE	0.098	0.180	0.107	0.100	-0.020	-0.025	-0.007	-0.011	-0.072	-0.064	-0.027	-0.351	0.463	0.617	1.000
RW-PV	-0.066	-0.102	-0.115	0.097	0.039	-0.008	0.059	-0.107	-0.085	0.099	-0.153	1.000	-0.435	-0.317	-0.351
RW-PS	0.086	-0.102	0.054	-0.014	0.312	-0.029	0.045	0.084	0.014	0.039	1.000	-0.153	0.314	-0.170	-0.027
RW-FC	-0.027	0.099	-0.006	0.117	-0.071	0.181	-0.083	-0.204	-0.044	0.000	-0.170	-0.317	0.304	1.000	0.617
RW-CAW	0.157	-0.038	-0.040	0.011	0.084	0.138	-0.074	0.017	-0.055	0.025	0.314	-0.435	1.000	0.304	0.463

No cross-loadings were detected, implying that there was no discriminant validity (see Table 7). Discriminant validity tests whether concepts or measurements that are not supposed to be related are unrelated. Hence it measures the extent to which items of one latent construct differ from the items of the other latent construct where these two latent constructs are not expected to be related. It was established by showing that indicators of one latent construct are not like the indicators of the other construct. Furthermore, this study assessed the Fornell Larcker and heterotrait–monotrait (HTMT) ratio to further test the discriminant validity. HTMT (see Table 8) values should be less than 0.85 (Hair et al., 2012; Lei et al., 2023; Phillip et al., 2023). The values for HTMT in Table 8 are all lower than 0.85 showing that the different latent constructs measure different things. For Fornell-Lacker (see Table 9), the square root of AVE must be greater than inter-constructs (inter correlations).

Table 8: HTMT (heterotrait–monotrait ratio)

	CAW	FC	GCL	CPBAP	PS	PUSE	PV	RW	RC	RE
CAW										
FC	0.35									
GCL	0.16	0.36								
CPBAP	0.54	0.3	0.16							
PS	0.34	0.1	0.11	0.24						
PUSE	0.39	0.39	0.070	0.53	0.15					
PV	0.28	0.14	0.1	0.42	0.14	0.32				
RW	0.093	0.069	0.041	0.15	0.031	0.1	0.045			
RC	0.29	0.15	0.21	0.23	0.37	0.14	0.19	0.072		
RE	0.56	0.42	0.26	0.62	0.38	0.62	0.17	0.084	0.29	

Table 9: Fornell-Lacker

	CAW	FC	GCL	CPBAP	PS	PUSE	PV	RW	RC	RE
CAW	0.84									
FC	0.33	0.92								
GCL	0.12	0.33	0.88							
CPBAP	0.44	0.26	0.099	0.74						
PS	0.29	0.084	-0.053	0.19	0.76					
PUSE	0.34	0.37	0.064	0.47	0.11	0.89				
PV	-0.23	-0.11	0.1	-0.39	0.047	-0.31	0.82			
RW	-0.025	0.066	-0.034	-0.12	-0.006	0.098	0.013	1		
RC	-0.25	-0.094	0.18	-0.21	-0.34	-0.13	0.17	0.06	0.78	
RE	0.46	0.35	0.22	0.49	0.29	0.53	-0.130	0.07	-0.25	0.76

In addition, this study assessed the variance inflation factor against the multicollinearity of collected data. Multicollinearity means there was no correlation between two or more independent variables (Saunders et al., 2009). In this case, there are five such variables, namely CAW, FC, GCL, LengthRemWk, and CPBAP. All the variance inflation factor values were above four (see Table 10) and no collinearity was observed (Ng et al., 2021).

Table 10: Variance Inflation Factor (VIF)

Construct	VIF	PS	1.29
CAW	1.42	PUSE	1.69
FC	1.37	PV	1.290
GCL	1.26	RC	1.27
LengthRemWk	1	RE	1.86
CPBAP	1.67		

4.6 Assessment of the Structural Model

This study used Smart PLS 4 to assess the structural equation modelling using 5000 bootstraps. The structural model was assessed using the significance of path coefficients and the coefficient of determination (R^2) for the cybersecurity protective behaviour against phishing, a dependent variable. R^2 is also called the goodness-of-fit measure as it shows the percentage of the dependent variables' variance that all the independent variables account for. A positive path coefficient indicated that 1 unit of independent variable results in particular R^2 value increase in the dependent variable. Also, a negative path coefficient means 1 unit increase in independent variable results in R^2 decrease in the dependent variable. The hypotheses were tested within a margin error or confidence interval of 5%, which is the probability ($p< 0.05, t > 1.96$) or confidence level at 95% for significance but for $p> 0.05$ or $t < 1.96$ it implied that the research hypotheses would be refuted (Bhattacherjee, 2012; Hair et al., 2011).

Table 11 Path coefficients, P-values, and T-values

Hypotheses	Path	Path Coefficient	t-Value	p-Value	Sig Level	Supported
H1	RW-CPBAP	-0.14	2.02	0.043	P<0.05	Yes
H2	CAW-CPBAP	0.2.	1.8	0.072	p< 0.1	Marginally supported
H3	PUSE-CPBAP	0.19	1.18	0.24	-	No
H4a	FC-CPBAP	0.	0.003	0.99	-	No
H4b	FC-PUSE-CPBAP	-0.051	0.6	0.51	-	No
H4c	FC-CAW	033	4.01	0	P<0.05	Yes
H4d	FC-PUSE	0.34	4.14	0	P<0.05	Yes
H5a	PV-CPBAP	-0.25.	2,94	0.003	P<0.05	No, opposite to what was hypothesised although significant

Hypotheses	Path	Path Coefficient	t-Value	p-Value	Sig Level	Supported
H5b	PV-PUSE	-0.274.	2.94	0.003	P<0.05	No, opposite to the hypothesis
H6a	PS-CPBAP	0.025	0.28	0.78	-	No
H6b	PS-RE	0.32	3.44	0.001	P<0.05	Yes
H7	RE-CPBAP	0.24	2	0.045	P<0.05	Yes
H8	RC-CPBAP	-0.021	0.19	0.85		No
H9a	GCL-CPBAP	0.009	0.11	0.91		
H9b	GCL-RC		1.83	0.067	P<0.1	Marginally supported

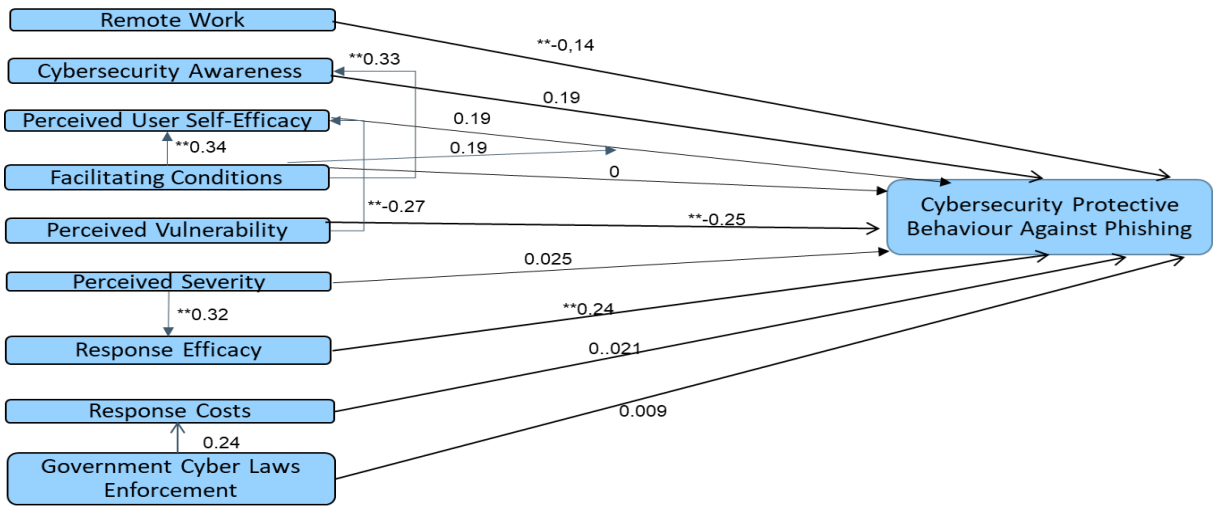

Figure 12: Final Model

4.7 Summary of Chapter

This dissertation used a questionnaire survey to collect responses from employees from South African organisations. Thereafter, the demographic profile, descriptive statistics, structural equation model, and measurement model were analysed. The structural model was assessed resulting in the final model using PLS-SEM.

5 Discussion

5.1 Introduction

This chapter presents key findings to answer the research question. The research question is: What factors influence cybersecurity protective behaviour against phishing in South African organisations? The research objective was met; however, some factors such as facilitating conditions which did not positively influence cybersecurity protective behaviour against phishing were rejected. The chapter discussed research limitations and recommendations for future studies.

5.2 Key Findings

This study sought to investigate factors that influence cybersecurity protective behaviour against phishing in South Africa. Because our sample is never equal to the population, we can never be certain that the conclusions we draw from sample data apply to the entire population, which is why statistical testing is always probabilistic (Bhattacherjee, 2012). The p-value is the likelihood that a statistical inference is the result of sheer chance and is set at a significance value of 0.05 (Bhattacherjee, 2012). The results in Table 12 (see Section 4.6) show that there is a negative relationship between remote work (independent variable) and cybersecurity protective behaviour against phishing (dependent variable) as was hypothesised from the literature review. Additionally, the t-value is more than the 1.96 (t-value=2.02) threshold and the p-value is above the 0.05 threshold (p-value=0.043). Therefore, the relationship is significant and the H1 hypothesis is accepted at a 95% confidence level. This was consistent with the researchers' view that remote work negatively influences cybersecurity protective behaviour against phishing (Klein, 2021; Mihailović et al., 2021; Mou et al., 2022; Nyarko & Fong, 2023; Vivekananth, 2022; Škiljić, 2020).

The path of the coefficient was found to be positive for H2. Also, the results in Table 12 (see Section 4.6) show that the t-value was slightly below 1.96 (t-value =1.797) and the p-value less than 0.1 (p-value=0.072). Therefore, the relationship was reasonably significant and the H2 hypothesis was marginally supported and accepted at a 90% confidence level. A p-value of less than 0.1 can be deemed to be marginally supported Li et al. (2018). Consistent with the work of many researchers, cybersecurity awareness was found to positively influence cybersecurity

protective behaviour against phishing (Alshaik, 2021; Hijji & Alam, 2022; Vivekananth, 2021). It should be noted that respondents were a hybrid from the private and public sectors from South African organisations receiving varying degrees of information and cybersecurity awareness, hence the marginal support for the hypothesis.

The results showed that the path of the coefficient was positive for hypothesis H3, the t-value was found to be below 1.96 (t-value =1.184), and the p-value was above 0.05 (p-value=0.236). Therefore, the relationship is not significant and the H3 hypothesis was rejected at a 95% confidence level. This means that perceived user self-efficacy was not found to have a significant and positive effect on cybersecurity protective behaviour against phishing (Bax et al., 2021; Bekkers et al., 2023). However, in the study of cybercrime reporting behaviour, self-efficacy was a contributing factor (Pilane et al., 2022).

In hypothesis H4a, the t-value was 0.003 (less than 1.96) and p-value was 0.998 (greater than 0.05). Also, no relationship was established since the path of the coefficient was 0. Therefore, the relationship was not significant and the H4a hypothesis was rejected at a 95% confidence level. This was inconsistent with researchers' view that facilitating conditions positively influence cybersecurity protective behaviour against phishing (Alqahtani and Braun, 2021; Chin and Chua, 2021; McLennan and Group, 2022). For hypothesis H4b, there was a negative relationship between facilitating conditions' positive moderation on the influence of perceived user self-efficacy on cybersecurity protective behaviour against phishing. The relationship was not significant as there was a t-value of 0.603 and a p-value of 0.547, resulting in H4b being rejected and inconsistent with the literature review (Alqahtani and Braun, 2021; Azjen, 1976; Chin and Chua, 2021; McLennan and Group, 2022). When looking at the research instrument, the questions used may not have been specific enough to allow the respondent room to understand, for example, resources, knowledge and experience can be interpreted differently depending on whether the organisation has a cybersecurity awareness program or not.

The t-value was 4.414, the p-value was 0, and there was a positive relationship for hypothesis H4c path of coefficient. The relationship was significant at a confidence level of 95% and consistent with cybersecurity research (Abroshan et al., 2021; Alqahtani and Braun, 2021; Azjen, 1976; Bispham et al., 2021; Butler and Butler, 2018; Hijji and Alam, 2022; Jansen &

van Schaik, 2019; Kabanda et al., 2018; Nyarko & Fong, 2023; Qabajeh et al., 2018). H4c was accepted.

For hypothesis H4d, the relationship was found to be positive, the t-value was 4.135, and the p-value was 0. Therefore, the relationship was significant at a confidence level of 95% and H4d was accepted, which was consistent with research work (Alshaik, 2021; Chin and Chua, 2021; Hijji & Alam, 2022; Vivekananth, 2021).

For hypothesis H5a, the t-value was 2.944 (above 1.96) and the p-value was 0.003 (below 0.05). The relationship was negative, meaning an increase in the independent variable resulted in a decrease in the dependent variable at R^2 of 41.5%. Although the relationship was significant, the H5a hypothesis was rejected at a 95% confidence level as the results were contrary to the hypothesis. This result was inconsistent with researchers' view that perceived vulnerability influences cybersecurity protective behaviour against phishing (Bax et al., 2021; Mou et al., 2022). However, some researchers suggested perceived vulnerability influence on phishing behaviour to be significant in a personal context than organisational context (Mou et al., 2022) Similarly, for the H5b hypothesis, the t-value was 2.942, the p-value was 0.003 and the relationship was negative. Therefore, H5b was accepted at a 95% confidence level since it was significant in terms of the hypothesised statement (Bekkers et al., 2023; Chen and Jackson, 2019; De Kimpe et al., 2022; Farkhondeh et al., 2023; Lei et al., 2023). This shows that threat appraisal (perceived vulnerability factor) does have an influence on coping appraisal (perceived user self-efficacy factor) which was little researched using Protection Motivation Theory. However, Mou et al. (2022) argued that perceived vulnerability was stronger in personal contexts.

For hypothesis H6a the path of the coefficient was found to be positive. However, the results in Table 12 showed that the t-value was below 1.96 (t-value =0.281) and the p-value was above 0.05 (p-value=0.779). Therefore, the relationship is not significant and the H6a hypothesis was rejected at a 95% confidence level. This was inconsistent with previous researchers' views that perceived severity influences cybersecurity protective behaviour against phishing (Bax et al., 2021; Chin and Chua, 2021; Rogers, 1975). The notion that perceived severity is strong in a personal context might be valid (Mou et al., 2022). On the other hand, hypothesis H6b was accepted at a 95% confidence level with a positive relationship, t-value of 3.349, and p-value

of 0.01, which was consistent with researchers' views (Bekkers et al., 2023; Chen and Jackson, 2019; De Kimpe et al., 2022; Farkhondeht et al., 2020; Lei et al., 2023). This shows that threat appraisal (perceived severity) influences coping appraisal (response efficacy), an issue which had been little researched previously according to the researcher's knowledge.

The path of the coefficient was found to be positive for hypothesis H7, the t-value was above 1.96 (t-value =2.002) and the p-value was below 0.05 (p-value=0.045). Therefore, the relationship was found to be significant and the H7 hypothesis was accepted at a 95% confidence level. Response efficacy was found to have a significant and positive effect on cybersecurity protective behaviour against phishing which was consistent with the work of researchers (Bax et al., 2021; Bekkers et al., 2023; Mou et al., 2022). In an organisational context, this finding agrees with the research by Mou et al. (2022).

The t-value for hypothesis H8 was 0.187 (below 1.96), while the p-value was 0852 (above 0.05), and the path of the coefficient was positive. Therefore, the relationship was not significant and the H8 hypothesis was rejected at a 95% confidence level. This indicated that response costs did not have a significant effect on cybersecurity protective behaviour against phishing which was inconsistent with researchers' views (Bax et al., 2021; Bekkers et al., 2023; Mou et al., 2022).

Hypothesis H9a had a positive relationship, a t-value of 0.11 and a p-value of 0.912. Therefore, the relationship was not significant resulting in H9a being rejected at a 95% confidence level. This was not consistent with reviewed literature (Buckley et al., 2023; Chin and Chua, 2021; Dlamini and Mbambo; 2019; Interpol, 2021; Mcanyana et al., 2020). Moreover, respondents may have interpreted statements differently, for example, efficacy and performance quality. H9b was marginally supported at the confidence level of 90% because the relationship was positive, t-value of 1.833 (slightly less than 1.96), and a p-value of 0.067 ($p<0.1$) in line with research work (Buckley et al., 2023; Chin and Chua, 2021; Dlamini and Mbambo; 2019; Interpol, 2021; Mcanyana et al., 2020).

These research findings answer the research question: What factors influence cybersecurity protective behaviour against phishing in South African organisations? Hypotheses H1, H2, H4c, H4d, H6b, H7 and H9b identified the factors that influence cybersecurity protective behaviour against phishing in South Africa. H5a and H5b results seem to establish an argument

by researchers that perceived vulnerability is stronger in personal contexts than organisational contexts as both hypotheses were significant although rejected (Mou et al., 2022). Also, cybersecurity researchers might acquire an in-depth understanding of factors influencing cybersecurity protective behaviour against phishing.

5.3 Research Limitations

This study was completed through a cross-sectional design, meaning it was conducted in a limited period. Firstly, a small sample size was used, which may reduce the chance of reaching satisfactory conclusions; it has a low statistical power compared to that obtained using a larger sample. Larger datasets from bigger samples may change results significantly, especially for hypotheses that were marginally supported. Secondly, the context of this study was for South African organisations. Hence, it may be difficult to generalise the results to other populations or contexts. However, the study may be used as a baseline study, especially in countries in the third world where the challenges are greater than in developed. Furthermore, this study did not establish the knowledge of respondents regarding phishing which could influence the results. Also, the sample was from more educated participants.

5.4 Recommendations for Future Research

For future research, considerations regarding conducting studies with longitudinal designs could be made; this would allow researchers to enlarge the sample and resulting dataset, making results more robust and rigorous. Consideration may also be made to include other third-world countries with developing economies as literature seemed to concentrate on developed economies. Also, cybercrime reduces African GDP (gross domestic product) by more than 10% per annum, and by more than 4.12 billion US dollars (Interpol, 2021).

Exploration of different mediating and moderating variables from the literature should be considered. Demographic variables may also be evaluated as moderating or mediating variables in future studies of cybersecurity protective behaviour against phishing, particularly in the South African context. As an example, some researchers claim that employees are susceptible to risky cybersecurity phishing behaviours based on gender (Gillan and White, 2021). Furthermore, researchers claim that newer employees may be more vulnerable to phishing attempts than those who have been at the organisation for a longer period (Beu et al., 2023). Other variables that future studies could include are employee loyalty and satisfaction.

5.5 Summary of Chapter

The results of the findings indicate that remote work, cybersecurity awareness, and response efficacy impact cybersecurity protective behaviour against phishing while facilitating conditions have a positive and direct influence on cybersecurity awareness and perceived user self-efficacy. Furthermore, perceived severity impacts response efficacy while government cyber laws impact response costs.

6. Conclusion

This dissertation explains the factors that influence cybersecurity protective behaviour against phishing in South African organisations and answers the research question. It was discovered that although remote working has benefits in terms of productivity, it may influence cybersecurity protective behaviour against phishing negatively for organisations that allow their employees to work from home. This implies that organisations may need to improve their cybersecurity strategies against phishing, allocating both sufficient human and financial resources to support the new remote ways of work. Furthermore, respondents commented that cybersecurity threats are on the rise with the adoption of remote working.

Contrary to many researchers, facilitating conditions were found to have no relationship nor a significant influence on cybersecurity protective behaviour against phishing. It neither confirms nor denies what other researchers argued, namely that in a workplace context, there are measures in place to manage cybersecurity risks. Hence, this was inconclusive in the South African context. Facilitating conditions were not found to positively moderate the influence of perceived user self-efficacy on cybersecurity protective behaviour against phishing but had a significant influence on both cybersecurity awareness and perceived user self-efficacy. This implies that South African organisations should consider bolstering and mobilising resources to maintain a posture of cybersecurity protective behaviour against phishing.

Cybersecurity awareness was marginally supported in its relationship with cybersecurity protective behaviour against phishing. This may be because of the low sample effect; most cybersecurity research confirms that cybersecurity awareness is a predictor of cybersecurity protective behaviour against phishing. In addition, respondents indicated more awareness is required. There are also new deep fake forms of phishing that some users may not know about. As for perceived vulnerability in cybersecurity protective behaviour against phishing, a significant influence was established, although the relationship was negative. Some researchers argue that perceived vulnerability has a stronger effect in a personal setting than in a workplace setting on which this study is grounded. Perhaps the feeling of being vulnerable makes users feel unable to address cybersecurity protective behaviour against phishing bearing in mind the challenges in South Africa regarding poor implementation of cyber laws. As for the influence of perceived vulnerability on perceived user self-efficacy, the negative but significant

relationship could be resolved when users gain phishing knowledge. Such knowledge may be acquired through simulations, and awareness, and explore the argument of a personal setting versus a workplace setting. There was an insignificant relationship and hence no confirmed influence by perceived severity on cybersecurity protective behaviour against phishing. However, this is inconclusive as perceived severity had a positive and significant relationship with response efficacy.

Response efficacy positively and significantly influenced cybersecurity protective behaviour against phishing. In contrast, response cost did not significantly influence cybersecurity protective behaviour against phishing. This might be due to the increasing costs associated with defence against attacks, including cyber insurance. However, government cyber law enforcement had a positive although marginally significant relationship with response costs. Despite this, government cyber law enforcement did not influence cybersecurity protective behaviour against phishing. However, respondents' comments highlighted that government efforts in curbing phishing were insufficient. Also, respondents felt that executives did not understand cybersecurity sufficiently. This is an area that is important to encourage because top or executive sponsorship for cybersecurity protective behaviour against phishing is critical.

Lastly, financial losses, reputational damage, disinformation, and legal implications (lawsuits) may be managed to acceptable thresholds or risk appetite within South African organisations through robust cybersecurity practices such as cybersecurity protective behaviour against phishing.

References

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). COVID-19 and Phishing: Effects of Human Emotions, Behaviour, and Demographics on the Success of Phishing Attempts during the Pandemic. *IEEE Access*, *9*, 121916–121929. https://doi.org/10.1109/ACCESS.2021.3109091.

Ahmad, I., Parvez, M. A., & Iqbal, A. (2019). TypoWriter: A tool to prevent typosquatting. *Proceedings - International Computer Software and Applications Conference*, *1*, 423–432. https://doi.org/10.1109/COMPSAC.2019.00068.

Akdemir, N., & Yenal, S. (2021). How Phishers Exploit the Coronavirus Pandemic: A Content Analysis of COVID-19-Themed Phishing Emails. *SAGE Open*, *11*(3). https://doi.org/10.1177/21582440211031879.

Alahmari, S., Renaud, K., & Omoronyia, I. (2023). Moving beyond cyber security awareness and training to engendering security knowledge sharing. *Information Systems and e-Business Management*, *21*(1), 123-158.

Alheneidi, H., Alsumait, L., Alsumait, D., & Smith, A. P. (2021). Loneliness and problematic internet use during COVID-19 lockdown. *Behavioral Sciences*, *11*(1). https://doi.org/10.3390/bs11010005.

Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the frontiers of cybersecurity behaviour: a systematic review of studies and theories. Applied Sciences, 13(9), 5700.

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behaviour: A practice perspective. *Computers & Security*, *98*, 102003.

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

Alqahtani, M., & Braun, R. (2021). Reviewing influence of UTAUT2 factors on cyber security compliance: A literature review. *IBIMA Business Review*, *2021*. https://doi.org/10.5171/2021.666987.

Alyahya, A., & Weir, G. R. (2021, March). Understanding responses to phishing in Saudi Arabia via the theory of planned behaviour. In *2021 National Computing Colleges Conference (NCCC)* (pp. 1-6). IEEE.

APWG, A.-P. W. G. (2021). Phishing Activity Trends Report 3 Quarter Unifying the Global Response to Cybercrime. November.

Arachchilage, N. A. G., Love, S., & Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior*, *60*, 185–197. https://doi.org/10.1016/j.chb.2016.02.065.

Azjen, I. (1991), "The theory of planned behaviour", *Organizational Behaviour and Human Decision Processes*, Vol. 50 No. 2, pp. 179-211, doi: 10.1016/0749-5978(91)90020-T.

Bakalovic, A. (2020). The Importance of Cybersecurity Education (Doctoral dissertation, Utica College).

Baral, G., & Arachchilage, N. A. G. (2019). Building confidence not to be phished through a gamified approach: Conceptualising user's self-efficacy in phishing threat avoidance behaviour. *Proceedings - 2019 Cybersecurity and Cyberforensics Conference, CCC 2019*, *Ccc*, 102–110. https://doi.org/10.1109/CCC.2019.000-1.

Bax, S., McGill, T., & Hobbs, V. (2021). Maladaptive behaviour in response to email phishing threats: The roles of rewards and response costs. *Computers and Security*, *106*, 102278. https://doi.org/10.1016/j.cose.2021.102278.

Bayl-Smith, P., Taib, R., Yu, K., & Wiggins, M. (2022). Response to a phishing attack: persuasion and protection motivation in an organizational context. *Information & Computer Security*, *30*(1), 63-78.

Bekkers, L., Van, S., Goede, H., Huurne, E. M., Van, Y., Spithoven, R., & Rutger, E. (2023). Computers & Security Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model. *Computers & Security*, *127*, 103099. https://doi.org/10.1016/j.cose.2023.103099.

Belli, L. (2021). Cybersecurity policymaking in the BRICS countries: From addressing national priorities to seeking international cooperation. *The African Journal of Information and Communication (AJIC), 28*, 1-14. https://doi.org/10.23962/10539/32208.

Bentler, P. M., & Bonett, D. G. (1980). Significance Tests and Goodness-of-Fit in the Analysis of Covariance Structures, *Psychological Bulletin*, 88: 588-600.

Berlilana, Noparumpa, T., Ruangkanjanases, A., Hariguna, T., & Sarmini. (2021). Organisation benefits as an outcome of organisational security adoption: The role of cyber security readiness and technology readiness. *Sustainability (Switzerland)*, *13*(24). https://doi.org/10.3390/su132413761.

Beu, N., Jayatilaka, A., Zahedi, M., Babar, A., Hartley, L., Lewinsmith, W., & Baetu, I. (2023). Computers & Security Falling for phishing attempts: An investigation of individual differences that are associated with behaviour in a naturalistic phishing simulation. *Computers & Security*, *131*, 103313. https://doi.org/10.1016/j.cose.2023.103313.

Bhattacherjee, A. (2012). Social science research: Principles, methods, and practices. USA.

Bispham, M., Creese, S., Dutton, W. H., Esteve-Gonzalez, P., & Goldsmith, M. (2021). Cybersecurity in Working from Home: An Exploratory Study. *SSRN Electronic Journal*, *April 2022*. https://doi.org/10.2139/ssrn.3897380.

Blanca, M. J., Arnau, J., López-Montiel, D., Bono, R., & Bendayan, R. (2013). Skewness and kurtosis in real data samples. *Methodology*.

Bodsberg, L., Grotan, T. O., Jaatun, M. G., & Waro, I. (2021). HSE and Cyber Security in Remote Work. *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2021*. https://doi.org/10.1109/CyberSA52016.2021.9478249.

Brewster, T. (2021, October 14). Fraudsters Cloned Company Director's Voice In $35 Million Heist, Police Find. *Forbes*.

https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/.

Büchi, M., Just, N., & Latzer, M. (2017). Caring is not enough: the importance of Internet skills for online privacy protection. *Information, Communication & Society*, *20*(8), 1261-1278.

Buckley, J., Lottridge, D., Murphy, J. G., & Corballis, P. M. (2023). Indicators of employee phishing email behaviours: Intuition, elaboration, attention, and email typology. *International Journal of Human-Computer Studies*, 102996. https://doi.org/10.1016/j.ijhcs.2023.102996.

Butler, R., & Butler, M. (2018). Assessing the information quality of phishing-related content on financial organisations' websites. *Information and Computer Security*, *26*(5), 514–532. https://doi.org/10.1108/ICS-09-2017-0067.

Calderaro, A., & Craig, A. J. S. (2020). Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building. *Third World Quarterly*, *41*(6), 917–938. https://doi.org/10.1080/01436597.2020.1729729.

Chambers, D. (2023, January 17). Africa's biggest law firm was just nailed for not stopping a R5.5 million hack – with R2,000 a month. *News 24*. https://www.news24.com/news24/bi-archive/ensafrica-hit-for-bad-online-security-that-cost-a-house-buyer-r55-million-2023-1.

Chen, S., & Jackson, T. (2019). Causal effects of challenge and threat appraisals on pain self-efficacy, pain coping, and tolerance for laboratory pain: An experimental path analysis study. *PLoS ONE*, *14*(4), e0215087. https://link-gale-com.ezproxy.uct.ac.za/apps/doc/A583328634/AONE?u=unict&sid=bookmark-AONE&xid=94c2b298.

Chin, W. W. (1998). The partial least squares approach to structural equation modelling. *Modern methods for business research*, *295*(2), 295-336.

Chin, W. Y., & Chua, H. N. (2021). Using the theory of interpersonal behaviour to predict information security policy compliance. *2021 8th International Conference on*

eDemocracy and eGovernment, ICEDEG 2021, 80–87. https://doi.org/10.1109/ICEDEG52154.2021.9530849.

Chng, S., Yu, H., Kumar, A., & Yau, D. (2022). Computers in Human Behaviour Reports Hacker types, motivations and strategies: A comprehensive framework IT. *Computers in Human Behavior Reports*, *5*, 100167. https://doi.org/10.1016/j.chbr.2022.100167.

Coetzee, A. (2022). *A Conceptual Model for Phishing Awareness: A South African Study*. University of Johannesburg (South Africa).

Collard, A. (2023). *KnowBe4 African Cybersecurity & Awareness Report 2023*. https://www.knowbe4.com/typ-research-2023-african-cybersecurity-awareness-report?submissionGuid=b97187a0-70ec-4e86-a5c3-17e94cd56833.

Crossler, R.E.; Bélanger, F.; and Ormond, D (2017). The quest for complete security: An empirical analysis of users' multi-layered protection from security threats. *Information Systems Frontiers, (2017*). doi: https://doi.org/10.1007/s10796-017-9755-1

Cybersecurity and Infrastructure Security Agency (CISA). (2020). DPRK Cyber Threat Advisory.https://www.cisa.gov/sites/default/files/2020-04/DPRK_Cyber_Threat_Advisory_04152020_S508C.pdf

De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2022). What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. *Behaviour and Information Technology*, *41*(8), 1796–1808. https://doi.org/10.1080/0144929X.2021.1905066.

Depietro, R., Wiarda, E., & Fleischer, M. (1990). The context for change: Organization, technology and environment. *The processes of technological innovation*, *199*(0), 151-175.

Dijkstra, T. K. and Henseler, J. (2015). Consistent and Asymptotically Normal PLS Estimators for Linear Structural Equations, *Computational Statistics & Data Analysis*, 81(1): 10-23.

Dlamini, S., & Mbambo, C. (2019). Understanding policing of cybercrime in South Africa: The phenomena, challenges and effective responses. *Cogent Social Sciences*, *5*(1). https://doi.org/10.1080/23311886.2019.1675404.

Domain name Authority of South Africa (.ZADNA). (2023). https://www.zadna.org.za/our-mandate/our-core-mandate.

Dremliuga, R. I., Korobee, A. I., Mamychev, A. Y., & Miroshnichenko, O. I. (2021). Trends and methods of fighting cybercrimes in the Russian Federation in terms of the transition to a digital economy. *Laplage Em Revista, 7(2),* 191-200. https://doi.org/10.24115/s2446-6220202172701p.191-200.

Eboibi, F. E. (2020). Concerns of cyber criminality in South Africa, Ghana, Ethiopia, and Nigeria: rethinking cybercrime policy implementation and organisational accountability. *In Commonwealth Law Bulletin (Vol. 46, Issue 1)*. Routledge. https://doi.org/10.1080/03050718.2020.1748075.

Falade, P. V. (2023). Decoding the threat landscape: Chatgpt, fraudgpt, and wormgpt in social engineering attacks. *arXiv preprint arXiv:2310.05595*.

Farkhondeh, H., Harminder, S., & Jocelyn, W. (2020). The Role of Contextualization in Users' Vulnerability to Phishing Attempts. *Australasian Journal of Information Systems*, *24*, 1-32.

Fay, M. J. (2007). Informal communication practices between peers in the remote work context (Doctoral dissertation, The Ohio State University).

Fei, J., Xia, Z., Yu, P., & Xiao, F. (2021). Exposing AI-generated videos with motion magnification. *Multimedia Tools and Applications*, *80*, 30789-30802.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research*, *18*(1), 39-50.

Gillam, A. R., & Waite, A. M. (2021). Gender differences in predictors of technology threat avoidance. *Information and Computer Security*, *29*(3), 393–412. https://doi.org/10.1108/ICS-01-2020-0008.

Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The Emerging Threat of AI-driven Cyber Attacks: A Review. Applied Artificial Intelligence, 36(1). https://doi.org/10.1080/08839514.2022.2037254

Haveibeenpwned.(2023). https://haveibeenpwned.com/PwnedWebsites.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice*, *19*(2), 139-152.

Hair, J. F., Sarstedt, M., Ringle, C. M., & Mena, J. A. (2012). An assessment of the use of partial least squares structural equation modelling in marketing research. *Journal of the academy of marketing science*, *40*, 414-433.

Henseler, J., Dijkstra, T. K., Sarstedt, M., Ringle, C. M., Diamantopoulos, A., Straub, D. W., Ketchen, D. J., Hair, J. F., Hult, G. T. M., and Calantone, R. J. (2014). Common Beliefs and Reality about Partial Least Squares: Comments on Rönkkö & Evermann (2013), *Organizational Research Methods*, 17(2): 182-209.

Hijji, M., & Alam, G. (2022). Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. *Sensors*, *22*(22), 8663. https://doi.org/10.3390/s22228663.

Hong, Y., & Furnell, S. (2021). Understanding cybersecurity behavioural habits: Insights from situational support. Journal of Information Security and Applications, 57, 102710.

Hu, L.-t., and Bentler, P. M. (1998). Fit Indices in Covariance Structure Modeling: Sensitivity to Underparameterized Model Misspecification, *Psychological Methods*, 3(4): 424-453.

Humaidi, N., & Balakrishnan, V. (2018). Indirect effect of management support on users' compliance behaviour towards information security policies. *Health Information Management Journal*, *47*(1), 17-27.

Information Regulator (South Africa). (2023). INFRINGEMENT NOTICE AND R5 MILLION ADMINISTRATIVE FINE ISSUED TO THE DEPARTMENT OF JUSTICE AND CONSTITUTIONAL DEVELOPMENT FOR CONTRAVENTION OF POPIA. *97*(JULY), 4–5. https://inforegulator.org.za/wp-content/uploads/2020/07/MEDIA-

STATEMENT-INFRINGEMENT-NOTICE-ISSUED-TO-THE-DEPARTMENT-OaF-JUSTICE-AND-CONSTITUTIONAL.pdf.

Internet Service Providers' Association (ISPA). (2023). https://ispa.org.za/about-ispa/.

Interpol. (2021). African cyber threat assessment report: Interpol's key Insight into Cybercrime in Africa. *Interpol*, *October* 1–34. https://www.interpol.int/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf.

Interpol (2023). African Cyber Threat Assessment Report 2023. African cyber threat assessment report cyber threat trends. https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations/AFJOC-African-Joint-Operation-against-Cybercrime.

Iqbal, S., Moleiro Martins, J., Nuno Mata, M., Naz, S., Akhtar, S., & Abreu, A. (2021). Linking entrepreneurial orientation with innovation performance in SMEs; the role of organizational commitment and transformational leadership using smart PLS-SEM. *Sustainability*, *13*(8), 4361.

Jansen, J., & van Schaik, P. (2019). The design and evaluation of a theory-based intervention to promote security behaviour against phishing. *International Journal of Human-Computer Studies*, *123* (September 2018), 40–55. https://doi.org/10.1016/j.ijhcs.2018.10.004.

Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, *28*(3), 269–282. https://doi.org/10.1080/10919392.2018.1484598.

Kara, I., & Aydos, M. (2022). The rise of ransomware: Forensic analysis for Windows-based ransomware attacks. *Expert Systems with Applications*, *190* (November 2021), 116198. https://doi.org/10.1016/j.eswa.2021.116198.

Kävrestad, J., Hagberg, A., Nohlberg, M., Rambusch, J., Roos, R., & Furnell, S. (2022). Evaluation of contextual and game-based training for phishing detection. *Future Internet, 14*(4), 104.

Kenneth, M. (2017). Cyber Threat or Cyber Threat Inflation? - Assessing the Risk to U.S. National Security. In *Small Wars Journal*. https://smallwarsjournal.com/jrnl/art/cyber-threat-or-cyber-threat-inflation-assessing-the-risk-to-us-national-security.

Khan, N. A., Brohi, S. N., & Zaman, N. (2020). Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. *TechRxiv Powered by IEEE*, *May*, 1–6. https://www.techrxiv.org/articles/Ten_Deadly_Cyber_Security_Threats_Amid_COVID-19_Pandemic/12278792.

Klein, J. (2021). *Committee Member*. xviii–xviii. https://doi.org/10.1109/pmis52742.2021.00006.

KPMG Africa. (2022). *Africa Cyber Security Outlook*. *September*, 1–49. https://kpmg.com/za/en/home/insights/2022/09/africa-cybersecurity-outlook-report-2022.html.

Kritzinger, E., Da Veiga, A., & van Staden, W. (2023). Measuring organizational information security awareness in South Africa. *Information Security Journal: A Global Perspective*, *32*(2), 120-133.

Kumar, R., Sharma, S., Vachhani, C., & Yadav, N. (2022). What changed in the cybersecurity after COVID-19? *Computers and Security*, *120*, 102821. https://doi.org/10.1016/j.cose.2022.102821.

Kwak, Y., Lee, S., Damiano, A., & Vishwanath, A. (2020). Why do users not report spear phishing emails? *Telematics and Informatics*, *48*(August 2019), 101343. https://doi.org/10.1016/j.tele.2020.101343.

Leet, E. S. (2020). About the Cover. *Postmedieval*, *11*(1). https://doi.org/10.1057/s41280-020-00164-x.

Lei, W., Hu, S., & Hsu, C. (2023). Computers & Security Unveiling the process of phishing precautions taking: The moderating role of optimism bias. *Computers & Security*, *129*, 103249. https://doi.org/10.1016/j.cose.2023.103249.

Li, Luo, X. (Robert), Zhang, J., & Sarathy, R. (2018). Self-control, organizational context, and rational choice in Internet abuses at work. *Information & Management*, *55*(3), 358–367. https://doi.org/10.1016/j.im.2017.09.002

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioural research: Integrating new and existing techniques. *MIS Quarterly*, 293-334.

Malwarebytes Labs: Q1 2019 Cybercrime Tactics and Techniques. (2019). *Computer Fraud & Security, 2019(5),* 4. https://doi.org/10.1016/s1361-3723(19)30049-1.

Malwarebytes. (2023). State of malware report. https://go.malwarebytes.com/rs/805-USG-300/images/MWB_State_of_Malware_Report_2023.pdf.

Matli, W. (2020). The changing work landscape as a result of the COVID-19 pandemic: insights from remote workers life situations in South Africa. *International Journal of Sociology and Social Policy*, *40*(9–10), 1237–1256. https://doi.org/10.1108/IJSSP-08-2020-0386.

Mcanyana, W., Brindley, C., & Seedat, Y. (2020). *Insight into the cyber threat landscape in South Africa*. 12. https://www.accenture.com/_acnmedia/PDF-125/Accenture-Insight-Into-The-Threat-Landscape-Of-South-Africa-V5.pdf.

McLennan, M., & Group, S. (2022). *The Global Risks Report 2022*. https://www.weforum.org/reports/global-risks-report-2022.

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems*, *34*(4), 1203-1230.

Microsoft. (2018). *Microsoft-Protect yourself from phishing*. https://support.microsoft.com/en-us/windows/protect-yourself-from-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44.

Mihailescu, M. I., Nita, S. L., Rogobete, M., & Marascu, V. (2023, June). Unveiling Threats: Leveraging User Behavior Analysis for Enhanced Cybersecurity. In *2023 15th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)* (pp. 01-06). IEEE.

Mihailović, A., Cerović Smolović, J., Radević, I., Rašović, N., & Martinović, N. (2021). COVID-19 and beyond: employee perceptions of the efficiency of teleworking and its cybersecurity implications. *Sustainability*, *13*(12), 6750.

Mirsky, Y., Demontis, A., Kotak, J., Shankar, R., Gelei, D., Yang, L., Zhang, X., Pintor, M., Lee, W., Elovici, Y., & Biggio, B. (2023). Computers & Security the Threat of Offensive AI to Organizations. *Computers & Security*, *124*, 103006. https://doi.org/10.1016/j.cose.2022.103006.

Min, H. (2023). Assessing the impact of a COVID-19 pandemic on supply chain transformation: an exploratory analysis. *Benchmarking: An International Journal, 30*(6), 1765-1781.

Mou, J., Cohen, J. F., Bhattacherjee, A., & Kim, J. (2022). A test of protection motivation theory in the information security literature: A meta-analytic structural equation modelling approach. *Journal of the Association for Information Systems*, *23*(1), 196-236.

Mustak, M., Salminen, J., Mäntymäki, M., Rahman, A., & Dwivedi, Y. K. (2023). Deepfakes: Deceptions, mitigations, and opportunities. *Journal of Business Research*, *154*, 113368.

Ng, K. C., Zhang, X., Thong, J. Y. L., & Tam, K. Y. (2021). Protecting Against Threats to Information Security: An Attitudinal Ambivalence Perspective. *Journal of Management Information Systems*, *38*(3), 732–764. https://doi.org/10.1080/07421222.2021.1962601.

Nyarko, D. A., & Fong, R. C. W. (2023, January). Cyber Security Compliance Among Remote Workers. In *Cybersecurity in the Age of Smart Societies: Proceedings of the 14th International Conference on Global Security, Safety and Sustainability, London, September 2022* (pp. 343-369). Cham: Springer International Publishing.

Parliament of the Republic of South Africa (2023). https://www.parliament.gov.za/acts?sorts[date]=-1&sorts[number]=-1.

Pasikowski, S. (2023). Snowball Sampling and Its Non-Trivial Nature. *Przegląd Badań Edukacyjnych (Educational Studies Review)*, *2*(43), 105-120.

Philip, S. J., Luu, T. J., & Carte, T. (2023). There's No place like home: Understanding users' intentions toward securing internet-of-things (IoT) smart home networks. *Computers in Human Behavior, 139*, 107551.

Pieterse, H. (2021). The Cyber Threat Landscape in South Africa: A 10-Year Review. *The African Journal of Information and Communication*, *28*(28), 1–21. https://doi.org/10.23962/10539/32213.

Pilane, K., Ruhwanya, Z., & Brown, I. (2022, July). Factors Influencing Cybercrime Reporting Behaviour in South African State-Owned Entities. In *International Symposium on Human Aspects of Information Security and Assurance* (pp. 285-299). Cham: Springer International Publishing.

Png, I. P. L., & Wang, Q.-H. (2009). Information Security: Facilitating User Precautions Vis-à-Vis Enforcement Against Attackers. *Journal of Management Information Systems*, *26*(2), 97–121. https://doi-org.ezproxy.uct.ac.za/10.2753/MIS0742-122226020.

Qabajeh, I., Thabtah, F., & Chiclana, F. (2018). A recent review of conventional vs. automated cybersecurity anti-phishing techniques. *Computer Science Review*, *29*, 44–55. https://doi.org/10.1016/j.cosrev.2018.05.003.

Rameem Zahra, S., Ahsan Chishti, M., Iqbal Baba, A., & Wu, F. (2021). Detecting COVID-19 chaos-driven phishing/malicious URL attacks by a fuzzy logic and data mining-based intelligence system. *Egyptian Informatics Journal*, *xxxx*. https://doi.org/10.1016/j.eij.2021.12.003.

Rogers, K. (2022). The effects of remote work on organizational culture: Examining the effects of external social support to mitigate social isolation within organizations.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology*, *91*(1), 93-114.

Ryan, G. (2018). Introduction to positivism, interpretivism and critical theory. *Nurse researcher, 25*(4), 41-49.

Salman, K. (2022). Assessing Work from Home Security Packages Vulnerabilities (Doctoral dissertation, Auckland University of Technology).

Saunders, M., Lewis, P., & Thornhill, A. (2009). Research methods for business students. Pearson education.

Saunders, M., Lewis, P. and Thornhill, A. (2012), *Research Methods for Business Students*, Pearson Education, London.

Scott, J., and Kyobe, M., 2021. Trends in cybersecurity management issues related to human behaviour and machine learning. In: *2021 International Conference on Electrical, Computer and Energy Technologies (ICECET) IEEE*. pp. 1-8. https://doi.org/10.1109/ICECET52533.2021.9698626.

Sharevski, F., Devine, A., Pieroni, E., & Jachim, P. (2022). Gone quishing: A field study of phishing with malicious qr codes. *arXiv preprint arXiv:2204.04086*.

Škiljić, A. (2020). Cybersecurity and remote working: Croatia's (non-)response to increased cyber threats. *International Cybersecurity Law Review*, *1*(1–2), 51–61. https://doi.org/10.1365/s43439-020-00014-3.

South African Banking Risk Information Centre (SABRIC). (2022). https://www.sabric.co.za/media-and-news/press-releases/sabric-statement-on-transunion-south-africa-and-personal-information/.

South African Banking Risk Information Centre. (2021). Annual crime statistics 2021.

South African Fraud Prevention Services (SAFPS). (2023). https://www.safps.org.za/Home/About.

South African Police Service (SAPS). (2022). *Police Recorded Crime Statistics: First Quarter of 2022/2023*. *January*. https://www.saps.gov.za/services/crimestats.php.

South African Police Service (SAPS). (2022). INTERPOL SA arrests Nigerian national wanted for online fraud and money laundering worth R192 million. https://www.saps.gov.za/newsroom/selnewsdetails.php?nid=40749.

South African Revenue Service (SARS). (n.d). https://www.sars.gov.za/types-of-tax/pay-as-you-earn/employment-tax-incentive-eti/standard-industrial-classification-codes/.

State, T., & Security, E. (2022). *PA*.

Stojnic, T. (2021). Phishing email strategies: Understanding cybercriminals' strategies of crafting phishing emails. February, 1–17. https://doi.org/10.1002/spy2.165.

Stratton, G., Powell, A., & Cameron, R. (2017). Crime and justice in digital society: Towards a "digital criminology"? *International Journal for Crime, Justice and Social Democracy, 6(2),* 17-33. https://doi.org/10.5204/ijcjsd.v6i2.355.

Stupp, C. (2019, August 30). Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case. *The Wall Street Journal.*

Sun, J. C. Y., Yu, S. J., Lin, S. S. J., & Tseng, S. S. (2016). The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behaviour and gender difference. *Computers in Human Behavior*, *59*, 249–257. https://doi.org/10.1016/j.chb.2016.02.004.

Šupa, M., Kaktinas, V., & Rinkevičiūtė, A. (2023). Computer-dependent or computer-assisted? The social context of online crime in Lithuanian court judgements. *International Journal of Law, Crime and Justice*, *73*(November 2022), 100577. https://doi.org/10.1016/j.ijlcj.2023.100577.

SWIFT. (2019). *SWIFT ISAC Report: Three years on from Bangladesh - Tackling the adversaries*. *April*.

Triandis, H. C. (1980). Reflections on trends in cross-cultural research. *Journal of cross-cultural psychology*, *11*(1), 35-58.

Us, A. (2018). Advancing Your Anti-Phishing Program A Look at the Situation. February, 1–13.

Van Zoonen, W., Sivunen, A., Blomqvist, K., Olsson, T., Ropponen, A., Henttonen, K., & Vartiainen, M. (2021). Understanding stressor–strain relationships during the COVID-19 pandemic: the role of social support, adjustment to remote work, and work-life conflict. *Journal of management & organization, 27(6)*, 1038-1059.

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly*, 21-54.

Vivekananth, P. (2022). Cybersecurity Risks in Remote Working Environment and Strategies to Mitigate Them. 1(1), 108–111.

Vrhovec, S., Bernik, I., & Markelj, B. (2023). Computers & Security Explaining information seeking intentions: Insights from a Slovenian social engineering awareness campaign. *Computers & Security*, *125*, 103038. https://doi.org/10.1016/j.cose.2022.103038.

Wannenburg, M. C., Nieman, A., Steyn, B., & Wannenburg, D. G. (2023). South Africans' susceptibility to phishing attacks. *Southern African Journal of Accountability and Auditing Research*, *25*(1), 53-72.

World Economic Forum. (2021). The Global Risks Report 2021: 16th Edition. In *Weforum.Org*. http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf.

Yang, Jing; Linkeschova, L. (n.d.). The Employee Perceptions of Remote Work and Cybersecurity in an International Organisation during COVID-19 Remote Working and Cybersecurity in the Pandemic Research on the Employee Perceptions of Remote Work and Academic Supervisor: Professor Jörg Balsig.

Zaman, U., Zahid, H., Habibullah, M. S., & Din, B. H. (2021). Adoption of Big Data Analytics (BDA) Technologies in Disaster Management: A Decomposed Theory of Planned Behaviour (DTPB) Approach. *Cogent Business and Management*, *8*(1). https://doi.org/10.1080/23311975.2021.1880253

Appendix A Ethics Form

1.1 UCT Ethics in Research Form

UNIVERSITY OF CAPE TOWN
FACULTY OF COMMERCE
Igniting Knowledge and Opportunity

Commerce Faculty Ethics in Research Application Form

Any person planning to undertake research in the Faculty of Commerce at the University of Cape Town is required to complete this form **before collecting or analysing data**. If any of the questions below have been answered YES, and the applicant is NOT an Honours student, the form it should be submitted to the supervisor (where applicable) and from there for approval by the Faculty EIR committee: Ms. Samantha Alexander (**samantha.alexander@uct.ac.za).**

It is assumed that the researcher has read the UCT Code for Research involving Human Subjects (Available at http://web.uct.ac.za/depts/educate/download/uctcodeforresearchinvolvinghumansubjects.pdf) in order to be able to answer the questions in this form.

Students must include a copy of the completed form with the dissertation/thesis when it is submitted for examination.

1. PROJECT DETAILS		
Project title: Cybersecurity in the workplace: Factors that influence positive cybersecurity behaviour against phishing		
Principal Researcher/s: KARABO PILANE	**Email address(es):**	Plnlet001@myuct.ac.za
Research Supervisor: Zainab Ruhwanya Irwin Brown	**Email address(es):**	Zainab.ruhwanya@uct.ac.za Irwin.brown@uct.ac.za
Co-researcher(s): N/A	**Email address(es):**	N/A
Department: Department of Information Systems		
Brief description of the project: The purpose of this research project is to explain the factors that influence positive cybersecurity behaviour against phishing in the workplace.		

2. PARTICIPANTS		
2.1 Does the research discriminate against participation by individuals, or differentiate between participants, on the grounds of gender, race or ethnic group, age range, religion, income, handicap, illness or any similar classification?	☐YES	☒NO
2.2 Does the research require the participation of socially or physically vulnerable people (children, aged, disabled, etc.) or legally restricted groups?	☐YES	☒NO
2.3 Will you be able to secure the informed consent of all participants in the research? (In the case of children, will you be able to obtain the consent of their guardians or parents?)	☒YES	☐NO
2.4 Will any confidential data be collected or will identifiable records of individuals be kept?	☐YES	☒NO
2.5 In reporting on this research is there any possibility that you will not be able to keep the identities of the individuals involved anonymous?	☐YES	☒NO
2.6 Are there any foreseeable risks of physical, psychological or social harm to participants that might occur in the course of the research?	☐YES	☒NO
2.7 Does the research include making payments or giving gifts to any participants?	☐YES	☒NO

If you have answered **YES to any of these questions**, please describe how you plan to address these issues (append to form):

Consent will be requested from all participants via an informed consent letter displayed at the start of the online questionnaire and interview participants consent to take part in research and to be recorded will be asked at the beginning of the interview session. Refer to Appendix 9.1 and 9.2 for informed consent cover letter accompanying this research design.

Affiliations of participants: (please select)

☐ Company employees ☐Hospital employees ☒General public ☐Military staff ☐Farm workers ☐

Students

☐Other (please specify): N/A

Gender: Are you asking a question about gender in your questionnaire?

☒Yes ☐No

If you answered Yes to the above - Have you included the option: "Prefer not to answer" as part of your gender question?

☒Yes ☐No

If you have selected "No" in the question above regarding gender, please explain why:

Race / Ethnicity:

Are you asking a question about race/ethics in your questionnaire?

☐Yes ☒No

Which race categories have been used?

Have you included the option: "Prefer not to answer" as part of your race/ethics question?

Does your research involve the participation of or provision of services to communities? ☐Yes ☒No
If your answer is YES, please complete below:

3.1 Is the community expected to make decisions for, during or based on the research?	☐YES	☒NO
3.2 At the end of the research will any economic or social process be terminated or left unsupported, or equipment or facilities used in the research be recovered from the participants or community?	☐YES	☒NO
3.3 Will any service be provided at a level below the generally accepted standards?	☐YES	☒NO

If you answered YES to any of these questions, please describe below how you plan to address these issues.

If your research is being conducted within a specific organisation, please state how organisational permission has been/will be obtained:

Letters will be sent to heads or directors of organisations for individual participation in the study

Have you attached the letter from the organisation granting permission? (please select)

☐Yes ☒No, but this **will be** obtained before commencing the research ☐Not applicable

Are you making use of **UCT students** as respondents for your research? (please select) ☐Yes ☒No

If yes, have you contacted Executive Director: Student Affairs for permission? (please select) ☐Yes ☐No

Was approval granted? (please select) ☐Yes ☐No ☐Awaiting a response

Are you making use of **UCT staff** as respondents for your research? (please select) ☐Yes ☒No

If yes, have you contacted Executive Director: Human Resources for permission? (please select) ☐Yes ☐No

Was approval granted? (please select) ☐Yes ☐ No ☐Awaiting a response

Contact Emails: Executive Director: Human Resources (Miriam.Hoosain@uct.ac.za)
Executive Director: Student Affairs (Moonira.Khan@uct.ac.za)

.

5. INFORMED CONSENT

What type of consent will be obtained from study participants?

☐Oral Consent

☐ Written Consent

☒Anonymous survey questionnaire (covering letter required, no consent form needed)

☐Other (please specify)

How and where will consent/permission be recorded?

Have you attached an informed consent form to your application? ☒Yes ☐No

6. SPONSORSHIP OF RESEARCH

If your research is sponsored, is there any potential for conflicts of interest? ☐Yes ☒No
If your answer is YES, please complete below

If you have answered **YES** to any of these questions, please describe how you plan to address these issues (append to form)

6. RISK TO PARTICIPANTS
Does the proposed research pose any physical, psychological, social, legal, economic, or other risks to study participants you can foresee, both immediate and long range? (please select) ☐Yes ☒No **If yes, answer the following questions:** 1. Describe in detail the nature and extent of the risk and provide the rationale for the necessity of such risks 2. Outline any alternative approaches that were or will be considered and why alternatives may not be feasible in the study 3. Outline whether and why you feel that the value of information to be gained outweighs the risks
1.
2.
3.

I certify that I have read the the Commerce Faculty Ethics in Research policy ☒

(http://www.commerce.uct.ac.za/Pages/ComFac-Downloads**)**

I hereby undertake to carry out my research in such a way that.

- there is no apparent legal objection to the nature or the method of research; and
- the research will not compromise staff or students or the other responsibilities of the University.
- the stated objective will be achieved, and the findings will have a high degree of validity.
- limitations and alternative interpretations will be considered.
- the findings could be subject to peer review and publicly available; and
- I will comply with the conventions of copyright and avoid any practice that would constitute plagiarism.

Signed by:

	Full name and signature	Date
Principal Researcher/Student:	Karabo Pilane	26/08/2022

This application is approved by:

Supervisor	ZAINAB RUHWANYA IRWIN BROWN	
HOD (or delegated nominee – for all Honours Projects):		
Chair: Faculty EIR Committee (only for postgraduate research at Master and PhD level)		

Cybersecurity in the workplace: Factors that influence cybersecurity protective behaviour against phishing in South Africa

CHECKLIST	SELECT
A full copy of a research proposal or a literature review with methodology is attached in a separate file	☒
Interview schedules / cover letters / questionnaires / forms and other materials used in the study are attached in separate files	☐
Organisational consent letter / UCT student or staff approval letter	☒
On your cover letter to your questionnaire have you included the following?	NA
1. The following UCT Logo	☒
2. A sentence explaining the aim of the research.	☒
3. Sentences of a similar nature to below must be included in the cover letter or consent form:	☒
This research has been approved by the Commerce Faculty Ethics in Research Committee.	☒
Your participation in this research is voluntary. You can choose to withdraw from the research at any time.	☒
The questionnaire will take approximately 15-20 minutes to complete.	☒
You will not be requested to supply any identifiable information, ensuring anonymity of your responses.	☒ OR
Due to the nature of the study, you will need to provide the researchers with some form of identifiable information however, all responses will be confidential and used for the purposes of this research only.	☒
Should you have any questions regarding the research please feel free to contact the researcher (insert contact details).	☒
4. Have you scanned in your signature for the last section of the form?	☒

UCT.

Appendix B Cover letter and Informed Consent (Organisation)

Dear Sir/Madam.

In terms of the requirements for completing a Master's Degree in Information Systems at the University of Cape Town, a research study is required.

My research topic is Cybersecurity in the Workplace: Factors that Influence Cybersecurity Protective Behaviour against Phishing in South Africa. The aim is to explain what factors influence cybersecurity protective behaviour against phishing post-lockdowns. This research has been approved by the Commerce Faculty Ethics in Research Committee.

Participation in this research by your organisation is voluntary. The organisation can choose to withdraw from the research at any time. The questionnaire will take approximately 15 minutes to complete. Participants will not be requested to supply personally identifiable information to maintain the anonymity of responses.

Should you have any questions regarding the research, please feel free to contact me via phone at +27 795238217, or email: plnlet001@myuct.ac.za.

If you authorise this study to be undertaken at your organisation, kindly sign the attached form and return it to me at your earliest convenience.

Your organisation's participation in this study would be greatly appreciated.

Sincerely,

Karabo Pilane

Researcher / B. Com Masters Student

Supervisors Names: Prof Irwin Brown,

Ms Zainab Ruhwanya.

Cybersecurity in the workplace: Factors that influence cybersecurity protective behaviour against phishing in South Africa

Department of Information Systems
University of Cape Town

Department of Information Systems.
University of Cape Town.

Email: plnlet001@myuct.ac.za

Management Consent.

I, _____, give the researcher, Karabo Pilane, consent to conduct the study 'Cybersecurity in the workplace: Factors that influence cybersecurity protective behaviour against phishing in South Africa at the identified Organisation Name.

I am aware that participation is voluntary and that respondents may choose to withdraw from this study at any time, should they choose to do so.

Signature Date.

Appendix C Cover Letter and Informed Consent (Individual)

Dear Sir/Madam.

In terms of the requirements for completing a Master's Degree in Information Systems at the University of Cape Town, a research study is required.

My research topic is Cybersecurity in the Workplace: Factors that Influence Cybersecurity Protective Behaviour against Phishing in South Africa. The aim is to explain what factors influence cybersecurity protective behaviour against phishing. This research has been approved by the Commerce Faculty Ethics in Research Committee.

Your participation in this research is voluntary. You can choose to withdraw from the research at any time. The questionnaire will take approximately 15 minutes to complete. You will not be requested to supply identifiable information to maintain the anonymity of your responses.

Should you have any questions regarding the research, please feel free to contact me via phone at +27 795238217, or email: plnlet001@myuct.ac.za.

By clicking the button below, you acknowledge that:

Your participation in the study is voluntary. You may choose to terminate your participation at any time.

I consent.

I do not consent.

Appendix D: Research Instrument

Table 12: Demographic Profile of Survey Respondents

(Adapted from Büchi et al. (2017); Crossler et al. (2017); Humaidi et al. (2018); Min (2022); Rogers (2022); South African Revenue Service (n.d), Van Zoonen et al. (2021); Yang et al. (n.d))

Item	Choice	Code
Age	18-20	1
	21-30	2
	31-40	3
	41-50	4
	51-60	5
	60+	6
Sex	Male	1
	Female	2
	Non-binary/Third Gender	3
	Prefer to self-describe	4 + answer
	Prefer not to answer	5
Highest education	Some school	1
	High School	2
	Certificate/Diploma	3
	Bachelor's degree/B-Tech	4
	Honours/Postgraduate-Diploma	5
	Master's degree	6
	Doctoral Degree	7
	Others	8
Type of Organisation	Private Company	1

	Personal Liability Company	2
	Public Company	3
	Non-Profit Organisation (NPO)	4
	State-Owned Company	5
	Government	6
	Non-Government Organisation (NGO)	7
Industry Type	Education	1
	Information and Communication	2
	Manufacturing	3
	Financial and Insurance Activities	4
	Human Health and Social Work Activities	5
	Public Administration and Defence	6
	Agriculture, Forestry, and Fishing	7
	Electricity, Gas, Steam, and Air Conditioning Supply	8
	Water Supply, Sewerage, Waste Management, and Remediation Activities	9
	Transportation and Storage	10
	Professional, Scientific, and Technical Activities	11
	Administrative and Support Service Activities	12
	Construction	13
	Retail	14
	Other Service Activities	15
Size of organisation	Micro (0-10)	1
	Small (11-50	2
	Medium (51-250)	3
	Large (250 and above)	4

Role in organisation	Information Technology	1
	Finance	2
	Supply Chain	3
	Human Resources	4
	Governance, Risk, and Compliance	5
	Other	6
Occupational Level	Top Management/Executive	1
	Senior Management	2
	Professionally Qualified/Experienced Specialist/Middle Management	3
	Skilled Technical and Academically Qualified/Junior Management/Supervisors/Foremen/Superintendents	4
	Semi-Skilled	
	Unskilled	5
		6
Length of Work	0-2 years	1
	2-5 years	2
	5-10 years	3
	> 10 years	4
Internet access years	Less than 1	1
	1-2	2
	2-5	3
	5+	4

Table 13: Questionnaire Survey

Items	Scale
Remote Work	
Percentage of Remote Work	
What percentage of your work time do you spend working remotely?	
76%-100%	1
51%-75%	2
26%-50%	3
1%-25%	4
0%	5
Frequency of Remote Work	
Select the best possible option which indicates how frequently you work remotely.	
All days of the week	1
Four days per week	2
Three days per week	3
One to two days per week	4
Never	5
Extent of Remote Work	
To what extent do you work remotely?	
Not at all	1
Minimal extent	2
To some extent	3
To a large extent	4

All the time	5
Length of Remote Work	
How long have you worked remotely?	
Less than 6 months	1
6 months to 3 years	2
3-5 years	3
5-10 years	4
More than 10 years	5
Intensity of Remote Work	
How intensely do you work remotely daily?	
I never work remotely.	1
I spend about two hours.	2
I spend about three to five hours.	3
I spend about six to eight hours.	4
I spend over eight hours.	5
Facilitating Conditions	
Select whether you disagree or agree with the following statements.	1 Strongly Disagree 2 3 Neutral 4 5 Strongly Agree
My organisation has the necessary resources to spot phishing.	
My organisation provides the necessary knowledge to act against phishing.	
My organisation has enough experience to manage phishing.	
Cybersecurity Awareness	
Select whether you disagree or agree with the following statements.	

Overall, I am aware of the potential phishing threats and their negative consequences. I am aware that a compromised system can be misused for phishing attacks in the future. I understand the concerns regarding phishing threats and the risks they pose in general.	1 2 3 4 5	Strongly Disagree Neutral Strongly Agree
Perceived Vulnerability		
Select whether you disagree or agree with the following statements. There is a chance of me falling victim to a phishing email threat. There is a good possibility that I could become a victim of a phishing email. I feel I will become a victim of phishing email in the future. I feel I could be vulnerable to falling victim to phishing email attempts. I feel I could be vulnerable to having my personal identification details stolen through a phishing email attempt. I feel I could be vulnerable to having my financial information stolen through a phishing email attempt.	1 2 3 4 5	Strongly Disagree Neutral Strongly Agree
Perceived Severity		
Select whether you disagree or agree with the following statements. Becoming a victim of phishing email would be a serious problem for me. Responding to a phishing email would have serious consequences for me. Providing my personal identification details to someone unknown to me would have serious consequences for me. Providing my financial details to someone unknown to me would have serious consequences for me. Becoming a victim of phishing would cause my whole life to change. If I were to become a victim of phishing email, I would suffer a lot of mental anguish.	1 2 3 4 5	Strongly Disagree Neutral Strongly Agree
Perceived User Self-efficacy		

Select whether you disagree or agree with the following statements. I am confident in my ability to recognise a potential phishing email. I am confident in my ability to act safely regarding a potential phishing email. I am confident in my ability to protect myself from phishing email threats. It is easy for me to recognise a potential phishing email. It is easy for me to act safely about a potential phishing email. It is easy for me to protect myself from phishing email threats.	1 Strongly Disagree 2 3 Neutral 4 5 Strongly Agree
Response Efficacy	
Select whether you disagree or agree with the following statements. Paying careful attention to the content of the emails I receive protects me from phishing email threats. Checking where an email's links are going before clicking on them protects me from phishing email threats. Using email 'spam filters' (which automatically direct suspicious-looking emails to 'junk' or 'spam' folders) is an effective way to prevent phishing email threats. If I look carefully at an email before taking any action in response to it, I am less likely to fall victim to phishing email threats.	1 Strongly Disagree 2 3 Neutral 4 5 Strongly Agree
Response Costs	
Select whether you disagree or agree with the following statements. Taking protective measures against phishing email threats would be time-consuming. Paying careful attention to the content of emails before acting on them is inconvenient. Taking protective measures against phishing email threats would cause me to be confused. Using protective measures against phishing email threats would slow me down. Taking protective measures against phishing email would cost me money.	1 Strongly Disagree 2 3 Neutral 4 5 Strongly Agree

Inspecting email links before clicking on them would be a waste of effort. Taking protective measures against phishing email threats means I have to search through my 'junk' and 'spam' folders looking for legitimate emails. Taking protective measures against phishing email threats makes me feel less trusting towards all the emails in my inbox.	
Positive Cybersecurity Behaviour Against Phishing	
Select whether you disagree or agree with the following statements. I never open emails from unknown senders. I immediately delete suspicious emails without reading them. I always check where an email link is going before I click on it. I always pay attention to the content of emails when checking my email messages. I do not take action in response to an email unless I am sure of who it is from. I use anti-phishing browser tools (which automatically alert me if I am accessing a potentially suspicious website) to protect myself from phishing email threats. I use email 'spam filters' (which automatically direct suspicious-looking emails to 'junk' or 'spam' folders) to protect myself from phishing email attempts.	1 Strongly Disagree 2 3 Neutral 4 5 Strongly Agree
Government Cyber Laws Enforcement	
Select whether you disagree or agree with the following statements. Government is enforcing cybersecurity laws. Government has efficacy in enforcing cybersecurity laws. Government is committed to cybersecurity law enforcement. I believe in the performance quality of government in enforcing cybersecurity laws.	1 Strongly Disagree 2 3 Neutral 4 5 Strongly Agree

Table 14: Initial Factor Loading

%RemWk <- Remote Work	-0.023
CAW1	0.86
CAW2	0.84
CAW3	0.83
ExtentRemWk <- Remote Work	-0.089
FC1	0.95
FC2	0.89
FC3	0.92
FreqRemWk <- Remote Work	-0.047
GCL1	0.92
GCL2	0.9
GCL3	0.86
GCL4	0.85
IntenseRemWk <- Remote Work	-0.058
LengthRemWk <- Remote Work	0.8
CPBAP1	0.54
CPBAP2	0.55
CPBAP3	0.73
CPBAP4	0.71
CPBAP5	0.69
CPBAP6	0.7
CPBAP7	0.79
PS1	0.611
PS2	0.71
PS3	0.78

PS4	0.88
PS5	0.225
PS6	-0.24
PUSE1 <- Perceived User Self-efficacy	0.8
PUSE2 <- Perceived User Self-efficacy	0.9
PUSE3 <- Perceived User Self-efficacy	0.941
PUSE4 <- Perceived User Self-efficacy	0.85
PUSE5 <- Perceived User Self-efficacy	0.9
PUSE6 <- Perceived User Self-efficacy	0.81
PV1 <- Perceived Vulnerability	0.78
PV2 <- Perceived Vulnerability	0.91
PV3 <- Perceived Vulnerability	0.75
PV4 <- Perceived Vulnerability	0.81
PV5 <- Perceived Vulnerability	0.81
PV6 <- Perceived Vulnerability	0.86
RC1 <- Response Costs	0.77
RC2 <- Response Costs	0.85
RC3 <- Response Costs	0.91
RC4 <- Response Costs	0.88
RC5 <- Response Costs	0.77
RC6 <- Response Costs	0.73
RC7 <- Response Costs	0.54
RC8 <- Response Costs	0.71
RE1 <- Response Efficacy	0.78
RE2 <- Response Efficacy	0.82
RE3 <- Response Efficacy	0.78

RE4 <- Response Efficacy	0.65
Remote Work x Perceived User Self-efficacy -> Remote Work x Perceived User Self-efficacy	1
Remote Work x Perceived Severity -> Remote Work x Perceived Severity	1
Cybersecurity Awareness x Perceived Severity -> Cybersecurity Awareness x Perceived Severity	1
Remote Work x Facilitating Conditions -> Remote Work x Facilitating Conditions	1
Cybersecurity Awareness x Perceived Vulnerability -> Cybersecurity Awareness x Perceived Vulnerability	1
Cybersecurity Awareness x Facilitating Conditions -> Cybersecurity Awareness x Facilitating Conditions	1
Cybersecurity Awareness x Response Efficacy -> Cybersecurity Awareness x Response Efficacy	1
Cybersecurity Awareness x Perceived User Self-efficacy -> Cybersecurity Awareness x Perceived User Self-efficacy	1
Remote Work x Cybersecurity Awareness -> Remote Work x Cybersecurity Awareness	1
Remote Work x Perceived Vulnerability -> Remote Work x Perceived Vulnerability	1

Table 15: Initial CA, CR and AVE

	Cronbach's alpha	Composite reliability (rho_a)	Composite reliability (rho_c)	Average variance extracted (AVE)
Cybersecurity Awareness	0.8	0.81	0.88	0.71
Facilitating Conditions	0.91	0.94	0.94	0.85
Government Cyber Laws	0.92	1.13	0.95	0.78
Cybersecurity protective behaviour against phishing	0.81	0.82	0.85	0.46

Perceived Severity	0.79	0.78	0.71	0.39
Perceived User self-efficacy	0.95	0.95	0.96	0.79
Perceived Vulnerability	0.90	0.95	0.92	0.67
Remote Work	0.92	-2.24	0.074	0.13
Response Costs	0.91	0.94	0.92	0.60
Response Efficacy	0.76	0.78	0.84	0.58

Table 16: Demographics

Age	Frequency	Percentage
18-20	0	0
21-30	10	9.9%
31-40	61	60.4%
41-50	21	20.8%
51-60	8	7.9%
60+	1	1%
Gender		
Male	41	40.6%
Female	59	58.4%
Non-binary/third gender	1	1%
Prefer to self-describe	0	0%
Prefer not to answer	0	0%
Highest Education		

Some school	0	0%
High school	1	1%
Certificate/Diploma	17	16.8%
Bachelor's degree/B-Tech	22	21.8%
Honours/Postgraduate-Diploma	39	38.6%
Master's degree	18	17.8%
Doctoral Degree	4	4%
Other	0	0%
Type of Organisation		
Private Company	48	40%
Personal Liability Company	0	0%
Public Company	13	10.8%
Non-Profit Organisation (NPO)	0	0%
State-Owned Company	15	12.5%
Government	43	35.8%
Non-Government Organisation (NGO)	1	0.8%
Industry Type		
Education	7	5.9%
Information and Communication	21	17.8%
Manufacturing	5	4.24%
Financial and Insurance Activities	38	32.2%
Human Health and Social Work Activities	3	2.5%
Public Administration and Defence	13	11%
Agriculture, Forestry, and Fishing	3	2.5%
Electricity, Gas, Steam, and Air Conditioning Supply	0	0%

Water Supply, Sewerage, Waste Management, and Remediation Activities	0	0%
Transportation and Storage	1	0.9
Professional, Scientific, and Technical Activities	4	3.4
Administrative and Support Service Activities	3	2.5
Construction	1	0.9
Retail	2	1.7
Other Service Activities	17	14.4
Organisation Size		
Micro (0-10)	2	1.7%
Small (11-50)	4	3.3%
Medium (51-250)	13	10.8%
Large (251 and above)	101	84.2%
Occupational Level		
Top Management/Executive	2	1.9%
Senior Management	11	10.9%
Professionally Qualified/Experienced Specialist/Middle Management	43	42.6%
Skilled Technical and Academically qualified/Junior Management/Supervisors/Foremen/Superintendents	35	34.7%
Semi-Skilled	10	9.9%
Unskilled	0	0%
Length of work in the current organisation		
0-2 year	24	23.8%
2-5 years	25	24.8%
5-10 years	21	20.8%
>10 years	31	30.7%

Internet for work		
Less than 1	0	0%
1-2	4	3.9%
2-5	7	6.9%
5+	90	89.1%