Angler phishing attacks on social media users in South Africa

Kemisetso Mogashoa

2520298

2520298@students.wits.ac.za

0658901588

Supervisor: Professor Nixon Ochara

This research report is submitted to the Faculty of Commerce, Law and Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business

Johannesburg, February 2024

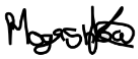
DECLARATION

Name and Surname:	Kemisetso Mogashoa
Student Number:	2520298
Degree:	Master of Management in the field of Digital Business

Angler phishing attacks on social media users in South Africa

---

I declare that this research report is my own work except as indicated in the references and acknowledgements. It is submitted in partial fulfilment of the requirements for the MMDB degree at Wits Business School. It has not been submitted before for any degree or examination in this or any other university.

Name: Kemisetso Mogashoa Signature: 

Signed at: Randburg

Date: 29 February 2024

DEDICATION

I dedicate this research to my younger self, the little girl who experienced trauma at the tender age of 12. You did not know then that God would change the trajectory of your life and have you rewrite your story. The pain is temporary, my dear Kemi. This is a reminder of how resilient and brilliant you are. You are your ancestors' wildest dreams; always look beyond the horizon and keep shooting for the stars.

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to Absa Group for being a learning organisation that invests in the growth and development of its people. Thank you for extending me this opportunity and funding this journey.

I extend a special thank you to my supervisor, Professor Nixon Ochara. The academic journey is seldom easy, yet you never lost your patience with me; instead, you continuously provided direction and guidance. Thank you for the vast knowledge you have imparted to me and the endless support.

To my mother, Fikile Rose Twala, you are the most phenomenal woman I know, a true prayer warrior. Your prayers have carried me Mom, thank you. I am also eternally grateful to my lovely sister, Lebohang Twala, for her love and support, and for always believing in me.

My sincere gratitude goes to my lovely friends and colleagues. To my line manager, Tina Arunajalam, I will cherish having walked this journey with you; you are one in a million, and I am so proud of you. Samantha Perumal, thank you for making this study possible, brainstorming ideas and always cheering me on. My lovely friend Tertia Swartz, for always lending a helping hand and for the amazing support. To Merriam Manamela, my mentor, thank you for being so tough on me and pushing me when I no longer had the strength to keep going. You are excellence personified, and I can only hope to accomplish as much as you have.

To my fellow students, specifically the 2023 MMDB Research Support WhatsApp group, you have been the wind beneath my wings. Thank you for all the support, guidance and endless memes shared to get us through this journey. I send regards and blessings to my dearest friends for their love and support, Nomtha, Tebogo, Matshidiso, Selicia and little Masie, Angela, Keamogetswe and Cosley.

Lastly, my deepest gratitude to the participants who were brave enough to share their stories. You are not what happened to you. From here, only carry the lessons with you.

To God, my redeemer, all things are possible because you are the beginning and the end. Philippians 4:13 "I can do all things through God who strengthens me".

ABSTRACT

Since its founding, the term ‘phishing’ has expanded significantly as new dynamics and paradigms keep shifting the technology space. New technology platforms have increased individuals’ use of the internet and changed the way in which we communicate forever.

Social media has steadily taken over traditional communication mediums, and the adoption is not slowing down anytime soon. What would have previously been sent as an email has now become a five-second WhatsApp message or Facebook post, and businesses are not lagging in this trend. Unfortunately, this has also led to a plethora of increased cybercrimes and has left the ecosphere of cybersecurity perturbed, as organisations scramble to find suitable solutions to combat phishing attacks internally and externally.

Seminal works have covered the impact of phishing attacks on organisations and have provided practical solutions as intervention strategies. However, the same cannot be said about individuals and consumers. As businesses start to transform digitally, social media has become an imperative mediator between businesses and consumers, and phishers have taken notice. This has birthed a new form of phishing called angler phishing. This research focused predominately on the experiences of social media users who have been victims of this type of phishing.

The study followed an interpretivist paradigm to understand victims’ realities and lived individual experiences. The snowball sampling method was executed to acquire participants, and social media was used to recruit 11 participants. Furthermore, an additional 7 participants consisting of a team of technical experts were interviewed in a focus group to evaluate the conceptual framework. The study incorporated theoretical frameworks such as the Big Five Personality Traits model and the Heuristic-systematic model (HSM) to understand personality types’ role in user behaviour and how users process information can lead to phishing susceptibility.

Key findings revealed that whilst angler phishing is a growing trend, South Africa and organisations continue to neglect documenting the severity of these crimes which subsequently contributes to increased cybercriminal attacks. Additionally, the findings revealed cybercriminals continue to evolve and adapt their strategies and techniques alongside the evolution of new technologies. As a result, findings revealed a gap in digital literacy and other factors, such as the environment and cybersecurity training, play a pivotal role in a phishing lifecycle. Furthermore, having reviewed the key theoretical frameworks and the findings from the study, an adapted conceptual framework was presented to include these additional constructs such as the environment and training.

Moreover, recommendations have been presented for both social media users and organisations on what effective interventions can be followed to prevent future attacks. Lastly, the study concludes by providing an all-encompassing view of the background of angler phishing, seminal works from the literature, a research methodology, presentation of key findings and recommendations. Ultimately, organisations and other institutions have a responsibility to ensure consumers are cyber-educated and protected. Noting the limitations of the study, suggestions for future research were provided.

KEYWORDS

Angler Phishing, phishing, social engineering, cybersecurity, social media, social networks, psychology, brand impersonation, fake accounts, personality traits, information processing

TABLE OF CONTENTS

CHAPTER 3: RESEARCH METHODOLOGY

CHAPTER 4: PRESENTATION OF FINDINGS

CHAPTER 5: DISCUSSION OF FINDINGS

CHAPTER 6: CONCLUSION AND RECOMMENDATIONS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ACRONYMS

AI	Artificial Intelligence
CAQDAS	Qualitative Data Analysis Software
CEO	Chief Executive Officer
COO	Chief Operating Officer
COVID-19	Coronavirus Disease 2019
ELM	Elaboration Like Model
HSM	Heuristic-Systematic Model
IT	Information Technology
LSM	Living Standard Measures
NPA	National Prosecuting Authority
POPI Act	Protection of Personal Information Act
SAPS	South African Police Service
SE	Social Engineering
TPB	Theory of Planned Behaviour
US	United States

CHAPTER 1: INTRODUCTION

1.1 Statement of purpose

This qualitative study investigated social media users' experiences of angler phishing attacks in South Africa. The study aimed to explore the experiences, perceptions, and behaviours of social media users who had encountered angler phishing attacks through their social media accounts, to understand the perceptions of users who are often exposed to phishing attempts and identify the strategies and techniques attackers use to successfully execute angler phishing attacks. Additionally, the study aimed to create awareness among social media users and businesses, and ensure businesses understand the role they need to play in educating consumers about cybersecurity and applying security controls earnestly.

In-depth interviews were conducted with social media users to achieve this goal. By gaining a better understanding of angler phishing attacks' impact on social media users, this study aimed to provide valuable insights to inform the development of more effective cybersecurity strategies and interventions.

1.2 Background of the study

The internet has become the biggest communication medium to date. From the simple days of email and instant messaging, networking sites such as Twitter, Facebook, and WhatsApp have become some of the largest communication channels for personal and business communication. Furthermore, considering the usage growth of the internet and its popularity as a result has influenced cybersecurity threats worldwide (Krombholz et al., 2015). South African businesses have not been exempted from this trend. Social engineering (SE), a form of cyberattack, has become rife in recent years, with various new technologies such as artificial intelligence (AI) and machine learning being leveraged to automate and personalise cyberattacks by exploiting human psychology and gaining access to data and systems (Manyam, 2022).

In the cybersecurity framework, SE is a type of attack where attackers exploit human vulnerabilities using social interaction to breach users' cybersecurity, with or without the use of technical means and technical vulnerabilities (Wang et al., 2020). There are various forms of SE attacks, but phishing has been ranked as the most common. In 2022, Cybercrime Statistics revealed that South Africa is ranked fifth among the world's most affected countries

by cyberattacks (Cybercrime Statistics, 2022). This statistic is noteworthy because it shows a correlation to the next crucial aspect of this study, namely social media usage.

In March 2023, a popular South African business journal, BusinessTech, released an article with the most contentious headline: “South Africans are the biggest internet addicts in the world” (BusinessTech, 2023).However, a contradiction to this headline followed in the article, which referenced the fact that South Africa’s average internet speed is deemed below average in comparison to its African peers (BusinessTech, 2023). Irrespective of this fact, research statistics do back up this headline; more than 40 million people in South Africa are reportedly on the internet, half of whom are registered on social media (Kemp, 2023). There is also copious literature on various definitions of ‘social media’, with definitions evolving over the years as technological disruption keeps rising. In research, social media is generally used as an umbrella term that describes a variety of online platforms, including blogs, business networks, collaborative projects, enterprise social networks, forums, microblogs, photo sharing, product reviews, social bookmarking, social gaming, social networks, video sharing, and the virtual world (Aichner et al., 2021). In this study, the Leyrer-Jackson JM and Wilson AK definition was used to define ‘social media’ as websites and technological applications that allow users to share content or participate in social networking (Aichner et al., 2021).

The average person uses 7.5 social media platforms and spends 2 hours 27 minutes on social media every day (Moran, 2023). Between 2022 and 2023, the number of social media users in South Africa increased by 0.8% (Kemp, 2023), indicating that social media’s use is growing at a rapid pace. This data has become an integral piece of information for businesses since the increase in social media presence essentially led to a shift in how companies interact with their consumers, who are also no longer confined to a passive role in their relationship with a company. Consumers are actively engaging by providing feedback quicker, asking questions, raising concerns, and ultimately expecting faster turnaround times for their queries to be addressed (Aichner et al., 2021). This phenomenon has accelerated the need to get closer to the consumer, and it has become imperative for organisations to adapt consumer management strategies. Therefore, this study aims to explore the angler phishing attacks on social media users in South Africa.

Figure 1.1 depicts a representation of social media usage in South Africa, while Figure 1.2 highlights which social media platforms have the most South African users and engagements.

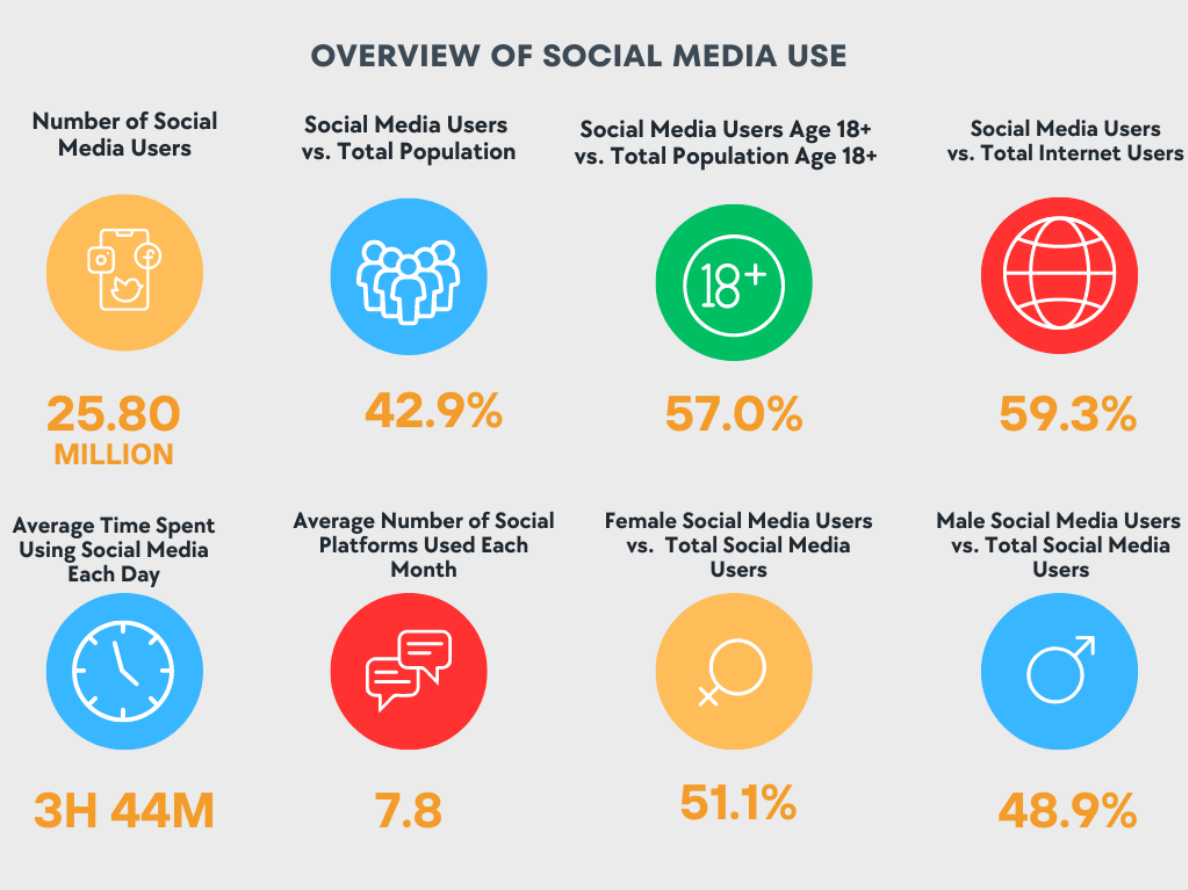


Figure 1.1: Overview of social media use in South Africa (Kemp, 2023)

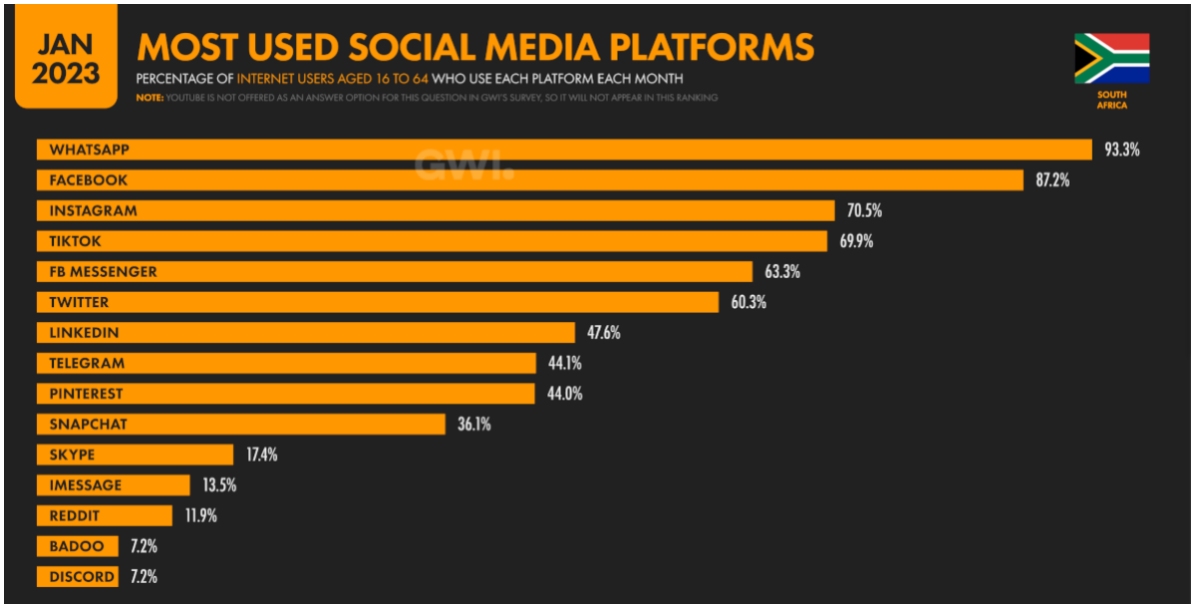


Figure 1.2: Most used social media platforms (Business Tech, 2023)

1.3 Research problem

The upsurge of internet usage has consequently led to global cybersecurity concerns. Over time, social media users have seen an increase in cyberattacks due to how exposed their lives have become on the internet. This has created opportunities for cybercriminals to exploit people's transparency, reckless online behaviour, and limited security knowledge. Phishing attacks are thus migrating to social media platforms, with a 30% increase in phishing links from the last quarter of 2017 to the first quarter of 2018 (Proofpoint, n.d.). Recent data reflects a 24% increase in phishing attacks on internet users since 2021. This increase is somewhat linked to the Coronavirus disease (COVID-19) pandemic, which forced many individuals and organisations to rely on digital communication (Al-Qahtani & Cresci, 2022).

Moreover, individuals' increased use of social media and businesses moving to social media have resulted in a new and emerging type of cyberattack, called angler phishing. This emerging technique stems from the anglerfish sea animal, which is known to lure and attack smaller prey. Similarly, with angler phishing, cybercriminals pose as legitimate businesses and lure consumers into giving up their personal details (Proofpoint, 2016).

Figure 1.3 provides a comprehensive example (Vasques, 2017). It reflects a consumer frustrated by their inability to transfer their funds; they tweet the business's account to receive instant assistance. The customer service account responds by requesting that the client try to log in again, while providing the consumer with a fraudulent link. Unbeknown to the client, this is not the real business's customer support account, despite the Twitter account appearing legit.

Figure 1.3: Angler phishing example (Proofpoint, 2016)

A few factors could result in the client disregarding this scenario as a possible phishing attempt. For example, they might be upset about the circumstance, distracted, and generally just need a quick response and solution. Alternatively, they might be accustomed to tweeting the business account, in which case a trusting relationship has already been established, and they might not suspect anything. Social media users may therefore not be aware that they have been chosen as cybercriminals' next victim because of their susceptibility, but this phenomenon is becoming more prevalent on these platforms.

Previous scholarly work primarily attributed phishing attacks to a lack of cybersecurity interventions and weak security, while more recent literature significantly focused on psychology and the human factor being the biggest contributors to SE attacks. These studies included Motivational and Psychological Triggers in Social Engineering (Kancherla, 2020), the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures (Siddiqi et al., 2022a), and Internet-based Social Engineering Attacks, Defenses and Psychology (Longtchi et al., 2022), to name a few.

Researchers have conducted in-depth studies on the effects of phishing attacks on organisations, but there has been scant research on how they affect social media users and the perceived consequences thereof. Therefore, a research gap potentially exists between theoretical frameworks and the theories being applied to humans in practical cyberattack situations.

The aim of this study was to explore the impact of cyberattacks and social media users' experiences of the phenomenon. Furthermore, to explore angler phishing attacks on social media users in South Africa, through determining the prevalence of angler phishing attacks, investigating strategies and techniques that cybercriminals are using to successfully execute these attacks. Additionally, to discover the experiences, perceptions and behaviours of users who fall prey to these deceptions. The impact can vary for different people depending on the extent of the attack. However, there are always ramifications associated with successful phishing attacks, including financial loss, diminished brand trust, anxiety about future social media interactions, and guilt over letting one's guard down, among others. Lastly, the study aims to look at practical interventions that social media users and businesses can apply to prevent future attacks.

1.4 Research questions

This research aimed to explore South African social media users' experiences of angler phishing attacks. Based on the research goal and title, the following research questions were formulated:

- What is the prevalence of angler phishing?
- What strategies and techniques are cybercriminals using to successfully execute angler phishing attacks?
- What are the experiences, perceptions and behaviours of users who fall prey to these deceptions?
- How do personality traits contribute to user behaviour, information processing and phishing susceptibility?
- What practical interventions can social media users apply to protect themselves from future attacks?

1.5 Rationale

The significance of this study can be assessed in the cybersecurity theory and behavioural psychology domain. As stated, extensive research has been conducted on various types of phishing, and this paper aims to contribute to the controversial conversations and existing literature base with a refined focus on social media users' experiences with angler phishing as a growing trend in SE.

The significance of the study is that it will provide awareness that angler phishing is the next big cybercrime, and although it is not prevalent yet, it is worth noting because social media will continue to grow with various new platforms constantly emerging (i.e., TikTok) and individuals and businesses will try to keep up to remain relevant. This ultimately leads to an increased social media footprint and potential recklessness in behaviour during content creation and poor security literacy.

Organisations are adapting to the evolving needs of consumers and aligning with digital trends and strategies that can get them closer to consumers. Gone are the days of traditionally contacting businesses through call centres. In fact, businesses and brands have taken advantage of this new form of communication to interact with their consumers, and to enable customer queries and feedback for marketing purposes (O'Hagan, 2018). The benefits of using social media have been efficient turnaround on customer queries, creating feedback loops, and growing brand loyalty by engaging with and meeting consumers where they are.

However, there are several drawbacks. Because of the rising use of social media among both businesses and individuals, cybercriminals have discovered new opportunities for deceptive schemes. Social media lacks face-to-face communication and is non-verbal, making it difficult to read social cues (O'Hagan, 2018). It creates a false sense of trust between users, which makes users susceptible because it is likely that once a relationship with a certain business or brand has been established, consumers automatically feel comfortable providing some personal information via direct messaging, which phishers use as bait.

Businesses in South Africa stand to gain from this research in several ways, including how they manage interactions with consumers on social media platforms, the security interventions they can implement to assist consumers, and how they can inform and put strategies in place that make consumers more security conscious. Ultimately, improved technology protects the organisation, but it does not protect consumers from cybercriminals' psychological manipulation.

This study aimed to achieve the following theoretical and empirical research objectives:

1.5.1 Theoretical significance

- Review the literature on the definitions and theories of angler phishing and social media.

- Review the literature on the key role behavioural psychology, personality traits, user behaviour, and information processing play in phishing susceptibility.
- Review the literature on phishing's impact on social media users.

1.5.2 Empirical significance

- Investigate angler phishing attacks' impact on social media users.
- Add to theoretical frameworks based on validated data.
- Conduct an exploratory study and assess the framework's applicability to new and emerging phishing trends.

1.6 Delimitations of the study

The study was delimited to the following:

- There are many types of phishing attacks, and this paper focused on angler phishing.
- In this study, the focus was only on users based in South Africa.
- The study focused on social media users' (individuals) experiences of angler phishing attacks and not the impact on businesses.
- Through the interviews that were conducted and based on the outcome, the study aimed to prove the theory that there is an emerging angler phishing problem in South Africa.
- A qualitative methodology was followed to conduct the study.

1.7 Definition of terms

The following are important definitions to note in the context of this study:

Angler phishing occurs when cybercriminals use direct messages on social media platforms to lure someone into taking a deceptive action, for instance, by clicking a malware link to complete one's details (El et al., 2022).

Social engineering is the art of getting users to compromise information systems. Instead of technical attacks on systems, social engineers target humans with access to information,

manipulating them into divulging confidential information or even carrying out malicious attacks through influence and persuasion (Wang et al., 2020).

Social media: social media platforms are internet-based channels that allow users to opportunistically interact and selectively self-present, either in real-time or asynchronously, with both broad and narrow audiences who derive value from user-generated content and the perception of interacting with others (Carr & Hayes, 2015).

Social media users: there are no academic definitions of a person who uses social media. However, for the purpose of this study, a social media user is defined as anyone who owns any form of social media platform, including but not limited to Facebook, Twitter (X), and LinkedIn.

Personality traits can be described as distinct characteristics that make up an individual's thoughts, behaviours, habits, and emotions (Frauenstein & Flowerday, 2020).

Openness - Openness to experience is the desire to seek out new experiences without anxiety and an appreciation of different ideas and beliefs (Parrish et al., n.d.). They have a vivid imagination and prioritise learning (Frauenstein & Flowerday, 2020).

Conscientiousness - People who exhibit Conscientiousness are upright, reliable and diligent (Frauenstein & Flowerday, 2020). They tend to follow the rules, are law-abiding citizens and hardworking (Brewer, 2019).

Extraversion - Is the personality trait associated with enthusiasm (Frauenstein & Flowerday, 2020). They tend to be sociable, energetic, talkative, thrive off energy and have dominating personalities (Brewer, 2019).

Agreeableness – They have a high tolerance and tend to go along with others, often go along with other people's opinions instead of asserting their own (Brewer, 2019).

Neuroticism – People associated with neuroticism tend to frequently experience negative emotions such as shame, guilt, humiliation and sadness or anger (Brewer, 2019). They

typically have low self-esteem, are anxious and easily irritable (Frauenstein & Flowerday, 2020).

Information processing is the processes through which individuals use their cognitive ability to process information based on previous assessments, theories, backgrounds, social cues, and the continuous stimulation of their information environment (Wood & Vedlitz, 2007).

Heuristic processing – involves applying judgemental shortcuts and can include the use of visual cues to process information (Lee & Lin, 2022).

Systematic processing – this form of information processing requires more cognitive application as it exerts paying attention to detail, profound thinking and intensive reasoning (Lee & Lin, 2022).

1.8 Assumptions

For this study, the following was assumed:

- Current phishing frameworks are impractical or do not extend to victims outside an organisational context.
- Literature has not fully investigated the psychological impact of phishing attacks on average social media users, only the impact on businesses.
- Participants would have experienced a form of angler phishing attack through social media platforms.
- South African businesses do not offer sufficient educational campaigns on cybersecurity when it comes to social media and ensuring their consumers know the basics.

The study aims to explore angler phishing attacks on social media users in South Africa, through determining the prevalence of angler phishing, investigating strategies and techniques that cybercriminals are using to successfully execute angler phishing attacks. Additionally, discover the experiences, perceptions and behaviours of users who fall prey to these deceptions.

1.9 Chapter outline

In summary, Chapter 1 for the study. The reader was introduced to the history of the internet and how that led to a surge in cybercrimes and, eventually, the increased use of social media. Further, it indicated potential challenges that social media users encounter from a phishing perspective, and provided evidence that this is a growing trend in cybercrime. Therefore, the study was worth conducting since scant literature exists on social media users and the concept of angler phishing. In addition, the chapter outlined the research questions, rationale, delimitations of the study, clear definitions, and assumptions of the research.

CHAPTER 2: LITERATURE REVIEW AND THEORETICAL FRAMEWORK

2.1 Introduction

This literature review begins by looking at the history of phishing and providing definitions of the top five phishing attacks that are emerging trends in the current era. A closer look is then taken at angler phishing and why it is emerging as one of the most perilous phishing acts despite being one of the most underwritten areas in SE literature to date. This is followed by a breakdown of two key elements in understanding cybercriminal behaviour: the strategies and techniques and the motivations for why criminals commit these crimes.

An exploration of global trends is provided, with examples to show that angler phishing is a manifesting problem. Following this, this trend in South Africa is discussed. This information leads to an understanding of the behaviours and experiences of those who have faced phishing attacks and the consequences and the impact thereof on users and businesses.

The theoretical frameworks proposed to prevent phishing attacks are explored and analysed. This chapter also describes whether these frameworks have been validated and accepted by scholars and are relevant to the current study. Lastly, a conceptual framework is proposed after the theoretical framework has been explored in order to unpack the different constructs in the model and offer propositions to measure and determine whether the conceptual framework and models are viable.

2.2 Definition of phishing and background

The term ‘phishing’ first originated in 1996 when hackers were stealing passwords from the accounts of American online platform users (Ollmann, 2002). Just like the anglerfish described earlier, scammers set out hooks to ‘fish’ for passwords and financial information from the ‘sea’ of internet users (El et al., 2022). Decades later, phishing remains one of the most perilous topics in cybersecurity based on its advancements over time.

Phishing prevention programmes in organisations and literature have focused on training users to spot phishing emails, fake websites, and bogus links, but social media platforms’ vulnerability to phishing attacks has been neglected. This raises the question of whether the

same traditional criminal tactics are being used for social networks. According to Proofpoint (2022), the top five most common phishing attacks include:

1. Email phishing – the most popular form of phishing. This attack still uses emails to impersonate organisations on fake domains. Links are infiltrated with malware, which gets stored on the user's device and monitors for credentials (El et al., 2022).

2. Smear phishing – this approach uses open-source intelligence to gather information. Companies are also active on social media and have websites that are open to public domains, so cybercriminals target people in the organisation using their real identities to send what seems like legitimate emails (Alkhalil et al., 2021).

3. Whaling –known as the 'CEO fraud'. In this instance, cybercriminals use social media or websites to impersonate the CEO or senior management using a similar email address. These threats often involve extortion, requiring signoffs and fake tax returns. It is important that people who are exposed to these emails always double-check procedures and question whether there is a change in tone and behaviour from the usual procedures adhered to (El et al., 2022).

4. Smishing and vishing – smishing entails sending a message and asking someone to take a form of action, typically through a link, when malware gets installed onto the person's device. Short for 'voice phishing', vishing entails deceiving people telephonically to divulge sensitive information (Alkhalil et al., 2021).

5. Angler phishing - The increased use of social media by legitimate businesses to communicate with their consumers led to the emergence of angler phishing in 2015 (O'Hagan, 2018). Angler phishing is built on the premise that users have a two-way trust relationship with brands they purchase, and as a result, cybercriminals use this to their advantage and create fake profiles to mimic and pose as legitimate businesses.

Spear phishing and angler phishing appear similar, but certain characteristics distinguish the two, making them two different types of phishing attacks. Table 1 provides a detailed breakdown of each mode of phishing.

Table 1: Steps of phishing modes

Steps	Traditional	Spear	Angler
1	Obtain email address	Collect information on victim from open source intelligence (could also buy profile on dark net)	Pick a brand Create false social media account
2	Create blanket email ("your account will be limited please respond now to save it")	Tailor email using social engineering (pose as work colleague / invoice / CEO) (pick an event/anniversary/ invoice to discuss)	Engineer brand page to replicate legitimate brand page
3	Send email	Send email	Either • Directly act as the brand • Monitor legitimate brand page and intercept
4	Assume a portion of messages will be delivered	Wait for response	Ask for account details directly or via link
5	Wait for response		

Source: O'Hagan (2018)

Phishing has become more popular on social media because social media attacks are 40% more successful than traditional email phishing scams (O'Hagan, 2018). This is likely because organisations have started introducing more awareness campaigns around phishing and educating personnel on phishing awareness, so there is a lower likelihood that traditional forms of phishing still have a high success rate. Organisations have also established threat detectors in their infrastructure to quickly identify any form of breaches or phishing attempts. Recently, reporting on phishing attempts in organisations has become very efficient, as more organisations have introduced add-ons in Microsoft Outlook for staff to report phishing mails immediately. This has been a great strategy to measure whether phishing training has been effective and identify where loopholes exist.

The sudden surge in social media phishing attacks and high success rate is attributed to several factors (O'Hagan, 2018):

- Users spend a third of their time on social media, if not more.
- Cybercriminals use minimal effort to gain personal detail accesses, including names, dates of birth, family information, email addresses and circles of engagement.
- Criminals can monitor businesses effortlessly and cheaply.
- Criminals use online digital marketing techniques as clickbait.
- People on social media are more curious and likely to click on links.
- Lack of use, application and privacy controls on social media.
- Logos and verification can easily be mimicked and is no longer an earned status.
- Social media influence 71% of consumers' buying behaviour, i.e., what is trending on TikTok, or what is the new trend among influencers?

- Users have a sense of trust and security when engaging with brands on social media. They may feel seen and connected as brands keep up with the times.
- There is a lack of cybercriminal education from the social media community; not everyone is exposed to cybersecurity education at work.
- People with low incomes do not have access to resources and are unaware of social media dangers. They therefore use these platforms carelessly and nonchalantly.

2.3 Understanding angler phishing's recent rise in popularity

As of April 2023, there were 5.18 billion internet users worldwide, which amounted to 64.6% of the global population. Of this total, 4.8 billion, or 59.9% of the world's population, were social media users (Petrosyan, 2023). Most major brands have thus switched to social media as their primary means of marketing and communicating with consumers, in turn providing criminals with a growing source of potential victims and a wealth of brands to impersonate (O'Hagan, 2018).

As an indication that cybercriminals keep evolving their techniques, in 2011, a content analysis of phishing messages indicated that messages do not contain obvious spelling or grammatical mistakes and have increasingly started to use genuine logos to deceive and persuade victims, demonstrating the sophistication in techniques that have facilitated the increase in phishing attacks (Blythe et al., 2011). In 2016, Proofpoint also witnessed a 150% increase in social media angler phishing attacks, and in the fourth quarter of 2016 alone, an astonishing 500% increase was recorded (Kinswood, 2016).

In 2009, a prominent public figure experienced an unfortunate incident when someone impersonated his Twitter account and published insensitive tweets. This resulted in a legal dispute with Twitter. Twitter then decided to launch account verification, an esteemed badge that would give blue check marks to verified accounts to signify their authenticity. Years later, Instagram followed suit and launched verification in 2014 (Lestraundra, 2023). While this may have helped reduce the extent to which people and brands were experiencing cyberattacks and getting phished, it did not stop this criminal act entirely.

The blue verification era sadly came to an end in late 2022, when the new owner and Chief Executive Officer (CEO) of Twitter, Elon Musk, announced that any user with a Twitter account could now subscribe to Twitter Blue (meaning verification), offering subscribers verified accounts with additional features (Lestraundra, 2023). This poses several security risks as it goes against the initial reason why Twitter verification was created, namely to eliminate the

personification of accounts. To add insult to injury, Twitter offers an additional layer of security, two-factor authentication to verified accounts only, exposing individuals with free accounts to greater security risks (Lestraundra, 2023).

In 2021, Pieterse wrote a 10-year review journal article documenting cyber incidents from 2010 to 2020. The article covered 74 incidents that made the news because they affected prominent South African businesses, bearing in mind that these were merely the ones that were reported. Data exposure was the number one incident affecting the public sector, while the most prevalent perpetrators were hackers, and the main motive was criminal intent. However, despite the described trends, a lack of significant research on angler phishing remains.

Based on the literature acquired, there has been limited research about angler phishing, furthermore which includes addressing the prevalence of newer cybercrimes such as angler phishing, and how the strategies and techniques cybercriminals are using have evolved to from standard mediums such as fake websites and emails to social media. Additionally, previous research has focused predominately on the consequences of phishing for organisations and not that of the individual's personal experiences and understanding user online behaviour.

2.3.1 The prevalence of angler phishing attacks

Globally, cyber incidents are well-documented in journals and research reports; however, South Africa faces the opposite dilemma. There are no formal processes or procedures to report such incidents in South Africa, making it difficult to track and report on such data. Neither the South African Police Service (SAPS) nor the National Prosecuting Authority (NPA) provide data related to regional cyber incidents (Pieterse, 2021).

2.3.1.1 Globally

Research in a recent YouMail (2023) survey reported that 78% of respondents had been targets of brand impersonation; this includes scams on social media. That translates to 200 million people in the United States (US) being targets of cybercrime. The financial services industry was the most targeted for cyber scams (51%).

In 2016, a Proofpoint report (n.d.) showed real-life examples of brands that were victims of angler phishing. An image of a fake PayPal social media account used to lure consumers

using Twitter to post their queries is presented below. The cybercriminal has imitated the original PayPal account by using the exact same logo and a handle that mimics a support account @AskPayPalCRT.

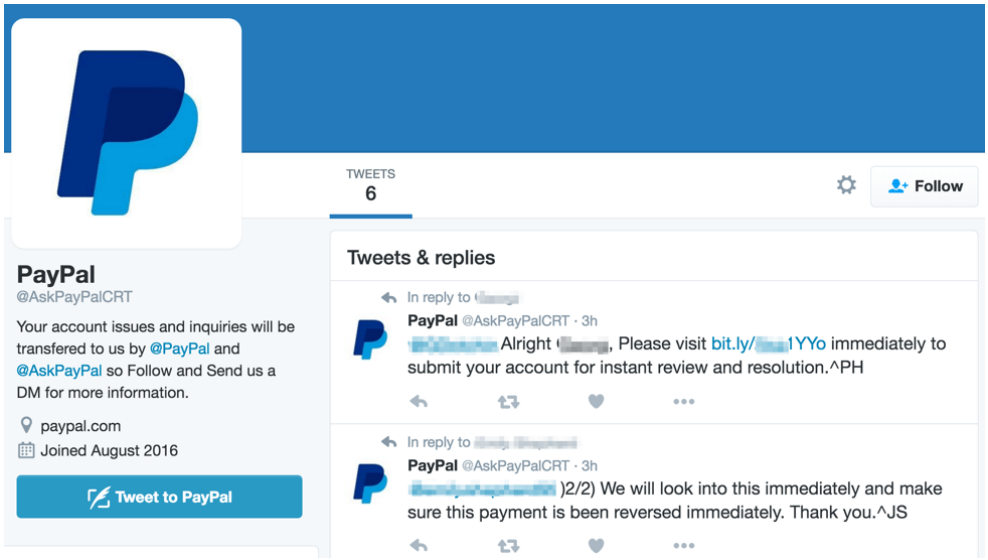


Figure 2.1: Example of a fake PayPal Twitter account (Proofpoint, 2016)

2.3.2.2 South Africa

There has been a lack of sources that have reported on angler phishing scams in South Africa. Some previous literature has indicated that South African citizens are unlikely to report cybercrimes, given their uncertainty about the SAPS's capability to handle illegal matters related to technology (Sutherland, 2017). However, this does not mean a problem does not exist. The ultimate purpose of this study was thus explorative to determine whether there is an angler phishing problem or to prove that it is emerging in South Africa by providing some relevant case studies.

In 2019, iDefense, a security intelligence associate of Accenture, investigated major cyber incidents and trends. They found several variables were causing South Africa's increasingly perilous cyber threat landscape (Mcanyana et al., 2020). Together with the findings in the iDefense report and his study, Pieterse (2021) summarised the following five elements as factors contributing to South Africa's increasing susceptibility to cyberattacks.

I. Lack of investment in cybersecurity

Socioeconomic factors, such as high crime rates, inequality and poverty, high unemployment and a shortage of skilled labour are some of the underlying reasons why businesses battle to

focus on cybersecurity investments. Developed countries have the resources to focus on cybersecurity because their economies are not collapsing or focused on making ends meet (Mcanyana et al., 2020). South Africa faces a plethora of social and economic issues, and businesses and the government often divert finances to other pressing matters.

II. Laggards in cybersecurity legislation

South Africa's adoption of cybersecurity legislation has not been as agile. The laws are outdated and inadequate to deal with brand impersonation on social media. In fact, social media may be one of the most unregulated areas. Like other laws and policies, the National Cybersecurity Policy Framework, which was adapted from international sources such as the European Union and the US, was the result of a diffusion (Sutherland, 2017). The framework was not conducive and fit for the South African climate, deemed a technology laggard, and the cultural differences between South African and international legislation were evident.

However, in 2021, the Protection of Personal Information Act (POPI Act) was launched, and the Cybercrimes Bill was also signed into law (Act 19 of 2020) (Bhagattjee, Govuza & Westcott, 2021). Despite the implementation of these laws, the POPI Act has not been in full effect, as most citizens still complain about unidentified sources accessing their personal details. South Africa needs a radical solution for adaptive regulation to combat cybercrimes and assist businesses in the excessive data leakage conundrum, and there needs to be consequent management for institutions that continue to break laws related to online data and consumers' protection.

III. Lack of awareness of cyber threats

The occurrence of incidents resulting in unintentional data exposure or compromised websites demonstrates South Africans' inexperience and lack of cybersecurity awareness when conducting business online. South Africans are prime targets for cyber threats because of this lack of understanding (Pieterse, 2021). Although large organisations often provide cybersecurity training to personnel, there is still the issue of consumers who are marginalised and do not have access to this training. These are the same individuals who have social media accounts and actively participate online but lack the resources and exposure to attain formal cybersecurity training.

IV. Surge in information technology (IT)

To keep abreast of technological trends and not remain laggards, South Africa has been trying to adopt technologies without properly assessing the country's infrastructure and measuring

citizens' technology appetite. This has led to premature implementation and technology rollouts, making these systems easy targets for breaches (Mcanyana et al., 2020).

V. Cyber attackers taking notice

iDefense analysts reported that in 2016 there was a spike in cybercrime activities in the South African underground landscape. This was attributed to several factors, including technology trends and businesses adopting new technologies, the social media footprint increasing across different platforms, and the adoption rates of technology and social media (Mcanyana et al., 2020).

2.3.2 Strategies and techniques that cybercriminals are using to successfully execute angler phishing

It is necessary to look at the fundamental problem, which is why cybercriminals commit these criminal acts in the first place, before attempting to grasp the effects of cyberattacks on social media users. Any form of crime is rooted in psychological behaviour and several academics thus refer to theories in psychology to try and explain cybercriminals' behaviour.

Allen (2021) opines that criminal activity usually has a common pattern that can be considered as a cycle consisting of four phases: information gathering, development of a relationship, exploitation, and execution. In their research, Parrish et al. (2009.) also identified that phishing attacks consist of three components: the hook (mechanism to collect information), the lure (SE incentive or tactics to provide the desired information), and the catch (information has been acquired by criminal), which relates to Allen's cycle. Figure 2.2 depicts the cycle of criminal behaviour.

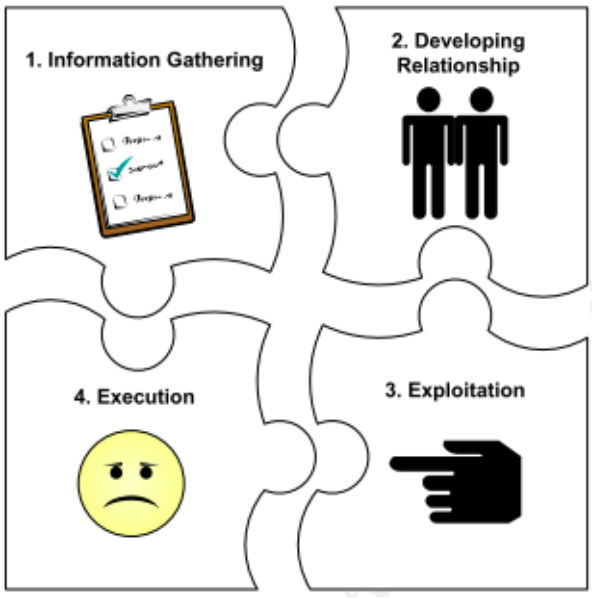


Figure 2.2: The Cycle (Allen, 2021)

I. Information gathering

Information gathering involves acquiring information about the person the cybercriminal is targeting (Allen, 2021). Cybercriminals carefully study the behavioural patterns of social media users. They may start on a single platform such as Facebook, and examine how often the person logs in, if they log in at specific types, what type of content the user posts and engages with, who the user frequently engages with, and whether the user's social media accounts are all linked (i.e., posting the same posts across all the platforms, etc.). This ultimately leads to cybercriminals then targeting users' second or third social media pages and following the same cycle in studying their behaviour.

II. Developing relationship

The information is then used to form relationships with the target or someone important that can contribute to the success of the attack's execution (Allen, 2021). In developing a relationship, the cybercriminal will use the information gathered to exploit the psychological aspect of trust (Kancherla, 2020). Once they have studied the user's behavioural patterns and engagements, they realise the relationship the user has established with businesses. This results in cybercriminals creating fake business profiles to exploit the trusting relationship someone has with specific businesses.

III. Exploitation

Using the trust already established between the user and the business, the attacker may then submit an instruction, asking the user to send their personal details, or they send a

compromising link that requires users to enter their personal information, including passwords, among other information.

IV. Execution

Once the user takes any step in actioning what the attacker has requested, the crime has been successfully executed.

2.3.1.1 Motivations

Allen (2021) identifies four types of motivations for humans to commit SE attacks:

a) *Financial gain* – various factors can lead to a fixation on money (Allen, 2021), including debt, poverty, greed or even syndicate operations. As indicated below, the primary reason behind cyberattacks in South Africa is criminal intent, namely to extort money from individuals.
b) *Self-interest* – wanting to alter information about family, friends, or acquaintances. Personal reasons drive this behaviour.
c) *Revenge* – for personal reasons, the cybercriminal might want to target an associate, colleague, or organisation for vengeance.
d) *External pressure* – external pressure is experienced by friends, family, and organised crime, for all the above reasons.

In South Africa, Pieterse (2021) discussed additional motivations and found that the most common motivation for cyberattacks was criminal intent (39.19%). Economic intent constituted 21.62% of incidents, and 16.22% was political. The two least common motives were accidental (12.6%) and fun/personal (10.81%) motives.

2.3.1.2 Techniques

Cybercriminals depend on various techniques to carry out a SE attack. Allen (2021) mentions techniques that are either human-based, which relies on interpersonal relationships, or computer-based, which is technology-dependent. Other techniques have been excluded from this discussion to maintain a focus on the purpose of this study.

Depending on the type of attack, these can be grouped into either human-based or computer-based approaches, and include direct approaches, being a helpless user, an important user, technical support channels, reverse SE, using marketing, sabotage, or support and lastly,

email, website, and phishing. Ultimately, fraudulent content is created strategically to invoke human emotion (e.g., fear or excitement) and stimulate cognitive abilities with the intention of reinforcing persuasive principles (Frauenstein & Flowerday, 2020). The strength of persuasion techniques lies in the vulnerability of human behaviour and phishers' ability to take advantage of victims' environment, whether it is linked to political affairs, religion or economics, as long as it elicits a response from the user (Frauenstein & Flowerday, 2020).

In their research, Frauenstein and Flowerday (2020) highlighted six fundamental principles of persuasion coined by Cialdini (2007):

1. Reciprocity – messages on social media are made to seem urgent and often come from a trusted source but are rather hoax messages. These require a form of action where a user may feel obligated to share to "warn others".
2. Commitment or consistency – this principle is based on the premise that after an individual has dedicated themselves or made a commitment to a specific cause or idea, they want to honour it at all costs to avoid shame and guilt. This is further driven by personal and interpersonal pressures to consistently fulfil that commitment.
3. Social proof conformity – this entails copying the actions of people in a group.
4. Authority – the primary method employed in phishing attacks. Key messages come from senior leaders and C-suite executives, and they seem legitimate because they are from a trusted source.
5. Liking – social media provides functionalities such as 'likes' to indicate support for posts or certain campaigns.
6. Scarcity – these messages incorporate 'scarcity' by deploying urgency and putting the user under pressure. Urgency messages can often have severe consequences for the user if they do not fulfil an action/instruction by a certain timeframe.

It is important to note that persuasive techniques play a significant role in the success of SE attacks, and the context in which they are received by the user may also have an impact on their success, as it is difficult to tell which persuasion techniques users are likely to fall victim to (Frauenstein & Flowerday, 2020). These techniques may not always be used independently, and cybercriminals often combine several techniques, which can affect the way in which the user responds.

2.3.3 Experiences, perceptions, and behavioural of users who fall prey to angler phishing attacks

Social media users tend to exhibit specific behaviours that show negligence on their end, which makes them more susceptible to being victims of phishing. They fail to implement privacy control settings, nonchalantly click on links and do not thoroughly review the content or source (Frauenstein & Flowerday, 2020). The Accenture Report (Mcanyana et al., 2020) also highlighted that 31% of South Africans thought that a cyber threat that encrypts files and demands payments was a Trojan virus, and more than 50% were unaware of multifactor authentication or what benefits it entails. This again proves the lack of cyber and digital literacy in South Africa.

2.3.4 The consequences for users who have been victims

Being a victim of any form of phishing could have severe consequences. There can be serious emotional and psychological impacts, leaving users feeling helpless and questioning how they could become a victim of phishing, especially when individuals consider themselves to be alert. It may also break the trust that an individual has established with a brand. Phishing victims are often tempted to end their relationship with the brand, and they consequently experience a loss by parting with a brand they trusted for years.

In some instances, being phished often leaves users with financial losses because cybercriminals were able to successfully access personal information and retrieve a user's hard-earned money. Some businesses are unwilling to compensate for this loss because the user may have willingly shared their personal information. Victims can also experience a physical impact, with a sense of their personal space and information being violated and dealing with the repercussions, potentially making users physically ill.

2.3.4.1 Business and brand impact

Businesses' interest in gaining an online presence became an important strategic directive when consumers started moving online. O'Hagan (2018) highlights that organisations started brand communities on social media because studies have shown the formation of brand communities helped promote brand trust, built stronger brands, increased engagement and showed an increase in new consumers. Consequently, consumers found value since they received information quicker, which ultimately reflected a positive outcome on the brand's

reputation. Additionally, consumers could engage with each other, creating social cohesion and showing brand loyalty.

However, what happens when brand impersonation takes place, and an organisation is faced with a repletion of consequences to deal with? Brand impersonation has become easy to achieve, and accounts can be so similar that it is sometimes indistinguishable from the legitimate brand (O'Hagan, 2018). One study found that brands and organisations do not actually report such cybercrimes to avoid reputational damage and publicity problems (O'Hagan, 2018). Organisations want to maintain a positive reputation with the consumers they already have and potential new consumers. However, it could potentially be a weakness if companies are not open and transparent with consumers. Consumers want to know what they are dealing with so they can always exercise their right to choose where their loyalties lie.

One major consequence for businesses is always revenue loss. Attacks on users have major financial implications for businesses, and not just the users. There are indirect costs, such as money and effort spent to reclaim the business's identity. Investigations to ensure other fake accounts do not exist are also costly, and consumers no longer wanting to use online services out of fear has a ripple effect, with redundant services not being utilised but impacting operational costs.

2.3.5 Practical interventions that social media users and businesses can apply to protect themselves from future attacks

Numerous scholars have noted there is no effective way to prevent a SE attack. Despite all the technological controls that organisations can implement to prevent attacks, these could potentially only solve computer-based approaches and not the most vulnerable factor in SE, which is human weakness. Nevertheless, this does not negate the need for or discourage measures to reduce the likelihood of an attack occurring.

2.3.5.1 Social media users

The following are practical interventions that users can apply to avoid future attacks; firstly, setting up two-factor authentication; this is a layer of protection that requires a second method of identity verification. Users need to apply a cautious mindset; be more sceptical of unsolicited messages, especially those requesting personal information, always verify the source, be more alert and security-conscious: if a link looks suspicious, it probably is. Furthermore, it is

important to self-educate, become educated on phishing and spam, typical attacks, and styles. The more users learn, the better they can educate others. Additionally, users need to become astute to emerging technologies, the trends and how to stay equipped to negate vulnerabilities, especially in the era of social media where engagement bait has become trendy and generative AI has made it difficult to discern between the real and fake. Users also need to cultivate habits of keeping phone software and applications updated so operating systems have the latest security patches and bug fixes. Outdated applications may have vulnerabilities that attackers can exploit to their advantage. Moreover, learning to report any suspicious activity and posts on social media can help assist businesses to improve security controls.

2.3.5.2 Organisations

When consumers go into an agreement with organisations, a level of trust relationship has been established, therefore it is important that education and awareness are key to any business and consumer relationship. Educating users and helping them by providing real-life examples of what to look out for in phishing attacks and having campaigns to create awareness may reduce the susceptibility of others getting phished. Good security architecture that is built internally can also apply to social media applications. This reduces the time and resources required to protect the organisation on social media platforms. Organisations can additionally limit data leakages by managing how much information a user can provide on social media, even for legitimate businesses. Anything that requires excessive information must be reported on alternative company platforms. Furthermore, incidence response strategies should be in place for users; if they are ever under pressure, they know exactly what to do in case they receive messages that require them to act instinctively. Finally, leveraging technologies such as AI and machine learning, spam filters and others can reduce artificial or spam messages.

2.3.6 Proposition

In the previous sections, the different factors and elements that impact the relationship between the user, businesses and social media, and cybercriminals' role in phishing attacks, were explored. There has been limited research investigating the correlation between personality traits and information processing, and available research has a significant focus on traditional phishing attacks and not emerging phishing attacks, such as angler phishing and the relationships users have on social media.

It is based on these limitations that this study explored social media users' experiences, using personality traits and information processing models to understand what factors influence users' susceptibility to getting phished. This research aimed to contribute to the body of knowledge through relevant data that can show trends and validate the importance of future studies incorporating social media as one of the major platforms for digital transformation.

2.4 Analytical framework

Victims of phishing often reflect a certain type of personality associated with specific behaviours. This phenomenon has resulted in researchers trying to understand what factors influence that behaviour. O'Hagan (2018) discussed angler phishing and identified reasons for the sudden surge and the need to focus on this specific type of phishing. Additional empirical research is thus required to investigate angler phishing further and identify where the main weaknesses in social media use lie, identify which users are most vulnerable, and develop strategies for users and brands to protect themselves.

Therefore, based on this recommendation, this study identified users' susceptibility to social media phishing based on personality traits. According to Frauenstein and Flowerday (2020), this is one of the dynamics found to influence user behaviour.

2.4.1 The Big Five Personality Traits Framework

Scholars have used various theoretical frameworks in phishing research, and personality traits and human behaviour remain fundamental factors among attackers and users. Previous studies have thus investigated personality traits in phishing and have had an immense influence in the field (Amichai-Hamburger & Vinitzky, 2010; Correa et al., 2010; Moore & McElroy, 2012; Ryan & Xenos, 2011).

Personality is a key element in understanding online user behaviour (Amichai-Hamburger et al., 2002). Personality traits can address the question of why cybercriminals are driven by criminal behaviour, and it can answer the question of why some users are more likely to become victims of cyberattacks than others.

Most studies have mentioned that The Big Five is a broadly accepted model because of the consistency across several factors in research, including time, culture, and demographics (Parrish et al., 2009). It also has considerable support among personality researchers (Frauenstein & Flowerday, 2020). The model consists of five broad factors that represent

personality at the highest level of construct that advocates of the model believe can classify differences in individuals' personalities (Parrish et al., 2009).

The model comprises five dimensions of openness, conscientiousness, extraversion, agreeableness, and neuroticism, commonly abbreviated as OCEAN (Frauenstein & Flowerday, 2020). The model has undergone several improvements, refinements and iterations, and the domains can be described as follows:

Openness to experience refers to the desire to seek out new experiences without anxiety and showing an appreciation for different ideas and beliefs (Parrish et al., 2009). Individuals who reflect an openness to experience have a vivid imagination and prioritise learning (Frauenstein & Flowerday, 2020).

People who exhibit *conscientiousness* are upright, reliable, and diligent. They tend to follow the rules and are law-abiding citizens (Frauenstein & Flowerday, 2020).

Extraversion is the personality trait associated with enthusiasm (Frauenstein & Flowerday, 2020). These individuals tend to be sociable, energetic, talkative, thrive on energy and have dominating personalities.

Agreeableness is seen among people with a high tolerance, who are usually compassionate, modest, polite and can be seen as naïve because of their trusting nature. They often believe people are genuinely honest, which can be a false misconception.

People with *neuroticism* frequently experience unpleasant emotions, including pessimism, humiliation, and guilt. They typically have low esteem, are anxious and occasionally irrational.

Previous research found that the different personality factors correlate to certain behaviours that determine whether individuals fall victim to phishing attacks or are more aware. As identified earlier in the study, persuasion was one of the techniques cybercriminals used, and some research was conducted to investigate which personality types were more likely to be victimised due to persuasion. In their study, Frauenstein and Flowerday (2020) provided a high-level summary of the different findings from various studies on how different factors, such as gender and behaviour, influence phishing susceptibility based on the five identified personality traits. For ease of reference, the findings are summarised in the table below.

Table 2: Summary of personality traits and susceptibility to phishing

Personality trait	Susceptibility to phishing
Openness	High likelihood of oversharing information on Facebook
Conscientiousness	At high risk for Spear Phishing
Extraversion, Openness	More adept at spotting phishing emails
Extreme Extraversion	A greater propensity to getting phished (opposing views in a different study)
Openness, Extraversion, Agreeableness	More prone to adhering to instructions in phishing emails
Conscientiousness, Agreeableness, Neuroticism	Less vulnerable to phishing on social media

In addition to personality traits, other factors have been found to contribute to phishing responsiveness, such as competence level, use of social media management, exposure, and cybersecurity literacy. Frauenstein and Flowerday (2020) propose that although 'scepticism' is not included in The Big Five, users were less likely to fall prey to phishing victimisation if they adopted a 'trust no one' approach. This approach could, however, be limiting with regard to engaging brands and businesses on social media, depriving users of the full user experience of services being provided. Users should adopt a more security-conscious mentality and learn to process information better rather than taking things at face value.

One of the most important reasons that phishing attacks are successful is because SE is designed to exploit the weakest element in technology, which is human nature and its cognitive biases. Cybercriminals leverage the trust that users have built with businesses and their relationships with social media counterparts. As a result, they use this trust to play on the user's emotions and use persuasion techniques to instil fearful messages in users, which then trigger a chemical imbalance based on their personality traits, causing them to react. Victimisation by phishing therefore bypasses the loopholes in technology controls by manipulating human tendencies and how individuals process information (Luo et al., 2012).

2.4.2 Theory of Planned Behaviour

The Theory of Planned Behaviour (TPB) is a broadly used psychological theory to understand user behaviour in phishing. The TPB posits that the individual's attitude towards a behaviour is driven by their intention or motivation for that behaviour (Siddiqi et al., 2022). The model focuses on the intention of the individual to perform the behaviour. This study did not only focus on the behaviours of users who got phished, but rather wanted to understand their

experiences and perceptions; hence, it was important to look at different factors, such as personality, that could potentially be the driving force behind certain behaviours. Subsequently, while the TPB could be suitable for understanding user behaviour, the researcher did not apply the theory as it is limited and provides a one-sided view.

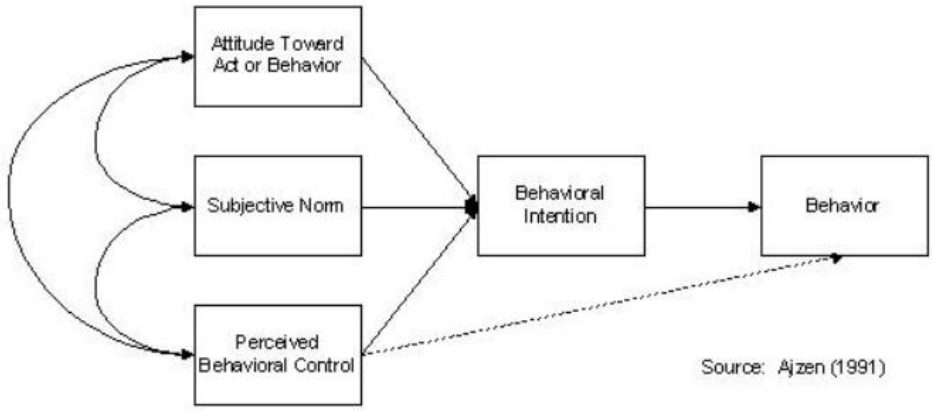


Figure 2.3: Theory of Planned Behaviour (Siddiqi et al., 2022)

2.4.3 Heuristic-systematic processing model

This study required a theoretical framework that encompasses information processing as a factor in phishing susceptibility, namely the Heuristic-systematic processing model (HSM). To understand the psychological mechanism and analyse human factors, the HSM and the personality traits model were explored as the theoretical framework underpinning this research. The HSM model is an information processing framework that stemmed from social psychology adjacent to persuasion research (Luo et al., 2012). The underlying construct of the HSM model is that when people receive persuasive messages or are being persuaded, they first try to validate the message being received by using heuristic or systematic processing.

The Elaboration Like Model (ELM), also known as a dual-process model because it combines two information processing modalities, and the Social Judgement Theory are two persuasion theories and models that are comparable (Frauenstein & Flowerday, 2020). The two models (ELM and HSM) are recognised as the most influential persuasion paradigms because they both propose two significant approaches to persuasion: the central route (systematic) and the peripheral route (heuristic). Information security research has recently praised the

HSM as a useful paradigm for comprehending phishing victimisation (Frauenstein & Flowerday, 2020).

Heuristic processing can be explained as factors embedded within or surrounding a message, such as format, length and subject (Luo et al., 2012). This can also be referred to as the visual quality of the message as it focuses on aspects such as logos, grammar, context and instructions in the message (Frauenstein & Flowerday, 2020). Systematic processing is concerned with the message's content and the validation thereof (Luo et al., 2012). Systematic processing therefore requires more effort and cognitive consciousness to accurately process messages.

Ideally, systematic processing is how we would want users to behave on social media platforms and how they should process information when receiving phishing messages. Moreover, despite this approach requiring effort and being time-consuming, systematic processing also depends on an individual's capacity to think critically, their self-efficacy and ability to validate information (Frauenstein & Flowerday, 2020). This study therefore found the proposed HSM model to be the most acceptable framework for this research.

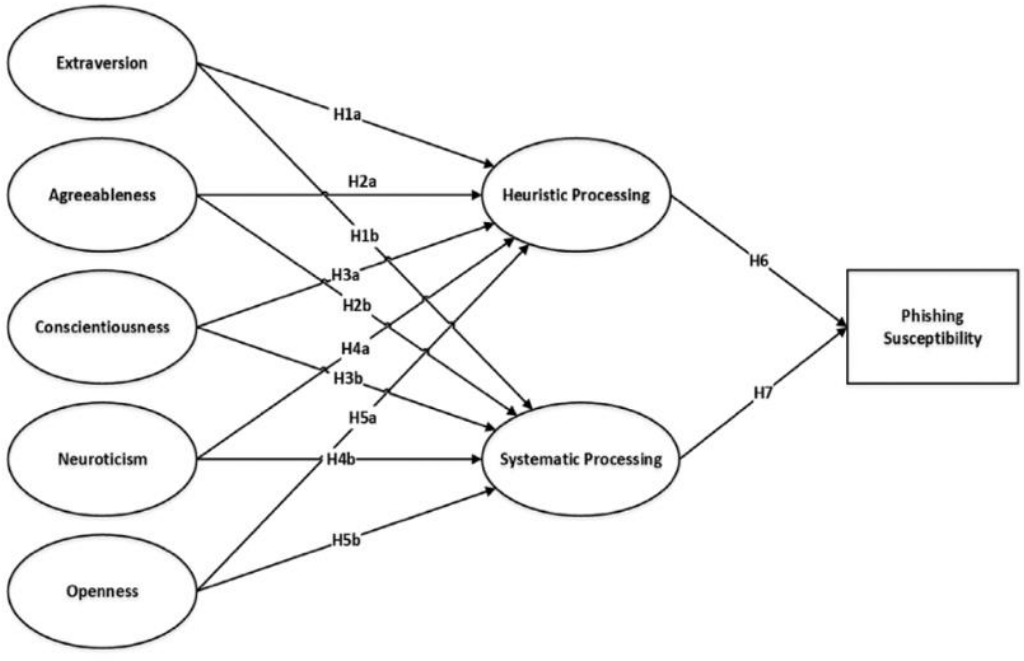


Figure 2.4: Heuristic-systematic model (Frauenstein & Flowerday, 2020)

The model consists of three major constructs, which are personality traits (The Big Five), information processing (HSM), and phishing susceptibility. The hypothesised associations in the model can be explained as follows: each of the five personality traits can either positively

or negatively influence users' information processing cues heuristically or systematically, depending on their personality. H6 and their negative association with heuristic processing are likely to increase the users' susceptibility to getting phished. H7 and their positive association with systematic processing will likely decrease the likelihood of getting phished.

2.4.4 Conceptual framework

Although the theoretical framework proposed above offers a comprehensive view of the three major constructs relevant to this study, there is a fourth construct that was excluded, namely social media. This fourth construct is important and relevant to visualise in a model because phishing can take many forms on different platforms. This research focused on getting phished on social media; therefore, the conceptual framework below is a visual presentation of the HSM framework's adaption to include a fourth construct to develop the conceptual framework.

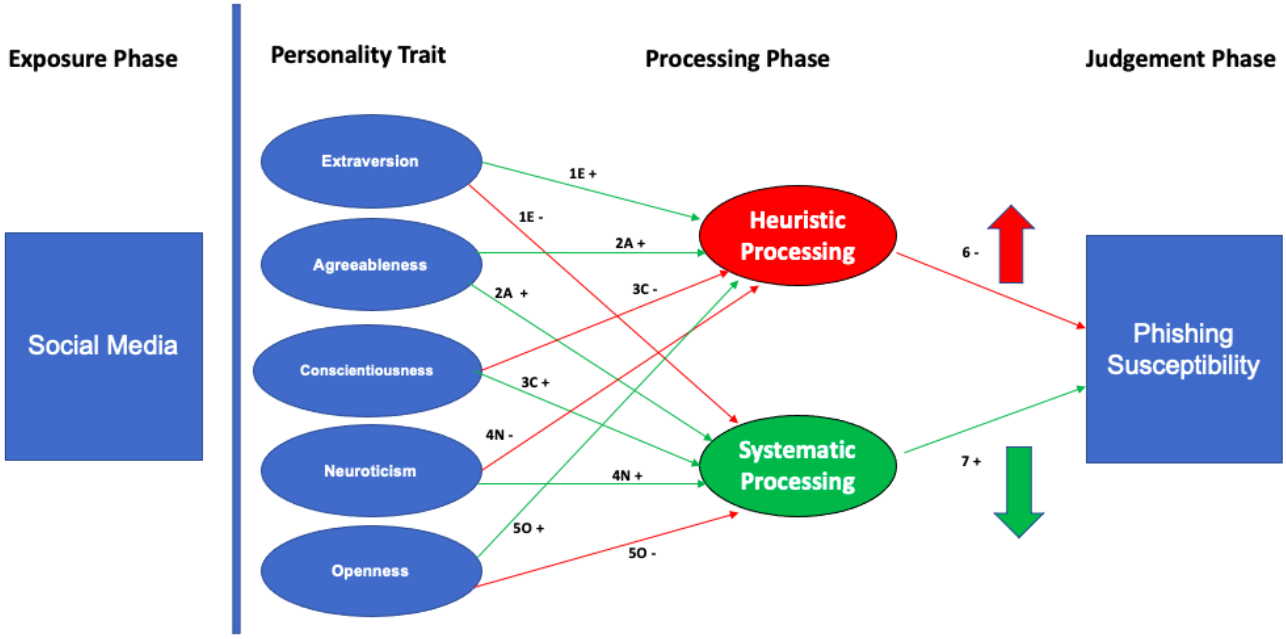


Figure 2.5: Conceptual Framework (researcher's own construct) with reference to (Frauenstein & Flowerday, 2020)

The framework consists of four dimensions:

Exposure Phase: this is considered the first stage, where a user is exposed to a social media platform that they actively use and engage with.

Personality Trait: the second phase, which is not an active step but an innate dimension, refers to the form of personality of the person exposed to the social media platform. This stage determines how users engage with information in the third phase.

Processing Phase: this is where users process the information to which they are exposed and the two information processing cues identified in the theoretical model, namely heuristic (visual) and systematic (analytical).

Judgement Phase: this is when the outcome of phase three proceeds to determine a user's susceptibility. Evidently, this research has indicated that at a heuristic level, susceptibility is high, while at a systematic level, risk susceptibility is low.

The five personality traits model as well as the HSM model were significant contributors to developing the conceptual framework by being able to identify and categorise a user in a specific personality group against the behaviours of that group and understanding how they apply information processing when accessing and actively using social media. This ultimately provides a better understanding on the increased or decreased susceptibility to phishing attempts. Therefore, by applying the conceptual framework, the research problem of understanding the experiences of angler phishing attacks on social media users can be assessed.

2.5 Conclusion of literature review

In conclusion, the literature review has demonstrated various scholarly viewpoints on phishing attacks. It has provided a comprehensive analysis of phishing victimisation from the user's point of view and business perspective.

There are limited contrasting views on phishing as the same types of findings are often reported across different studies. However, the literature review still shows that insufficient research is being conducted on angler phishing and the phenomenon in South Africa specifically; the country needs to start documenting and reporting on cybercrimes more frequently. As indicated by O'Hagan (2018), there is opportunity for future research to assess the impact of angler phishing attacks on users, therefore making the purpose of this research significant.

The described frameworks provide a good baseline to test users' susceptibility to phishing on social media. As a result, this study employed a qualitative approach to explore the extent to which angler phishing is emerging to create more awareness.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction

Thus far, this research has provided an overview of different types of phishing, with a specific focus on angler phishing, and it has shown emerging trends on social media to outline how potentially disruptive angler phishing can be. The literature provided insight from previous studies; however, these were all based on traditional types of phishing with minimal focus on angler phishing and social media as an important construct. The literature revealed a gap in this area and empirical research is still required to further unpack angler phishing. The need to explore whether current acceptable theories and frameworks would be applicable and investigate whether enough groundwork has been established to understand human behaviour and how social psychology and the applicability of information processing ultimately could alleviate phishing susceptibility was emphasised.

Therefore, an opportunity to explore this concept by bridging theory with practice and exploring real-world experiences provided the research with the prospect of understanding social media users' experiences of angler phishing attacks. Strategies businesses can employ to strengthen cybersecurity controls when engaging and providing services to consumers on social media platforms were described. An opportunity to test the four constructs presented in the conceptual framework (social media, personality traits, information processing and susceptibility to getting phished) also determined whether the theory was viable.

The research methodology section presents the research paradigm and approach used to test the framework, collect data, conduct the analysis, and the identified population for participation in the research. Lastly, potential limitations and issues with the identified research approach are also addressed.

Therefore, this chapter assesses the methods and procedures used to investigate the HSM framework with a population and sample of social media users in South Africa. This explorative study on angler phishing experiences used a qualitative research methodology.

3.2 Research paradigm

A paradigm (meaning 'pattern') can be defined as the philosophical worldview of the researcher. It collectively influences researchers' perspectives, thinking and beliefs, and determines how research should be interpreted (Kivunja & Kuyini, 2017). A paradigm informs researchers' ideologies and attitudes to interpret the world and the beliefs that shape how they act in that world. Paradigms are crucial because they are an essential factor that outlines what, why and how research should be conducted (Kivunja & Kuyini, 2017).

Theorists of paradigms (Lincoln & Guba, 1985) established that a paradigm should include four dimensions: a) epistemology, defined as the knowledge and truths of our realities in the world; b) ontology, defined as the assumptions we make in order to justify our beliefs; c) methodology, the logical and natural process of the research being conducted; and d) axiology, defined as the philosophy of right and wrong concerned with the ethical issues of research. According to Grix (2019), paradigms guide broad research approaches, which can be positivist or interpretive approaches. Tenets of the interpretive paradigm can find its traces in qualitative methodology. Several theoretical perspectives underpin qualitative research, such as constructivist-interpretive, critical, post-positivist, post-structural and feminist, or qualitative research can alternatively be underpinned by specific research approaches, namely phenomenology, grounded theory, ethnography, and case studies (Moerane, 2016).

The interpretivist paradigm was adopted as the chosen paradigm that underpins this research. The rationale behind this choice is that interpretivism allows for complex issues, such as individual behaviour, to be studied, and the problems being explored ultimately concern people more than technology (Gichuru, 2017).

3.3 Research approach

There are several approaches researchers can apply during data gathering and analysis to develop a literary representation of the real-life human experience. It has been demonstrated

in literature that qualitative research methodologies allow researchers to dive into concerns of meaning, study social practices and processes, identify obstacles and promote change, and ascertain the causes for the success or failure of interventions (Moerane, 2016). Qualitative research provides a natural language to understand complex human affairs by using words and themes to tell a story.

To answer the questions associated with this research, the participants needed to have an opportunity to engage and share their lived experiences outside of what the literature has presented. The act of transcribing lived experiences also validates information from the literature and grants researchers an opportunity to listen without preconceived philosophies. Hence, it was important that this study ensues a qualitative methodological approach which would be suited for this study.

According to Busetto et al. (2020), qualitative research is the study of the nature of phenomena, including their quality, manifestations, or perspectives. Additionally, the data collection method most associated with the qualitative approach meant the data sources could be frequently reviewed to clarify what participants meant as opposed to making incorrect assumptions and possibly manipulating data.

This study used the phenomenological approach associated with qualitative research to contribute to the body of knowledge by interpreting the constructs in this study of the individuals' lived experiences.

3.4 Research design

Phenomenology, known as both a philosophy and a research method, can be traced back to the writings of Edmund Husserl (1913/1966) (Prosek & Gibson, 2021). Van Manen (2017) described it as the study of the fundamental, experienced, pre-reflective, pre-predictive significance of an event. To simplify, phenomenology is used to describe the meaning of phenomena as opposed to interpretations of phenomena (Prosek & Gibson, 2021).

A qualitative and phenomenological research design was a relevant strategy for this research because it sought to understand social media users' experiences of angler phishing attacks. To understand 'experiences', only the people who have lived an event can explain it in their own words, share their emotions, and what it meant to them when experiencing this phenomenon.

The qualitative research approach provided this study with the following advantages:

- The researcher engaged with the participants directly in the data collection process. This allowed for a dialogue conversation to occur, making participants comfortable in the process, and it could lead to unexpected topics emerging.
- It allows participants to engage with the researcher, ask questions and clarify terms with which they are unfamiliar.
- It allows the researcher to clarify information in the data instead of making assumptions.
- It provides flexibility and experimental analysis.
- The results can further be explained to other audiences who do not understand angler phishing.
- Qualitative research strategies provide various data collection options; however, for this research, individual interviews were conducted in a comfortable setting with participants, and they were not pressured to respond in a group setting.

Qualitative research also has disadvantages that may prove limiting to this study:

- Researchers may have preferences and filter the data to influence the outcome of the study so that it reflects their own preferential biases.
- Qualitative studies are not easy to adopt in other research constructs.
- Readers of statistical data may have difficulty absorbing the value of the content.
- This approach may lack proper reflection on the issue since it includes only a small sample population.

3.5 Data collection methods

The purpose of data collection is to gather supporting evidence from participants to sustain the integrity of the study by providing examples of their lived experiences. The primary data collection method for this research was interviews with social media users who indicated an interest in participating in the study. Interviews provide the key benefits of allowing interactions between humans and probing to dig deeper during the interview (Guest et al., 2006). Comparably, interviews are known to provide insights into subjective experiences, opinions, and motivations (Busetto et al., 2020).

There are mainly two types of interview formats: structured interviews follow a stringent interview format, and semi-structured interviews are more adaptable and allow for probing scenarios and further engagement. To gain an in-depth understanding of participants' experiences, a semi-structured interview approach with open-ended questions was preferred for this research. According to Guest et al. (2006), at least six participants are needed for phenomenological studies; however, if more participants are willing to participate, they should be included to enrich the data. This study aimed to include as many variations of participants as possible, so there was no intention of recruiting a minimum number of participants deemed acceptable for a phenomenological study.

3.5.1 One-on-one interviews

Due to the severity and complexity of the study's topic, other data collection methods, such as focus groups, were not suitable to preserve the confidentiality of the individual participants. Therefore, semi-structured one-on-one interviews were the most appropriate method. One-on-one interviews have several benefits, such as the participant being comfortable enough to express their true feelings, the participant establishing a level of engagement with the researcher that is comfortable for them, and participants are not in a group setting and do not have to be swayed by the opinions and beliefs of other participants. Unfamiliar concepts were also thoroughly explained using this approach, such as angler phishing, what personality traits the participants associated with, and information processing.

Open-ended questions were asked, and participants had an opportunity to provide detailed responses of their experiences pertaining to the constructs of the study. All interviews were conducted in English, but in the event participants were more comfortable expressing themselves in another language, the transcripts were translated. For instance, some participants responded to certain questions or made statements in IsiZulu and Sesotho to emphasise or clarify what they intended to say. The researcher was able to translate these responses into English and clarify their intended meaning with the participants because the researcher is multilingual and could understand the other languages.

All the interviews were conducted online, in a safe environment for both the researcher and participants and were recorded via MS Teams. The interviews were scheduled for a minimum of one hour to ensure enough time was provided to address all questions in the research instrument and allow participants to ask the researcher questions. To ensure the data were transcribed appropriately, consent was received from the participants to record the sessions for referencing purposes.

3.6 Population and sample

The population for this study was everyone who uses social media platforms in South Africa. There was no specific sampling for this research because the researcher did not want to limit the study to a specific group of people based on their demographics or homogeneity since the topic being investigated may potentially impact people of all ages, races, and demographic settings.

The researcher had no awareness of who has or has not experienced angler phishing attacks, and it would have been inappropriate to limit the scope. As a result, it was important that recruitment was opened to all social media users; that way, there would be cases of referrals.

3.6.1 Population

As a starting point to recruit appropriate participants, the researcher leveraged their own social media platforms (Instagram, LinkedIn, Facebook, etc.) to source suitable candidates to participate in the research if they met the criteria of the targeted population. The following message was posted on the researcher's social media platforms and was further reposted by other people to assist the researcher in the recruitment process:

"Hi all. I am completing my Masters Degree in Digital Business at WBS. I'm researching how user behaviour and social media engagements with brands potentially increase phishing susceptibility. I am looking for people who have encountered phishing attempts in the form of businesses that have been impersonated by criminals, fake business accounts or received phoney links that appeared to be from legitimate South African companies. If you have encountered social media phishing or know anyone else that may have, kindly let me know if you/they would be interested in a short interview. Referrals are welcome. All responses and participation will be recorded anonymously. Thank you"

Furthermore, the researcher also reached out to respective work colleagues and networks to participate, not on behalf of the organisation but in their own personal capacity. The researcher leveraged their own network and gained referrals from their network for the population.

3.6.2 Sample and sampling method

Non-probability sampling was used because the actual probability of the researcher knowing any victims of cybercrimes was unknown. Snowball sampling was used in this study and is a recognised and viable method of recruiting study participants not easily accessible or known to the researcher (Leighton et al., 2021). In snowball sampling, participants can be seen as recruiters of other participants, basically through a referral channel. Therefore, the two sampling methods identified as non-probability sampling and snowball sampling were applied in this study. This assisted the researcher in acquiring victims of phishing on social media platforms where they were previously unknown.

Post the snowball sampling, the study was conducted with 11 participants of which seven were acquired on social media and four were within the researcher's network. Furthermore, triangulation was conducted with one focus group to validate the accuracy of the conceptual framework. Overall, the study was conducted with eleven participants for one-on-one interviews followed by seven participants in one Focus Group, totalling the number of participants to 18 for this study. The significance of sampling is to ensure the study was not overloaded by participants as the population of interest consists of a targeted group of individuals.

3.7 The research instrument

To ensure the proper collection of data, a single qualitative research instrument was used for this study, namely individual interviews. The research instrument comprised 30 open-ended questions to allow for probing and engagement with participants. The research instrument (Appendix D) was constructed with precision, and all necessary confidential elements were applied to ensure a highly detailed dataset was obtained and effectively transcribed.

The research questions were compiled in an orderly format to not overwhelm participants. The data collection instrument was divided into different measurable constructs, namely social media, to understand participants' current usage and assess online behaviour, followed by the big five personality traits. Each personality trait included a set of its own questions, and based on the personality users identified with, only the questions relevant to that personality type were asked to ensure appropriate data were collected. Information processing also formed part of the interview guide, which provided various situational scenarios and examples that would assist in evaluating whether the participants' strength was heuristic processing or systematic processing. Lastly, generic phishing questions were posed to understand participants' digital literacy level and knowledge of security controls.

In the event the researcher was not satisfied with a response or was unclear about participants' answers, probing questions were posed to the participants, such as: 'What do you mean when you say…?', 'Can you explain further for clarity?', 'Would you please give me an example of…?' (Moerane, 2016). The research instrument was first piloted with the first two participants that were interviewed which were within the researcher's network. This assisted the researcher in a getting a feel of the interview flow and whether participants were comfortable with the set of questions in the research instrument. Participants were continuously asked if they were comfortable to proceed and were guaranteed confidentiality if there questions in the research instrument they were concerned about.

3.8 Procedure for data collection

The data collection process went as follows: first, participants were asked to provide an appropriate time and date for the interview. The necessary sessions could then be scheduled. The participant information form and consent form were sent to the participants to complete prior to the interview session. In the session, participants were briefed about general guidelines about the research upfront, and consent to record the sessions was required.

A standard research instrument (Appendix D) was applicable to all the participants, unless circumstances forced the researcher to adjust questions. The questions were designed to stimulate participants' responses and ensure the HSM framework's validity.

Some challenges experienced during the data collection process included:

i. Participants not honouring the meeting slot timeously.
ii. Having to reschedule interviews because participants had work or family commitments.
iii. Load-shedding was a challenge because interviews would be progressing seamlessly, then a participant would encounter load-shedding and not have backup power, the network would be unstable, and the researcher and participants would struggle to hear each other.
iv. Following up with participants to complete and return consent forms.

3.9 Data analysis strategies and interpretation

The strength of a qualitative study is judged based on the manner in which the analysis has been conducted (Moerane, 2016). Thus, the way in which data are analysed underpins the outcomes of a study.

To analyse any data collected through observations, interviews and focus groups, these need to be transcribed into protocols and transcripts (Busetto et al., 2020). A more detailed description of the data analysis approach employed in this study is provided in Chapter 4.

3.10 Possible limitations and challenges of the study

There are some possible limitations to the research:

First, this was a qualitative study, and the participants may not have been a sufficiently representative population to reflect that angler phishing is an emerging threat in South Africa. A future study could potentially take a quantitative approach and reach a larger group of people and potentially have a specific sample, i.e., Millennials or Generation Z.

Second, participants may not have been truthful about the information they were providing. It had to be assumed that the data being provided was truthful, and where evidence could be provided, it was incorporated into the study.

Third, not focusing on a specific industry, such as financial institutions or telecommunications, may be a flawed approach and make the study strenuous because the target population has not been narrowed down.

Lastly, participants may not have honoured the invites and withdrew from the study.

3.11 Quality assurance

Quality assurance entails research-related activities that comprise methods, tools, and resources to provide assurance and ensure quality. Qualitative researchers speak of trustworthiness, which simply poses the question, ‘Can the findings be trusted?’ (Lincoln & Guba, 1985). Several quality assurance criteria exist, but the best known and most accepted are transferability, credibility, dependability and confirmability.

3.11.1 Transferability

Transferability is concerned with applicability. In this study, sufficiently rich data has been provided to ensure transferability is applicable to future researchers.

3.11.2 Credibility

Credibility is concerned with truth value. In this study, credibility could be promoted because the interviews were conducted in one-on-one sessions. Participants also felt comfortable asking the researcher questions to clarify their understanding of concepts instead of assuming or pretending to understand the concepts discussed in this research. The participants also mentioned to the researcher that they would be truthful in their responses because they were guaranteed anonymity as part of the study. The standard process with triangulation was used to affirm the credibility of the study (Noble & Heale, 2019) .

3.11.3 Dependability and confirmability

Dependability is about consistency, while confirmability is about neutrality (Korstjens & Moser, 2018). All the research data and recordings can be made available for this study. The transcribed notes documented in the interviews are available for audit purposes. The data are stored securely, password-protected, and only accessible to the researcher or when requested by external stakeholders. All files are stored and backed up on the researcher's iCloud drive.

3.12 Ethical considerations

Ethical approval: the researcher completed an ethics training course as part of the research methodology. An ethics consent form was submitted to the appropriate ethics committee and board, and approval was granted on the premise that participants' confidentiality would be guaranteed. The ethics document addressed all the ethical issues described below.

Informed consent: All participants in this research were older than 18; therefore, no additional consent was required from parents and guardians. All participants' capacity to consent to the research was ascertained.

Voluntary participation: Participation in this study was completely voluntary. All participants were informed that no compensation would be provided for this study. All participants were informed of their right to withdraw participation at any time.

Confidentiality: No personal information of participants was revealed in this study. Pseudonyms and a numbering system were applied to each participant for all data collection purposes. A non-disclosure form was also provided.

Potential risks: This is a low-risk study, and none of the interviews intended harm or provided radical findings. No risk was thus anticipated for this study, except in terms of participants' commitment to interviews.

3.13 Summary

This chapter outlined the methodology used in conducting this research, namely the qualitative methodology. Additionally, it appropriately justified the relevance of the method and how it was applied in the data collection process while protecting the data and participants of this study. Ethical considerations were also outlined in this chapter.

CHAPTER 4: PRESENTATION OF FINDINGS

4.1 Introduction

This chapter presents the empirical findings following the interviews that were conducted with the participants. The chapter highlights the qualitative methodology that was used to analyse the data and the findings pertaining to each of the identified propositions. Additionally, the chapter details how the data were obtained and analysed, what qualitative analysis software was applied in the data analysis process, and how thematic analysis was concluded. The themes that were extracted following the analysis process are also presented.

4.2 Participant description and demographics

The study sought to explore social media users' experiences of angler phishing attacks. To achieve this aim, snowball sampling was used to source participants who had experienced these attacks. Initially, 17 individuals responded to the request to be interviewed and indicated they had been a victim of cybercrimes. Unfortunately, some respondents were based outside South Africa, and fell outside the scope of this study. Some individuals who responded to the call on social media were not actual victims of phishing but had rather experienced phishing attempts. Due to the low response rate of actual victims, a decision was made by the researcher to include non-victims as part of the study in order to get their perspectives on angler phishing. This approach was important so the research could achieve a viable sample for the data collection process and provide other philosophical perspectives from consumers.

Table 3 provides a summary of the 11 participants who participated in the study's demographic characteristics.

Table 3: Participants' characteristics

Participant no.	Gender	Area	Job/Industry	Race
1	F	Gauteng	Psychometrist	African
2	M	Gauteng	Software Engineer	White
3	M	Gauteng	Business Analyst	African
4	F	Gauteng	Learning Specialist	African
5	M	Cape Town	Digital Marketing	African
6	F	Gauteng	Tourism	African
7	F	Gauteng	Digital Marketing	African
8	F	Gauteng	Banking	African
9	F	Gauteng	Comms Specialist	Indian
10	F	Cape Town	Risk Manager	African
11	M	Gauteng	Entrepreneur	African

Initially, focus groups were not considered for this research study, but phase two in the process required an evaluation of the conceptual framework. A focus group was conducted for this purpose with cybersecurity and technology experts. Thus, in addition to the 11 participants who took part in individual interviews, one focus group was conducted with an additional seven participants.

Table 4: Focus group participants' characteristics

Gender	Area	Job title	Race
M	Gauteng	Lead Support Engineer	White
M	Gauteng	Specialist Support Engineer	White
M	Gauteng	DevOps Engineer	African
M	Gauteng	Lead Product Engineer	African
M	Gauteng	Lead Support Engineer	African
F	Gauteng	Project Manager	White
F	Gauteng	Lead Scrum Master	African

4.3 Data analysis process

In a qualitative study, the aim is to understand a phenomenon. Hence, semi-structured interviews underpinned this study to gain in-depth information on the phenomenon by allowing participants to express their experiences. This research aimed to highlight social media users' experiences of angler phishing attacks, and a theoretical thematic analysis (based on an inductive approach) was conducted. Thematic analysis is the process of identifying, analysing and interpreting patterns that have meaning, often referred to as 'themes' in qualitative data (Clarke & Braun, 2017).

Thematic analysis can be used to identify patterns within and across data in relation to participants' lived experiences, their views and perspectives, behaviour and practices. This approach offers an understanding of experiential research, which seeks to understand what participants think, feel, and do (Clarke & Braun, 2017). In Figure 4.1, Braun and Clarke (2006) outline the six phases of thematic analysis. They note that this is not a linear exercise but a recurring process that occurs throughout the phases until the entire analysis process is complete.

Phase	Description of the process
1. Familiarizing yourself with your data:	Transcribing data (if necessary), reading and re-reading the data, noting down initial ideas.
2. Generating initial codes:	Coding interesting features of the data in a systematic fashion across the entire data set, collating data relevant to each code.
3. Searching for themes:	Collating codes into potential themes, gathering all data relevant to each potential theme.
4. Reviewing themes:	Checking if the themes work in relation to the coded extracts (Level 1) and the entire data set (Level 2), generating a thematic 'map' of the analysis.
5. Defining and naming themes:	Ongoing analysis to refine the specifics of each theme, and the overall story the analysis tells, generating clear definitions and names for each theme.
6. Producing the report:	The final opportunity for analysis. Selection of vivid, compelling extract examples, final analysis of selected extracts, relating back of the analysis to the research question and literature, producing a scholarly report of the analysis.

Figure 4.1: Phases of thematic analysis (Braun & Clarke, 2006)

The data for this study were gathered using a semi-structured interview guide. The interview guide consisted of 30 questions, split over four measurable constructs, namely social media, personality traits, information processing (heuristic and systematic), and phishing susceptibility. The interview guide provided guidance on initiating the interviews and setting the scene with the participants. The interviews varied with regard to the questions' sequencing based on participants' responses, peculiarities, and dynamics. Each participant was treated as a single case, and as a result, some participants answered probing questions in addition to those included in the instrument guide to elaborate on their individual experiences.

Literature has shown a general positive consensus on using Qualitative Data Analysis Software (CAQDAS) because it enhances the transparency, validity, rigour, and trustworthiness of qualitative research projects (Gestão et al., 2020). To ensure translucence, the theoretical thematic analysis was married with a CAQDAS-based tool, ATLAS.ti version 23.4, to complete the data analysis. The software made the coding process seamless, and the data management for all the participants' transcripts was made easier. For ease of reference, ATLAS.ti is referred to as 'software' in this study, and the software terminology and concepts are provided.

The following sections provide details on the thematic analysis that was performed, including the steps taken using the software.

4.3.1 Familiarising yourself with your data

All the interviews were conducted via MS Teams, and the platform provides a standard transcript after the meeting. Unfortunately, the MS Teams transcripts are not always accurate and can contain errors, so the first step in the data analysis process was to read all the transcripts in their entirety and edit the transcripts so they accurately reflected what was discussed in the interview and got a sense of the data. This process was repeated verbatim to ensure the scripts reflected participants' true experiences and remove unnecessary inserts so the transcripts would be easy to analyse in the software.

4.3.2 Generating initial codes

The next step was to start generating codes from the transcripts. Codes are interesting features from the data that are connected to the research questions. It is important to note that the initial coding process was kept close to the participants' words and statements to not dilute their experience.

The researcher watched several YouTube tutorial videos from various lecturers and professors to gain an understanding of how to use the software effectively. Once the researcher was comfortable with the software terminology and some of the main fundamental features that were highlighted, a project was created in the software to start the analysis.

The first step was to upload all the documents essential to the analysis; this was a total of 11 transcripts. This step was followed by intensive coding processing, reviewing all the transcripts and highlighting important features, extracting, and systematically organising all the codes. Initially, 19 codes were produced through this process. A further step was taken to clean up the codes and merge codes that were redundant or did not need to stand alone in the *code manager*[1]; this resulted in a total reduction of nine codes. It is important to note that the codes were matched with direct quotations, and in some instances, an *in-vivo node*[2] was coded from the participants' transcripts. The codes were then colour-coded to show differentiation and grouping. 4.2 shows a screenshot of the nine codes.

[1] Assists in creating and managing the codes by displaying their occurrence across the different documents being analysed. It helps show the comments created by the researcher and the dates on which they were created.
[2] These are codes that have been created by directly using the participants' quotations as they are.

In summary, the code manager consisted of 11 documents and 19 codes were initially identified. These were reduced to nine codes, six code groups, 313 quotations and two network groups.

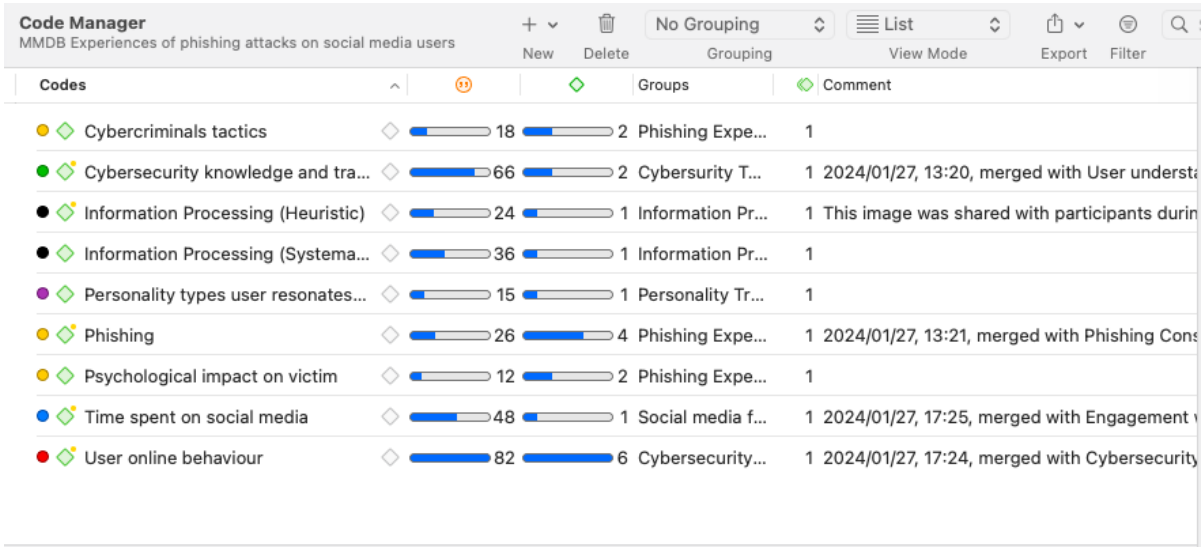
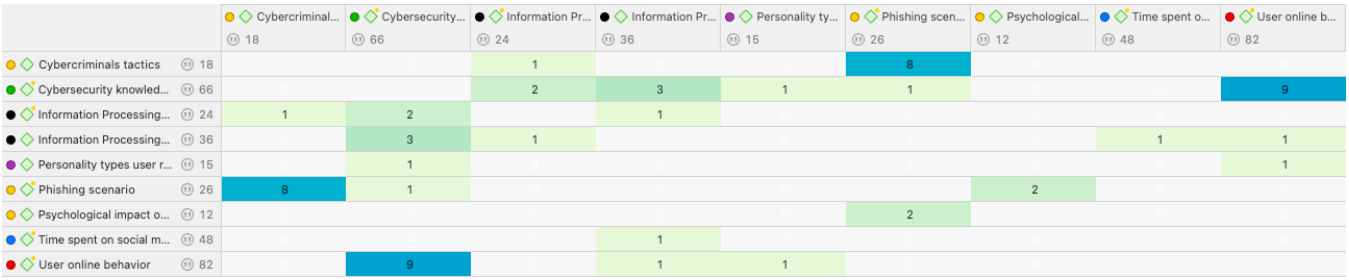


Figure 4.2: Total number of codes in the software code manager (researcher's own construct) with reference to ATLAS.ti software

4.3.3 Searching for themes, reviewing, and naming themes

The process of searching for themes commenced after certain codes were merged because they were essentially referring to the same thing; the codes that were grouped were identified as potential themes. To analyse the potential relationships among the codes, a *code co-occurrence*[3] table analysis was conducted in the software. Figure 4.3 provides a matrix of the coded segments and highlights where two or more codes appeared together in the data. For instance, in column 2, Cybersecurity knowledge and training intersect nine times with row 9 (User online behaviour), and column 6's Phishing scenarios intersect eight times with row 1 (Cybercriminals tactics). The numbers in the table indicate the number of participant quotations where the codes co-occur because they were speaking about the same thing.

[3] This is a matrix that displays the frequency of codes' co-occurrence, where two or more codes keep occurring together in a data set.



	Cybercriminal... 18	Cybersecurity... 66	Information Pr... 24	Information Pr... 36	Personality ty... 15	Phishing scen... 26	Psychological... 12	Time spent o... 48	User online b... 82
Cybercriminals tactics 18			1			8			
Cybersecurity knowled... 66			2	3	1	1			9
Information Processing... 24	1	2		1					
Information Processing... 36		3	1					1	1
Personality types user r... 15		1							1
Phishing scenario 26	8	1					2		
Psychological impact o... 12						2			
Time spent on social m... 48				1					
User online behavior 82		9		1	1				

Figure 4.3: A code co-occurrence table analysis (researcher's own construct) with reference to ATLAS.ti software

After the researcher identified the potential themes, the themes were created as *code groups*[4] in the software. Figure 4.4 illustrates six code groups that were relevant to the study's theory. In the figure, the number next to each code group indicates the total number of codes grouped into that code group, meaning these could also be sub-themes that fall under the larger theme. These themes are linked to each of the constructs included in the conceptual framework, which is further unpacked in this chapter.

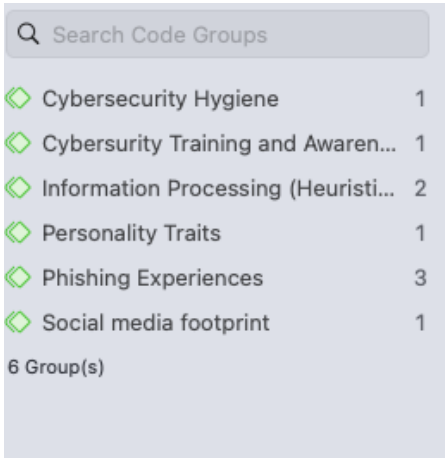


Figure 4.4: Themes that were identified from the codes (researcher's own construct) with reference to ATLAS.ti software

4.3.4 Producing the report

The final step in the thematic analysis process is to produce a research report compiled from various extracts and excerpts from the data analysis process and software. Relevant themes should be aligned with the research objectives and questions. This step is further detailed in the remainder of this chapter, where the researcher dives into each of the themes, producing findings from the data that reinforce the themes.

[4] Help organise a long list of codes into groups that can be filtered for the data.

4.4 Findings pertaining to strategies and techniques cybercriminals use to successfully execute angler phishing attacks

The literature revealed that cybercriminals use various strategies and techniques to execute angler phishing attacks. This forms part of human-based SE, where cybercriminals take advantage of human factors to infiltrate users' weaknesses. This is because human nature is susceptible, and individuals are likely to trust other human beings over technology. Research has shown that human-based SE is on the rise and happens to be the biggest threat in cybersecurity because attacks can on(Salahdine & Kaabouch, 2019).d (Salahdine & Kaabouch, 2019).

There is also a lack of awareness among users about what phishing techniques are, as they do not know what to look out for. An understanding of strategies and human-based techniques forms part of the first proposition, and the first theme that emerged focused on the deceptive tactics phishers use and how cybersecurity hygiene, which refers to how users behave online, is related to this theme. Participants answered various questions regarding their social media activity, the time spent on social media, and how they engage with content, communities, and online strangers.

4.4.1 Social media footprint

Social media is growing rapidly, with new platforms being introduced and taking over traditional mediums of communication. Having an online presence has brought communication closer to people and paved the way for individuals to meet people from all over the world. In recent years, social media has become one of the fastest platforms for generating income and is a key player in digital businesses getting closer to consumers. As a result, people have social media footprints everywhere; however, there is some question about whether being registered on a platform necessarily means an individual is using that platform. The likely answer is no. Some people are registered but not actively using certain accounts, as stated by one participant: "I try limit being on all these social platforms because it can get overwhelming" (participant 3).

For this study, it was imperative to gain insight into users' social media activity and how they show up online. Participants answered various questions to illustrate their social media presence. Figure 4.5 shows the key highlights from the interviews; the most popular social

media platform was Instagram, and users averaged four hours across their social media activity per day.

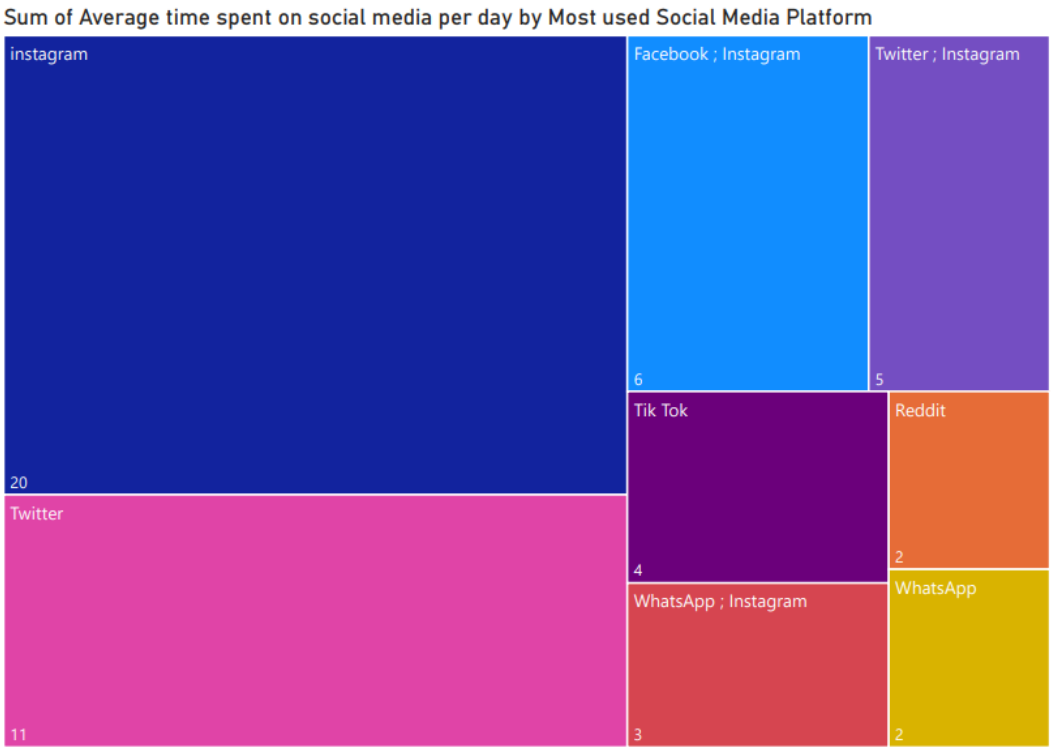


Figure 4.5: Social media overview (researcher's own construct)

4.4.2 User online behaviour

Once insight was obtained on participants' social media presence, it was necessary to understand how users behave online. Table 5 indicates that various questions were posed to understand the way in which participants interacted or responded to certain online engagements. The abbreviation 'PT' is used to refer to a 'participant'.

Table 5: Participants online engagements activity

Participant code	Do you frequently explore new websites, online communities, and pages?	Do you frequently click on unsolicited links?	Do you tend to engage or entertain strangers online?
PT 1	Yes	No	No
PT 2	No	No	No
PT 3	Yes	Yes	Yes
PT 4	No	Yes	No
PT 5	Yes	Yes	Yes

Participant code	Do you frequently explore new websites, online communities, and pages?	Do you frequently click on unsolicited links?	Do you tend to engage or entertain strangers online?
PT 6	Yes	Yes	Yes
PT 7	No	No	No
PT 8	Yes	No	No
PT 9	Yes	No	Yes
PT 10	Yes	No	No
PT 11	No	No	No

In the table synopsis, 64% of the participants said they frequently visit new websites, online communities, and platforms, while 36% said they do not. The 64% said they are generally curious by nature and open to learning and exploring new things. In comparison, the 36% said they prefer things that are familiar and remain in their comfort zones, and unless someone recommended a new website or platform, it is unlikely they would go looking for it themselves.

When asked whether they clicked on unsolicited links, 36% said yes, they did, while 64% said no, they did not. Lastly, when asked whether they engaged with or entertained strangers online, 36% said yes, while 64% said no. A closer look at the data indicates a pattern in that the same individuals who explored new forums usually clicked on unsolicited links and were likely to engage strangers online. These same individuals also happened to be victims of phishing incidents.

4.4.3 Cybercriminals strategies and techniques

When participants were asked to share their phishing experiences, it was important that they reflected on what happened during that moment and talked about the perpetrator's behaviours during the incident. Some participants expressed this was a defining moment for them, having to reflect and recall the events that led to that incident. Participants were in vulnerable states during the phishing incidents and oblivious to the attackers' techniques. Table 6 highlights some of the human-based techniques that were used based on participants' shared experiences.

Table 6: Social engineering techniques perpetrators employed

Participants	Responses
PT 3	So, it was one of those Bitcoin things and I fell for it and the person, like, made it **seem real**. They **were convincing**. I guess **I trusted** that human to a certain extent.
PT 5	I got a link that said please check out our content, this is the type of work we do, and it **seemed genuine** because they were **not too pushy**. I went on my first instinct since this is the kind of work I do on a daily.
PT 8	I felt like it was an inside job to a certain extent because the people were **so accurate, in their utterances**, in everything that you would have gone through in internal training or things like that, you would have, you would have been very **easily convinced** of what the story was. And I insisted through the person who was helping me from fraud that they need to look into their internal processes and employees because this **sounds quite legit**.
PT 9	So, I thought when I heard that, I thought, oh, wow, that's like, you know, that **sounds legit**. And it **looked like it was legit**, considering that I was now paying money, getting my money back every time I completed 5 tasks, I was getting like 50 bucks back every single time. **They almost do like some form of research on the back end**, because now that they have your name and your bank account number and whatever, they could also see who your spouse is or whatever. And they go into their own homework in the background, so that knowing that you're going to try different forms to reach out, because now you've made this huge investment. Like I was **convincing myself that it was real,** but obviously it wasn't.

One correlation that stands out is that everything either seemed “real”, “legit”, or “genuine”. This form of SE attack is the most dangerous and is classified as a social-based attack because the perpetrators leverage a relationship with the victims and use psychology and emotion to trick users’ minds (Salahdine & Kaabouch, 2019).

The participants explained everything looked convincing, and they were also convincing themselves that it was real. This shows that attackers have mastered the art of showing up genuinely, taking advantage of emotions, and knowing exactly how to manipulate victims without them even realising they are being manipulated.

4.5 Findings pertaining to understanding experiences, perceptions and behaviours of victims who fall prey to these deceptions

Great emphasis has been placed on the impact of phishing experiences on big corporates and organisations. Various organisations have implemented interventions that strengthen and protect their infrastructure against cybercriminals and potential breaches. However, little to no research has managed to delve into what is happening externally, how consumers are

experiencing attacks, and how they are being impacted by the rising cybercrime rate. In the literature review section, it was evident that South Africa was one of the countries where victims seldom reported cybercrimes because of their lack of faith in the justice system. Consequently, this leaves a major loophole where organisations fail to improve security for the consumer, the government is also not pressured to strengthen legislation on cybersecurity, ultimately allowing criminals to become arrogant.

Therefore, it was imperative that this study focused on the consumers and gave them a platform to express themselves. A key research question in this study was: "What are the experiences, perceptions and behaviours of users who fall prey to these deceptions?". This question led to the second theme, namely the psychological impact of phishing attacks. The participants expressed deep regret and strong emotions over the incidents that occurred. It was therefore important to ask the participants to put into words how these experiences made them feel.

4.5.1 Phishing scenario

In the interviews, participants were asked to share their phishing experiences in detail, and Figure 4.6 provides a summarised snapshot of what one participant went through. The participant was initially approached on WhatsApp and received "false work instructions" to complete tasks on Telegram. The participant emphasised that the perpetrators were stern and consistently mentioned that the instructions must be strictly followed. Various instructions were given to the participant to complete, followed by screenshots to prove that the tasks had been completed before proceeding to the next stage.

Participant 3, who experienced a similar phishing incident, said:

> *"…they showed me the platform they gave me login credentials; they created an account so you could see market trends. So, when I saw the site, I thought this is legit right? Then I sent the first batch, send the second batch and then there was always something wrong that I was doing. So, I sent the first R2k and he was like which account did you use? And I showed him. I told you to do it like this. Now you're going to lose your money. You need to do it like the instructions*" (Participant 3).

Despite all the investments she made, participant 9 mentioned that she only ever received one cashback payment, which was when she made the initial investment of R500 and received R650 as returns. When the participant was asked why she kept making investments despite

not receiving any further returns, the participant said she could see all the investments she kept making on this trading platform, and she could essentially see all the money on that platform, and it gave her a sense of comfort. Finally, the participant reached out to the person assigned as her touchpoint, and she informed them she was ready to cash out; she never received a response ever again. She also tried to access Telegram and received an error that she was blocked. The participant has not been able to access Telegram since the incident. In total, the victim suffered a financial loss of R160 000.

Figure 4.6: Phishing scenario (researcher's own construct)

The participant was asked if she ever pursued the matter by reporting the incident formally to the police. She explained:

> *"I did. So, I sat on it for a few days because obviously you're a smart, intelligent person who's familiar with cybercrime and all these other things. And yet here I am, being a victim, right? So, there's obviously, uh, an element of shame that comes with it*

*because you are thinking oh s*** like, how can an educated person do something so stupid? Right. So, I sat on it for a few days thinking like I was embarrassed.*

I'll be honest, I was very embarrassed by what had just happened and like I was doing all these transactions, and I didn't say anything to my husband because I was thinking that should it be a win, then all of us benefit from it and not, you know, so. But anyways, I didn't say anything, and I was actually quite far into it when I did, then raised it with him and said I think this is a scam and he was obviously very shocked by it and whatever. Which he actually said to me. He said no, I think, but you should report it" (Participant 9).

She initially engaged a private investigator who informed her the perpetrators are sometimes found, but there was no guarantee the money would be returned. She then made a conscious decision that the matter was not worth pursuing because she had already lost enough money. She let the matter go and treated this incident as a learning experience.

4.5.2 Psychological impact

Other participants also expressed their grievances and financial losses. However, what was emphasised most was the psychological impact of having been a victim of phishing. Figure 4.7 provides an *ad hoc network*[5] view that was created in the software. It provides direct quotations of what the participants felt after they fell victim to phishing attacks.

[5] This is a chain of devices that are connected to each other by using the linked neighbours in the data set.

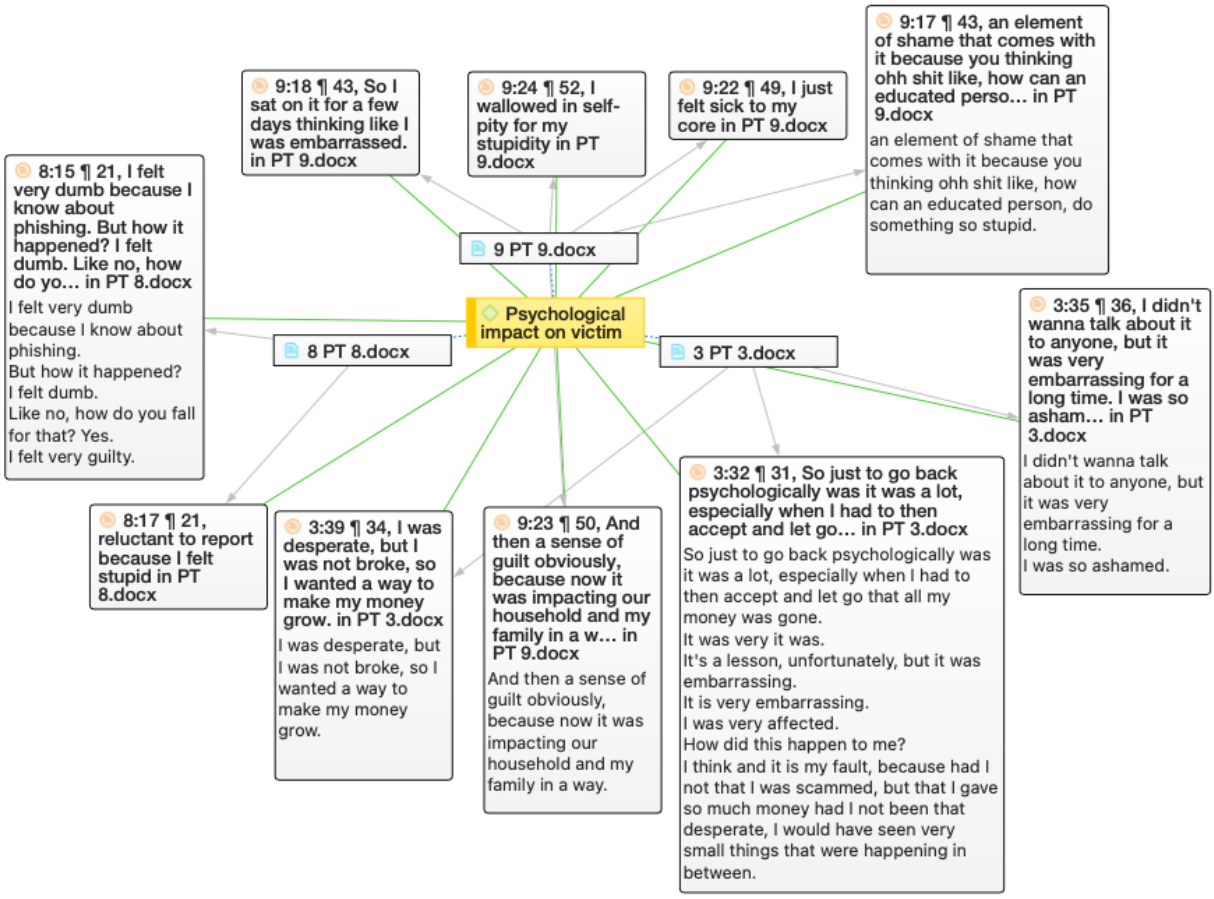


Figure 4.7: Ad hoc network showing the psychological impact on victims (researcher's own construct) with reference to ATLAS.ti software

Emotions consistently mentioned included: "I felt embarrassed, I felt so stupid, so dumb, I felt guilty, and ashamed". In all these phrases, the participants are blaming themselves for what transpired. Little retribution nor anger was directed at the perpetrators of these malicious crimes. This shows the participants were engaged in emotion-focused coping, which is when people redirect their emotions to blaming themselves (Wang et al., 2017).

4.6 Findings pertaining to The Big Five Personality Traits as a contributing factor to user behaviour, information processing and phishing susceptibility

The Big Five Personality Traits model has contributed significantly to research, helping researchers understand whether there is a link between certain types of personalities and related behaviours associated with individuals getting phished. During the interviews, the researcher provided definitions of each personality trait, namely openness, conscientiousness, extraversion, agreeableness, and neuroticism. Participants were then asked to identify which personality trait they resonated with the most. Figure 4.8 indicates the

results of participants' personality traits. The circles outlined in red were the personality traits associated with phishing in this study.

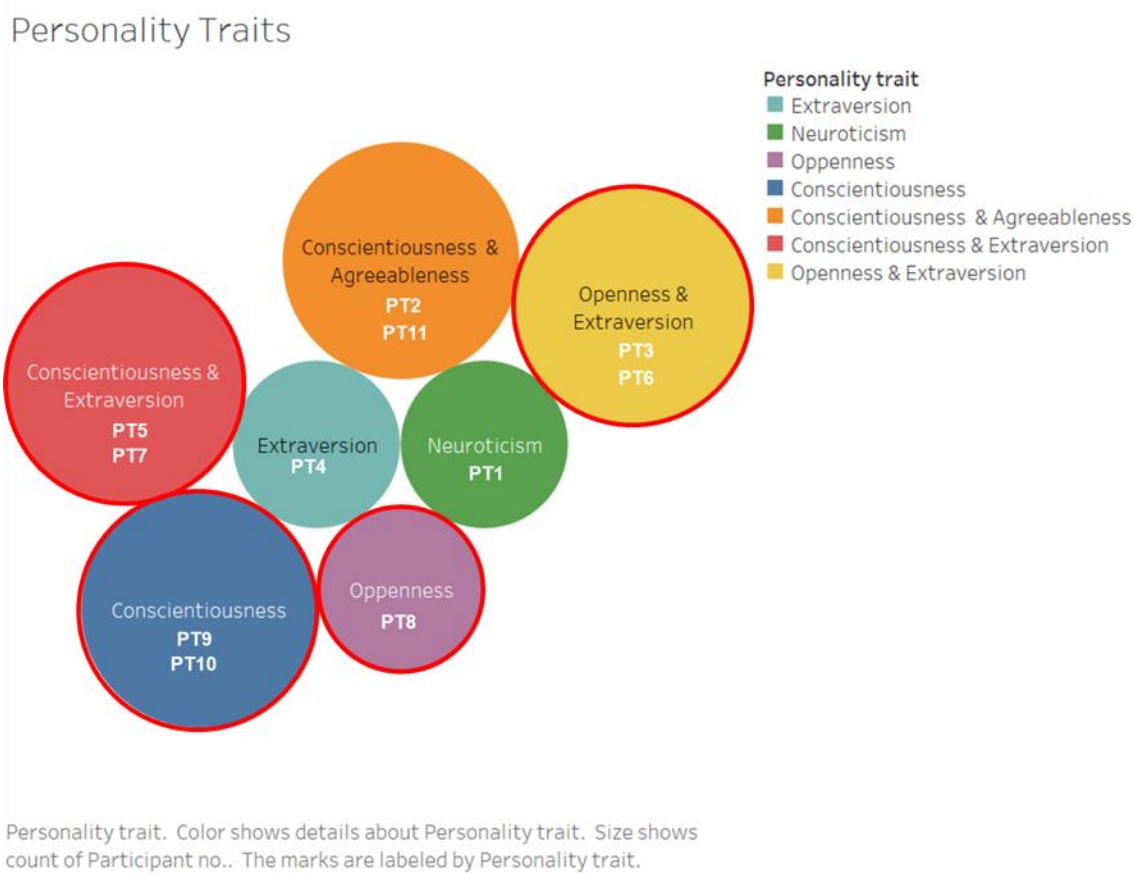


Figure 4.8: Highlight of personality traits and phishing victims (researcher's own construct)

In most cases, participants found that they resonated with more than one personality trait and felt it was a disservice only to be boxed into one. As a result, some opted to focus on the top two traits they resonated with.

Both participants 5 and 7 worked as digital marketers and their job demanded them to be extroverts, but in their personal capacities, they identified as conscientious. Participants 2 and 11 were both individual males who identified as being conscientious and agreeable. Participants 3 and 6 identified with openness and extraversion, and both said they have a very curious nature and can easily adapt to be social. Participant 8 was introverted by nature but found she identified with openness; she also mentioned that she was a more active person on social media since it does not require her to engage with people physically. Participant 1 was the only participant who effusively identified with neuroticism, while participant 4 was an extreme extrovert. Lastly, participants 9 and 10 both identified as conscientious.

4.7 Findings pertaining to practical interventions social media users can apply to prevent future attacks

The data indicates a growing pattern of phishing attacks, and criminals keep advancing their strategies to terrorise victims online. Some participants had received phishing attempts on various platforms, including WhatsApp, Facebook, and Instagram, but the participants were able to identify the scams. The question thus emerged about what distinguishing factors these participants portrayed compared to those who got phished. The answer lies in information processing, and cybersecurity knowledge and awareness play a key role in phishing susceptibility; this is the final theme.

4.7.1 Information processing

In Chapter 2, information processing and the difference between a heuristic (cues) and a systematic (effortful) processor were defined. Participants who showed strength in systematic processing were less likely to get phished, regardless of their personal circumstances.

For instance, the researcher asked various questions to determine how participants process information (see Table 7). Of the participants, 55% said they are likely to trust a business on social media just based on a verification tick. All the participants said they are unlikely to trust a business based on just the logo. Moreover, 64% said they do not thoroughly go through business posts, while all the participants said they are likely to go through a post if it is sentimental to them. Most (82%) participants said a spelling mistake is a valid enough reason not to trust the legitimacy of a message, while 18% said it is not a valid reason; these individuals also happened to be phishing victims.

Table 7: Information processing overview

Participant code	Is the PT likely to trust a business on social media if the business is verified?	Is the PT likely to trust the business on social media based on the logo?	Does the PT thoroughly go through business posts or skims?	Is the PT likely to check the legitimacy of a message if its contents are sentimental to them?	Is a spelling mistake a valid reason not to trust the legitimacy of a message?
PT 1	Unsure	N	N	Y	Y
PT 2	Y	N	N	Y	Y
PT 3	N	N	N	Y	Y
PT 4	N	N	Thorough	Y	Y

Participant code	Is the PT likely to trust a business on social media if the business is verified?	Is the PT likely to trust the business on social media based on the logo?	Does the PT thoroughly go through business posts or skims?	Is the PT likely to check the legitimacy of a message if its contents are sentimental to them?	Is a spelling mistake a valid reason not to trust the legitimacy of a message?
PT 5	Y	N	Thorough	Y	N
PT 6	Y	N	Thorough	Y	Y
PT 7	N	N	Thorough	Y	Y
PT 8	Y	N	N	Y	N
PT 9	N	N	N	Y	Y
PT 10	Y	N	N	Y	Y
PT 11	N	N	N	Y	Y

Participants who had been victims of phishing (highlighted in darker blue) generally showed low awareness and seldom thoroughly verified posts. Although some participants showed some effort (e.g., Participant 3), they still experienced a phishing incident. This indicates that there are factors to consider outside personality traits and information processing, such as how the user behaves online (discussed in Table 5), what personal circumstances the user is facing at the time, and their overall online habits.

4.7.2 Practical interventions

Participants highlighted some practical interventions they used to stay protected on social media.

- 98% said they have two-factor authentication applied to their applications.
- Users said they often update applications to the latest versions to keep up with security controls.
- 82% said they frequently change passwords. Participant 10 said they use a password safe as it becomes difficult to remember passwords for various applications. In contrast, Participant 11 said he was still very old school and kept a folder on his laptop with all his passwords.
- Participant 10 mentioned the best way to verify the legitimacy of business posts on social media is to check the posts across all their social media pages. Businesses will likely post the same messages across their platforms, not just one.
- “Take everything on social media with a pinch of salt” (Participants 8 and 10).

4.7.3 Cybersecurity training and awareness as a key player

Various organisations have placed great effort into training personnel on cybersecurity awareness and encouraging staff to actively play their part in combating phishing attacks. This level of cyber literacy typically includes mandatory cybersecurity training courses, masterclasses on the dark web, and occasionally sending out hoax phishing emails to employees to gauge who will report the emails as phishing and who will click on the link.

This exposure to cybersecurity knowledge is beneficial for people employed at and whose companies invest in this level of learning. When the researcher asked participants whether they had received formal training on cybersecurity, 82% said yes; these were participants who formed part of corporate South Africa. The remaining 18% were self-employed and had never formally received cyber-education. Subsequently, a significant number of people are still marginalised because of a lack of resources and access to this level of education. This includes individuals who fall within the lower living standards measure (LSM).

One participant commented on this very issue by saying:

> *"there's quite a vigour approach for us as employees just around phishing, phishing attacks, campaigns, and so forth. From a customer perspective, I am keen to know, if they ever will be such an effort made to protect their customers and from that end, you know, it is the responsibility of the organisations. Yes, I know it's a matter of the customers kind of upskilling themselves so they're responsible, but I just always wonder what the companies are doing to equip their customers in this area as well"* (Participant 10).

Participant 2 mentioned he was employed with a global cryptocurrency company called Luno Global. He mentioned that the company often receives consumer reports that they were scammed via phishing, and Instagram was usually the platform where consumers got scammed. During the interview, the participant was asked whether Luno was investing in educating consumers about phishing, and he said:

> "*I believe there is comms that goes out for that stuff, like emails that will tell people, we will never ask you for your password, they also get notifications in the app, umm yeah, but I don't know beyond that I'm not 100% sure"* (Participant 2).

When Participant 9 (from the phishing scenario in Figure 4.6) was asked about cybersecurity training, the participant expressed that the training provided in work environments was insufficient.

> *"If you're looking in the work environments, they are training you to look for links. Ok, nowhere does it say this is happening on social media, right? We know that it's happening, but what I'm saying is from a work perspective, most of the training focuses on you clicking on a suspicious link. All right, nowhere does it say that… Hey, you're going to get a WhatsApp message… Hey, they're going to ask you to join a new social media platform… Hey, they're going to ask you to make investments and there's a ripple effect. Everything is not happening on one platform. Work training is only training you to respond to a link"* (Participant 9).

Participant 10 was asked whether the same training provided at work has assisted her from a social media perspective. She explained:

> *"yeah, its just bringing that awareness, which is something I think from a societal view it's not a lot of people are not aware of things like phishing, vishing, smishing and so forth, it's actually a foreign concept and that's why you're continuously receive these chain messages of 'click here for free' and family and friends share that and all the time".* (Participant 10)

In Figure 4.9, some of the themes identified in the software and how each of the constructs is linked together are presented. Starting in the yellow block labelled "phishing", "user online behaviour" is mentioned and is associated with information processing because that determines how the user receives information online and processes it. "User online behaviour" should be guided by "cybersecurity knowledge and training", which ultimately then prevents "phishing". Phishing cannot necessarily be prevented, but it can be detected, preventing users from becoming victims. An in-vivo node quotation by Participant 10 was included, corroborating the importance of cyber-awareness.

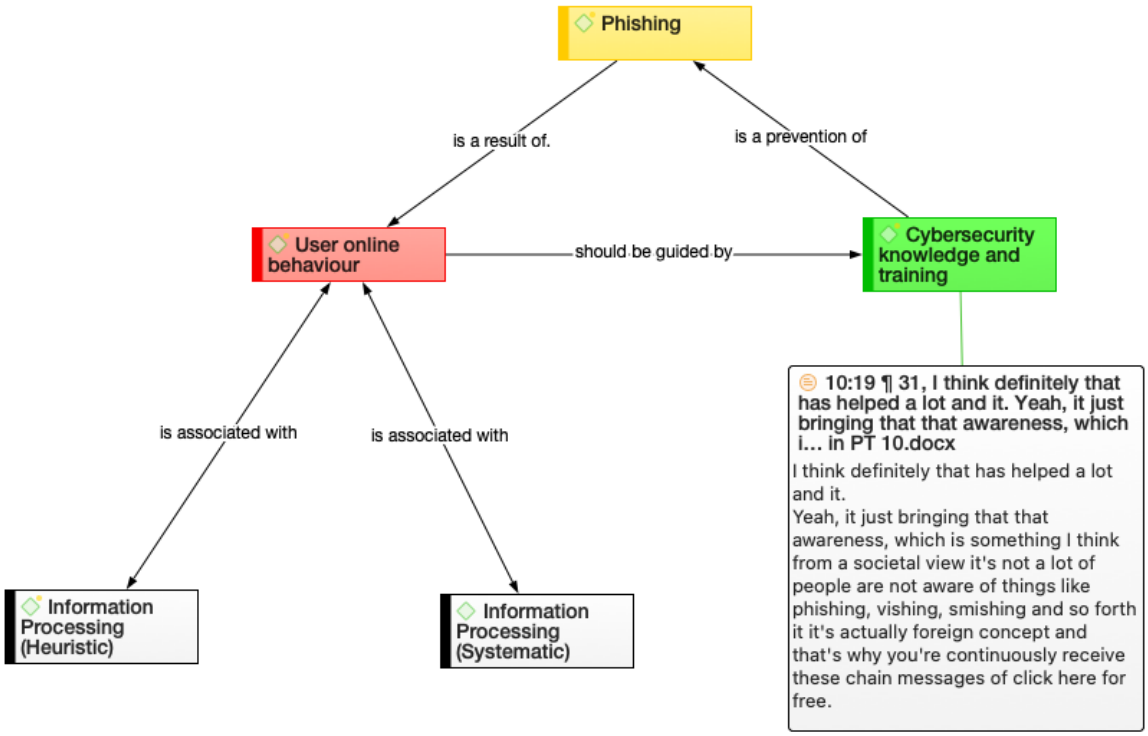


Figure 4.9: An ad hoc network of phishing (researcher's own construct) with reference to ATLAS.ti software

4.8 Unexpected findings

A *Sankey diagram*[6] is a great visualisation that can illustrate the relationships between codes and how relative they are to one another. This is produced by the code co-occurrence table discussed earlier in the coding development process. As seen in the diagram below (Figure 4.10), there is a strong correlation between cybersecurity knowledge and training and users' online behaviour. This is then followed by a relation between information processing, personality types and phishing scenarios.

The code relationships reflected with a darker-coloured strand in the Sankey diagram illustrate a compelling argument; that the data indicates a poor relationship between certain types of personalities and the potential of getting phished. A deeper discussion is presented in Chapter 5. In the literature, it was also assumed that an angler phishing attack occurs when the user reaches out first. In all the phishing attacks in this study, the perpetrators reached out to the participants first.

[6] This demonstrates the strength and correlation between various codes that are relative to other code relationships.

Figure 4.10: Sankey diagram (researcher's own construct) with reference to ATLAS.ti software

4.9 Summary

This chapter provided a comprehensive view of the realities and experiences phishing victims face. Although not all the participants experienced phishing, it was imperative to provide a view of the perceptions people have with regard to phishing. The findings in this study illustrated that an inductive approach was applied to analyse the data, followed by a thematic analysis and an interpretive coding strategy. The findings illustrate that personality traits have little influence over individuals' likelihood of getting phished; instead, the environment in which the person finds themselves at the time can be a contributing factor, and sometimes it is just an unfortunate turn of events. The themes provided a glimpse of the participants' lived experiences, and each added value to each of the propositions. The themes were presented in chronological order to provide the reader with a nuanced view.

It was challenging to present this chapter and convey the gravity of these crimes to the reader. Therefore, it was crucial to portray the participants' perspectives in an open and honest manner to keep the details and idiosyncrasies of the individuals' experiences intact. To

conclude, Table 8 provides a snapshot view of the themes and their features, supported by excerpts from the participants.

Table 8: Summary of themes and their features

Theme	Sub-themes	Description (What it represents)	Cases (No. of Participants)	Counts (No. of Empirical Indicators)	Empirical Indicator (Evidence)
Cybersecurity Hygiene	User online behaviour, social media usage and footprint	This reflects the type of behaviours users display online	11	212	*"I do often explore new platforms and engage with strangers online. I am curious by nature"*
Phishing tactics	Strategies and techniques, phishing experiences, false urgency	The type of SE tactics that occurred and their impact	4	120	*"They were convincing. I guess I trusted that human to a certain extent"*
Cybersecurity Training and Awareness	Identifying strategies, techniques	This highlights the role and importance of cybersecurity training	11	66	*"The phishing training received from work falls short. It teaches you to look for a link, but nowhere does it speak about what's happening on social media"*
Information processing (Heuristic vs Systematic)	Personality traits	How do users process information online	11	75	*"I don't thoroughly read business posts unless it's something or relevant to me"*

CHAPTER 5: DISCUSSION OF FINDINGS

5.1 Introduction

In this chapter, the discussion links the findings presented in the previous chapter to the context of the literature and the relevant research questions identified in Chapter 1. Furthermore, this chapter revisits the proposed conceptual framework from Chapter 2 and explores whether it is still suitable based on the findings or needs to be adjusted. Lastly, the chapter examines relevant and practical interventions to alleviate future phishing incidents.

5.2 Discussion on strategies and techniques cybercriminals are using to successfully execute angler phishing attacks

In the literature, Allen (2021) introduced a cycle that cybercriminals follow to execute a phishing attack, which consists of four phases: information gathering, relationship development, exploitation, and execution. The findings revealed that phishing perpetrators indeed follow this cycle, although it can be said that information gathering is not visible to the victim in some instances. In the previous chapter, Participant 9 alluded that it almost seemed as if research had been done on her and her family. Once she could no longer access Telegram because her account had been blocked, she tried accessing it from her husband's phone, where she also received a message that the account was blocked despite her husband never previously registering on Telegram. This raised the question of how he could be blocked.

The participant proceeded to do her own research after the incident and discovered the following:

> *"Through my own research, what I discovered is that Telegram doesn't have a support centre or a call centre. All the people that are on Telegram, they are volunteers who, offer their assistance to helping others with Telegram. But it's not an actual formal support centre. So, which is also interesting because it could be the entire syndicate has probably registered as volunteers on this, right, they are probably the people who go and ban your account after you've made the investment"* (Participant 9).

It was an interesting discovery that Telegram had no formal headquarters. This could be another reason perpetrators use that specific platform for criminal activities. Conversely, WhatsApp, Facebook, and Instagram are social media platforms managed by Meta. This does

not necessarily mean phishing incidents are non-existent on Meta-managed platforms, but there is some form of oversight.

Participant 5 had a phishing incident occur on Facebook. He was a digital marketer responsible for the social media management of various South African retail businesses. He received a link asking him to review the content in the link so an opportunity could be presented if the content was deemed worthy. Unfortunately, this link contained malware that infected his computer with a virus, and the perpetrators gained access to his accounts. The perpetrators then tried to access millions of rands by fabricating a social media campaign. Fortunately, the amount requested exceeded the budget the business typically spends on campaigns, so Meta quickly flagged an alert. He recalled the moment he realised it was a phishing incident:

> *"So, it was when they set up a campaign, they were supposed to spend half a million a day on social media. The next day we then realised that this was not what we thought it was and it was phishing. So, what happens then Meta. So, this incident happened on a Meta platform (Facebook). Meta triggered a security warning because it was an unusual activity. Then they blocked that account, so they blocked everything. They blocked my own account from running it. When that is blocked, they are not able to run it because the account is blocked and then we need to go into a security process where we have to now get the account back and unblock it. So, if Facebook did not block the account that night, I would have woken up to millions and millions of rands, having been spent"* (Participant 5).

This specific incident indicates that Meta platforms have enhanced security measures to protect businesses from cybercrime attacks. Additionally, these two scenarios exemplify that perpetrators indeed try to understand their targets' backgrounds, jobs, and even family backgrounds. In South Africa, Pieterse (2021) found that the primary motive for phishing was criminal intent, which aligns with Allen's (2021) most common motive for SE attacks, which is financial gain. Money was at the centre of all the phishing incidents participants reported.

The findings reflect that the perpetrators used different persuasion techniques to mislead the participants. According to Frauenstein and Flowerday (2020), the six fundamental principles of persuasion techniques are reciprocation, commitment or consistency, social proof conformity, authority, liking and scarcity. Without realising it, the participants had already committed themselves and were dedicated to completing the falsified work instructions received from the perpetrators and were anticipating a good ending. The perpetrators used

authority and scarcity techniques to consistently persuade the participants to trust them and convince the participants that they were making a good financial investment and would reap the rewards. In Chapter 4, the participants disclosed that they had to adhere to the false instructions once they were targeted because failing to do so would have dire consequences, including threats of financial loss.

The scarcity technique entails using time boxes to put pressure on victims (Siddiqi et al., 2022). It was as though they were in a maze and needed to keep going through levels to get to the next one. The victims had deadlines for every task they had to perform, everything was timeboxed, and they always needed to submit proof that they had completed the task.

5.3 Discussion on experiences, perceptions and behaviours of users who fall prey to these deceptions

When organisations face phishing incidents, they often do not want to report them publicly because they need to maintain a positive image with consumers. Businesses can suffer major consequences such as reputational damage, revenue loss, and loss of consumers' trust and retention in the event that phishing scandals come to light (O'Hagan, 2018). However, in the long run, organisations typically recover from such setbacks, but the same cannot be said for individuals who personally experience phishing attacks.

In one study, when individuals were asked about the consequences of phishing, psychological impacts emerged most prominently, highlighting negative emotions such as embarrassment, shame, and a loss of self-confidence (Kelley et al., 2012). Similar findings were reported in this study when participants shared their various emotions. In Figure 4.7, the psychological impact on victims was presented, and they all expressed similar sentiments of guilt, shame, embarrassment, and self-blame.

In addition to the psychological impact, participants mentioned the grievance of the financial loss. Participant 3 lost more than R10 000; Participant 8 lost over R11 000 (which was refunded by her bank); and Participant 9 was scammed out of R160 000. Participants 3 and 9 unfortunately never recovered any of their money.

Users' experiences matter, and not enough is being documented and shared on the severe impact individuals face when they become victims of phishing. When this study's participants were asked about the post-recovery phase after having been phished, participants referred to lingering anxiety and fear of being a victim again. Worry and self-criticism dominated as an

emotion-focused coping mechanism in other studies as well (Wang et al., 2017). In severe cases, similar to the recent global Ant Ranch scam (Specialised Security Services, 2023), reports of victims retaliating with physical assaults, abductions and suicides emerged.

The researcher opines that phishing victims should always be compensated by the relevant business/financial institutions where financial loss is experienced, and professional healthcare interventions are also important. These include therapy so victims can receive the help they need to recover psychologically.

5.4 Discussion on how personality traits contribute to user behaviour, information processing and phishing susceptibility

The Big Five Personality Framework is one of the most significant models contributing to behavioural research because personality traits play a key role in understanding users' online behaviour (Amichai-Hamburger et al., 2002). By understanding which personality traits an individual associates with, character traits can indicate how certain users respond to phishing stimuli and whether certain behaviours or habits lead to phishing susceptibility.

In their study, Frauenstein and Flowerday (2020) found individuals with specific personality factors were more likely to respond to persuasion techniques. A summary of the findings is documented in Table 9, including an additional comparison of the findings from this study in the third column.

Table 9: Summary of personality traits and phishing susceptibility: post-findings comparisons

Personality Trait	Susceptibility to phishing	Findings of this study
Openness	High likelihood of oversharing information on Facebook	Participants who related to openness, as a personality trait, were more likely to be active on social media in general.
Conscientiousness	At high risk for spear phishing	Participant 5, who identified as both conscientious and extraverted, did in fact experience spear phishing.
Extraversion, Openness	More adept at spotting phishing emails	Participant 6 said she is naturally curious and consequently often comes across multiple phishing scams. However, she is alert and has never been a victim.
Extreme Extraversion	A greater propensity to getting phished (opposing views in a different study)	Only Participant 4 showed extreme extraversion, but was alert, able to spot phishing scams, and had never been phished.

Personality Trait	Susceptibility to phishing	Findings of this study
Openness, Extraversion, Agreeableness	More prone to adhering to instructions in phishing emails	Participants 3 and 5 followed scammers' instructions.
Conscientiousness, Agreeableness, Neuroticism	Less vulnerable to phishing on social media	Participant 1, who identified as neurotic, was less likely to get phished because of their anxiety related to neuroticism. However, individuals who reflect conscientiousness and agreeableness are more likely to get phished on social media and follow phishing instructions.

The findings in this study indicate that there are similarities to Frauenstein and Flowerday's (2020) findings with regard to the openness personality trait and users having a higher likelihood of oversharing on Facebook. Participants who identified with openness as a personality trait in this study were more likely to be active on social media. Participant 8 said she spends most of her time on Facebook Marketplace and Instagram. Frauenstein and Flowerday (2020) found that participants who identified as conscientious were more likely to fall victim to spear phishing. One of the main goals of spear phishing is stealing an individual's login details or infecting their devices with malicious malware to gain access to their personal information. Similarly, Participant 5, who identified as conscientious, experienced a form of spear phishing on Facebook.

Although individuals who identified with extreme extraversion have been found to be more prone to getting phished, this study found that extroverted participants showed signs of being alert. Further, conscientiousness and agreeableness were highlighted as personality traits that were less likely to get phished; however, in this study, participants with these two traits appeared more likely to get phished and follow phishing instructions.

The findings are not concise and show different results, just as previous personality studies have determined. It is also important to consider that users can identify with more than one personality trait, and people may not necessarily have the same personality in person and online. For instance, Participants 5 and 7, who have to show up as extroverts for their careers, portrayed different personalities online; they were actually conscientious people. When asked whether the lines can sometimes be blurred between the two constructs, they concurred and said yes, because there is only one of them, but they must coexist in both worlds equally.

It can be argued that personalities may even present differently based on what environment the person is facing at the time. Participant 9, who identified as conscientious and, according to Frauenstein and Flowerday (2020), is less likely to be phished on social media, did fall

victim to a phishing scam because her circumstances at the time were compromised. Participant 3 had a similar experience as a result of being vulnerable and desperate at that moment. The environment can heavily influence an individual's response triggers and that can ultimately determine their potential of getting phished.

It can also be said that personality traits have a significant influence on an individual's ability to engage in information processing. Participants who resonated with openness and extraversion identified more with heuristic processing and often deemed themselves as visual people. In contrast, participants who were conscientious, agreeable and neurotic were found to be systematic information processors.

5.5 Discussion on practical interventions social media users can apply to protect themselves from future attacks?

While businesses are responsible for educating and protecting consumers against online phishing scams, social media users are responsible for ensuring they have applied basic security interventions. However, social media users tend to be negligent, and they fail to implement privacy control settings and nonchalantly click on links without reviewing the content (Frauenstein & Flowerday, 2020). The findings indicated that this was the case with the study participants.

The Accenture Report (Mcanyana et al., 2020) alluded that 50% of South Africans did not know what multifactor authentication was. When asked whether they knew what two-factor authentication was, 90% of the participants in this study said they knew what it was, but only 72% had applied it to their applications. Additionally, the participants were asked what they do to keep up with security controls on their applications, and the top three answers were: "I update my applications frequently", "I try to change passwords when I remember to", and "I have multifactor across my devices". The participants showed a strong attentiveness in understanding how to protect themselves and keep abreast with security controls.

However, despite this finding, when participants were asked whether they often click on unsolicited links, 36% said yes because they have a curious nature, and 64% said they did not thoroughly investigate the content or source (see Table 4). This proves that even though an individual may have the necessary cyber knowledge, it is not often applied when presented with possible phishing attempts.

The findings in the study indicate that cybersecurity training and awareness play a significant role in understanding the fundamentals of phishing. Wang et al. (2017) similarly argue that training can improve individuals' phishing detection abilities. Many of the participants could provide a decent definition of phishing. Moreover, when they were asked to rate their ability to identify a potential phishing attempt, 36% rated themselves an 8 out of 10, 36% rated themselves a 9 out of 10, and 18% said 11 out of 10.

Training, however, requires resources. As mentioned in Chapter 4, a large population of South Africans are disadvantaged because of a lack of access to resources and knowledge. In his white paper report, Improving Cybersecurity Awareness in Underserved Populations, Ahmad Sultan (2019) wrote about how underserved citizens in San Francisco (particularly the poor, the elderly and foreign-speaking individuals,) were more likely to become victims of phishing than the average San Francisco citizen. Key findings in his research highlighted that 20% did not know about online cybercrime, 21% did not know about email scams, 26% did not know about phone or mobile viruses, and 31% did not know about antivirus software. He found that underserved citizens had lower confidence in their ability to protect themselves online and no confidence in digital businesses to protect their information online (Sultan, 2019). Moreover, respondents had misconstrued perceptions about security knowledge and what it entails and were unable to provide perspectives on cybercrime's impact because they lacked a basic understanding of cybersecurity concepts (Sultan, 2019).

The main recommendations in his study had a significant focus on pushing the responsibility to city leaders, i.e., the government. He started by stating that leaders cannot fix what is unknown, and as a first step, they need to assess how severe the problem is in their underserved communities by conducting relevant surveys that will gauge the current cybersecurity landscape. He further emphasised that these surveys should be conducted in collaboration with businesses that serve underserved communities. Secondly, he opined that cities need to offer digital literacy training sessions to the communities. This training needs to be tailored to targeted groups and audiences, so it meets their cybersecurity level, current needs, cultural sensitivities, and trust habits (Sultan, 2019).

One study that focused on marginalised groups in Africa, specifically Kenya, Uganda and South Africa, found that there were higher security risks for marginalised individuals, including exploitation of lower digital literacy and familiarity with technology, lack of affordability and resources to apply secure software, poor and confusing cybersecurity regulations, and gender disparities, with cyber threats varying for women and men (Anthony, 2023). However, some noteworthy partnerships and initiatives were established to prioritise cyber resilience for

marginalised groups. For instance, the Consultative Group to Assist the Poor and West African Economic and Monetary Union partnered with other financial sectors to launch a consumer protection laboratory. The lab aims to strategise alternative approaches to enhance consumers' protection against cybercrimes and focus on more consumer-centric approaches (Anthony, 2023).

Anthony (2023) recommends three practical interventions for consumers to become more cyber resilient, namely customer-centric policies and regulations, more robust technical security controls for vulnerable consumers, and increased support for research and platforms that allow information sharing among consumers to expose individual challenges (Anthony, 2023). More importantly, publicising digital fraud could contribute to higher consumer protection because digital awareness can help users understand basic phishing vulnerabilities.

Businesses thus need to implement aggressive strategies that focus on educating the lower LSM market on cybersecurity awareness and how to protect themselves online, bearing in mind that this strategy needs to be at the level of the consumer for them to understand what phishing is.

5.6 Revisiting the conceptual framework

The initial conceptual framework presented in Chapter 2 required a fourth construct (social media) to be included because it links to the exposure phase when a user accesses a social media platform. However, after reviewing the data and findings from the participants, the researcher determined it is important for the framework to be adjusted to include two additional constructs, as discussed next.

5.6.1 The environment

As mentioned previously, various external factors can influence a user's environment, such as personal matters, work, and the economy, among others. These factors are part of our daily lives. When there is a slight shift in the environment, this can easily affect the way in which individuals usually present themselves. Similar to a flight or fright quandary, a user could face an unprecedented situation, such as a family challenge or retrenchment, inducing stress and leading to financial challenges. As a result, when individuals face a plethora of financial issues, the urge to look for a quick way to make money seems like a viable solution, and it becomes easy to fall prey to "investment scams".

5.6.2 Cybersecurity training and awareness

Additionally, the participants emphasised cybersecurity training played an essential role in how they show up online. Training is important as it can assist with phishing scam detection; by knowing and understanding what signs to look for and keeping abreast with security news, users are able to stay in the loop on new cyber trends and the latest scams. They can consequently continue to improve privacy controls and safeguard themselves online. The training aspect should essentially be applied in the processing phase where information processing takes place. The knowledge acquired in the training should emerge when users review suspicious messages and know what to look out for.

Figure 5.1 is an adapted conceptual framework design and includes the environment and training constructs.

5.7 Discussion on the conceptual framework and focus group review

To further evaluate the updated conceptual framework presented in Figure 5.1, a short focus group session was conducted with technical lead experts who have in-depth experience and insights on cybersecurity. It was important to get subject matter experts to critique the conceptual framework and weigh the framework's validity and applicability.

In the focus group session, the researcher started by providing context to the study and explaining the study's objective. Each of the constructs in the conceptual framework – social media, personality traits, information processing (heuristic and systematic), phishing susceptibility, the environment and cybersecurity training – were unpacked and explained to the focus group participants so they could understand the framework's purpose.

The experts agreed that the environment plays a crucial role in influencing how a person responds to a phishing message, and it can affect their regular way of information processing. One participant mentioned that a major issue users are unaware of is the challenge of consumers giving access to applications to track their activity across different applications. The participant mentioned that providing permissions for social media activity to be tracked across different applications leads to higher phishing susceptibility because cybercriminals can access and profile you based on what information brands tailor for you based on your online behaviour. Additionally, the participants mentioned that newer phishing attacks are using AI, and emotional and mental manipulation of the users is at the core of phishing attacks.

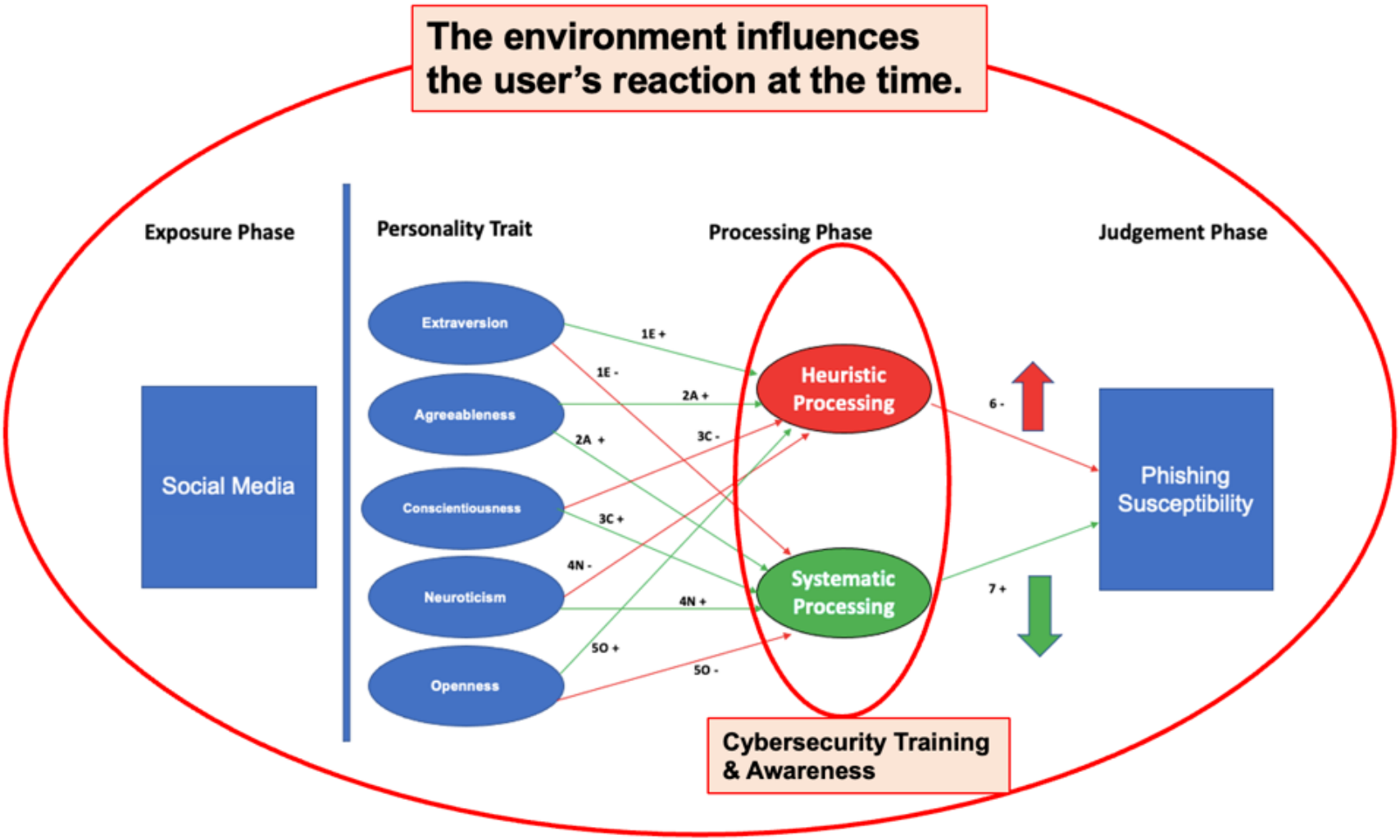


Figure 5.1: Revised conceptual framework (researcher's own construct)

Social media construct in the conceptual framework was deemed vague and broad. It was questioned whether social media meant the consumer was active on their social media platforms or whether it was the cybercriminals accessing social media to conduct phishing attacks or target consumers. To clarify, it was explained that the conceptual framework focused on social media users, so it would be the consumer accessing social media.

A recommendation was made that the social media construct in the framework be made explicit that the social media exposure phase refers to cyberattack threats that the users get exposed to. Additionally, it was recommended to emphasise that emotional stimuli, referring to the users' emotional state, can influence how they react and process information. As a result, the conceptual framework was adapted to reflect this in Figure 5.2.

.

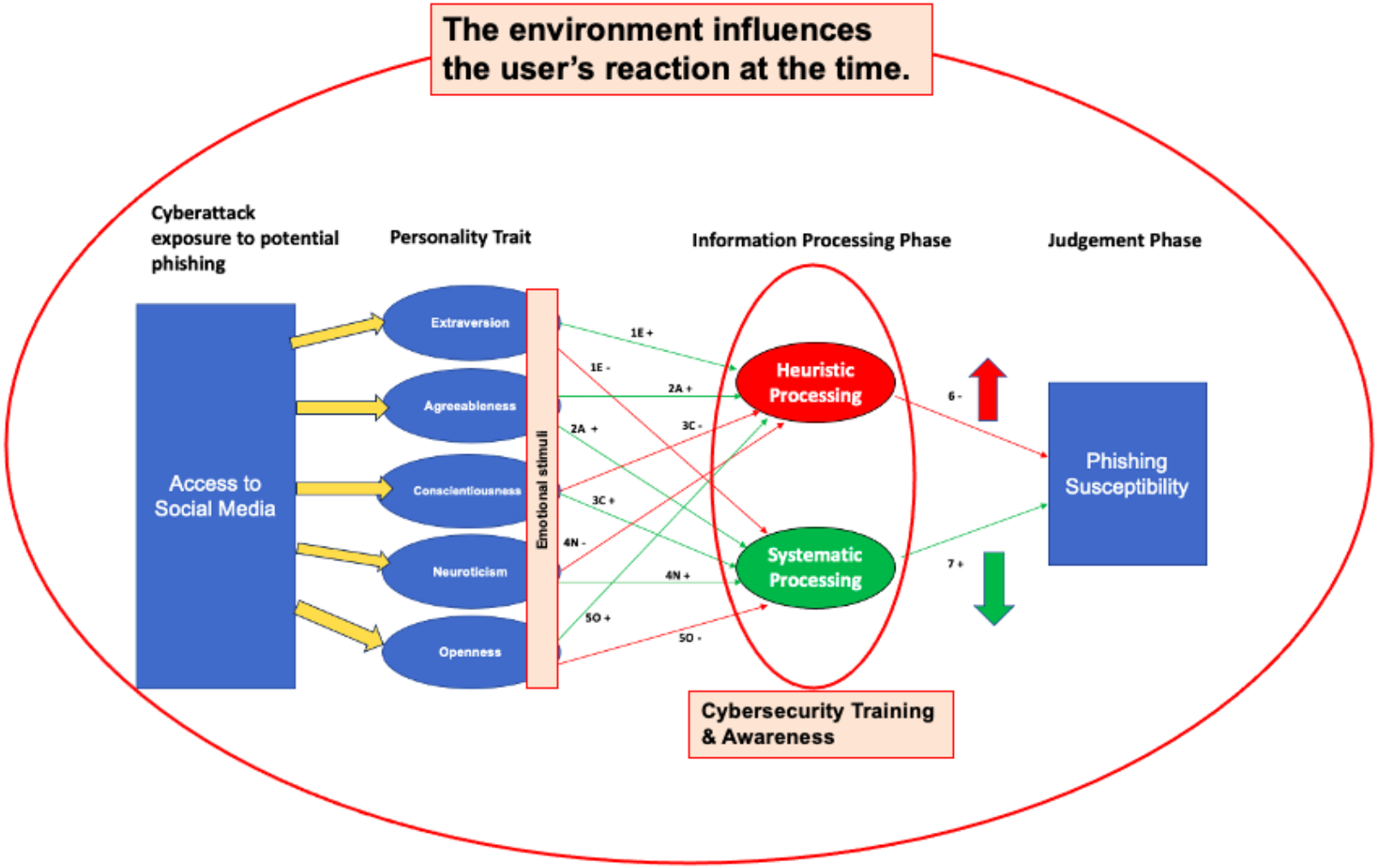


Figure 5.2: Re-adapted framework post-focus groups (researcher's own construct)

5.8 Summary

Each dimension of the four propositions was discussed in accordance with the relevant literature. The chapter provided a review of the context according to the four constructs of the study (cybercriminal techniques and motivations, user experiences, personality traits and interventions). The conceptual framework was also augmented to include additional factors, namely the environment and cybersecurity training as vital in the phishing susceptibility framework. Furthermore, a focus group was conducted to evaluate the framework, and additional recommendations and adaptations to the conceptual framework were provided. The adopted framework provides a richer picture of users' behaviour in a phishing lifecycle and is inclusive of the users' emotional stimuli playing a pivotal role in a phishing threat.

CHAPTER 6: CONCLUSION AND RECOMMENDATIONS

6.1 Introduction

This chapter is an amalgamation of this research study, providing a conclusive summary of the research aim and objectives. It includes an evaluation of the research methods used, the contributors that made it possible to answer the research questions, possible recommendations, limitations of the study, and suggestions for future research.

6.2 Summary of research questions and findings

The study aimed to explore the experiences of angler phishing attacks on social media users in South Africa. To achieve this objective, users were contacted on social media to participate in the study if they had previously been victims of phishing attacks. Due to the low response rate of actual victims, non-victims were included as part of the sample in order to get their perspectives on angler phishing. This approach was important so the research could achieve a viable sample for the data collection process and provide other philosophical perspectives from consumers. Eleven participants took part in the interviews, four of whom were victims of phishing, and seven were non-victims but had previously experienced several phishing attempts. Additionally, in phase two of the study, it was deemed fit to conduct a focus group session with seven participants who are subject matter experts. The study yielded the following results:

6.2.1 Prevalence of angler phishing in South Africa

Only 27% of the cases presented in this study experienced angler phishing incidents. This is an insignificant number to ascertain the prevalence of angler phishers in South Africa. However, it is enough to assume that there are other victims of social media phishing, angler phishing is indeed emerging, and it has dire consequences. As seen in recent reports, the statistics indicate that in the past year alone (2023), impersonation fraud and scams had increased by 365% in South Africa (Tredger, 2023). Ultimately more of these cases need to be reported to the relevant channels to get a better view of the phenomenon’s severity in South Africa.

6.2.2 Strategies and techniques cybercriminals use to successfully execute angler phishing attacks

Based on the findings, persuasion remains the most prevalent SE technique perpetrators use to sway victims. Human-based techniques will keep evolving as technology advances, making it even harder to discern between what is real or fake on the internet. Ultimately, the use of different persuasion techniques can affect the intended response or outcome from a user (Zhuo et al., 2023). One of the participants alluded that generative AI and deepfakes are spreading quickly. Generative AI tools have become a double-edged sword in cybersecurity for perpetrators, enabling them to use larger sums of data to generate responses quicker and teaching humans to advance their human-based techniques for more sophisticated attacks (Gupta et al., 2023). This advantage will only increase cybercrimes and make it difficult to have solid human interactions on the internet.

6.2.3 Users' experiences, perceptions and behaviours related to phishing attacks

Overall, the interview data suggests that the psychological impact on victims remains the most ominous consequence of cybercrimes. There is a lack of intervention from organisations and financial institutions when users experience phishing, probably because the onus is on users to ensure their own safety online. This perception that consumers are entirely responsible for their own online security measures can be misleading and flawed. If organisations do not provide the necessary education to promote consumers' awareness, they will not know any better and fail to apply the necessary precautions online, continuously falling victim to phishing attacks. Organisations (private and public), governments, and city leaders are all part of an ecosystem that needs to drive consumers' protection (Anthony, 2023).

6.2.4 Personality traits that contribute to users' behaviour and phishing susceptibility

The data revealed an inconsequential correlation between personality traits and phishing susceptibility. Although some similarities with previous studies were found, there were also some differences. It is important to consider that users may resonate with more than one personality trait, and how users behave online may not necessarily be the same persona portrayed in person. Zhuo et al. (2023) concur that personality remains one minor opportunity for user impact. Since participants highlighted that their careers demanded them to portray a different personality, the dimension of personality traits and its influence on phishing susceptibility can be inconclusive.

6.2.5 Practical interventions social media users can apply to protect themselves from future attacks

A user's online behaviour is guided by two main factors: how they process the information they are exposed to and how they apply the knowledge gained in cyber training. In alignment with the literature and findings, cybersecurity training and education remain a key factor for users not to become victims of phishing. Cybersecurity training needs to start taking an approach of tailoring training for different audiences and not applying an umbrella one size-fits-all approach because there are less-knowledgeable users to consider (Zhuo et al., 2023). As previously indicated, practical interventions are included in the recommendation section.

6.3 Conclusion

Phishing will continue to pose massive threats to individuals and organisations (Frauenstein & Flowerday, 2020). As the internet and technology evolve, new social media platforms are constantly being introduced to the market, cybercrimes are advancing to adapt to the newest trends, and phishers continually find loopholes. SE techniques are advancing and adapting new technologies, such as generative AI and deepfakes; social media users consequently need to tighten the reins on sharing information online.

Cybersecurity training needs to be enhanced and include new and rising phishing scams, such as angler phishing. Organisations need to broaden their training scope and provide solutions that solve different kinds of human-based manipulation techniques and persuasive tactics used by phishers, identify what the popular strategies are, and move beyond the traditional "identifying fake links and fake websites". The training scope needs to be broadened, and consumers should be educated on changing certain online behaviours and cultivating a new security-conscious mindset.

Government policies and regulators must assist organisations by releasing new cybersecurity policies as quickly as new technologies are released. Social media platforms, such as Telegram, which do not have headquarters and formal call centre support, should be policed and some regulation needs to be applied. Several countries have banned the use of Telegram for various reasons, including political propaganda, hate speech, and poor security controls on the application (Benjamin, 2018).

No amount of research will ever be able to account for human behaviour, and researchers can only try and understand it. Therefore, individuals' understanding of their own personality traits and prudently applying a more cognitive approach to information processing can potentially prevent phishing victimisation.

6.3.1 Conclusion of research question one: What is the prevalence of angler phishing?

There needs to be more focus on businesses creating platforms for individuals to share their lived experiences. Organisations, governments, and the private and public sectors need to start publicising fraud scams and ensuring the necessary institutions are documenting these appropriately. Trust in the system must be restored so consumers know their experiences are taken seriously. Only then will South Africa start obtaining sufficient data, and future studies can properly report on the prevalence of phishing attacks in the country.

6.3.2 Conclusion of research question two: What strategies and techniques are cybercriminals using to successfully execute angler phishing attacks?

The strategies that attackers use will keep evolving with the introduction of generative AI and other technologies. It will become even more difficult for users to discern what is real and fake. Hence, consumers need to understand the basic principles of cybersecurity and exposure to the right cybersecurity training can aid this understanding.

6.3.3 Conclusion of research question three: What are the experiences, perceptions and behaviours of users who fall prey to these deceptions?

There is a need for platforms and interventions where users share their phishing experiences. This study aimed to encourage victims to share their lived experiences, and even with anonymity being guaranteed, users were still not comfortable coming forward. The perception about phishing and becoming a victim needs to shift from individuals feeling shame and guilt to the perpetrators being accountable for their criminal actions.

6.3.4 Conclusion of research question four: How do personality traits contribute to user behaviour, information processing and phishing susceptibility?

The idea that the construct of personality traits alone can assist in understanding an individual getting phished proved to be inadequate. Personality can provide guidance in understanding

users' online behaviour, but other factors, such as the environment, training, culture and habits, among others, need to be factored into the entire user experience phishing lifecycle.

6.3.5 Conclusion of research question five: What practical interventions can social media users apply to protect themselves from future attacks?

It is important to note that the interventions and recommendations provided aim to alleviate the probability of phishing and are not meant to combat phishing. Phishing has been around for centuries, and it will only keep evolving as technology evolves. Therefore, applying the necessary security protocols and interventions can assist users but not remediate the problem. Organisations are responsible for educating and continuously improving security measures so consumers can feel protected.

6.4 Conclusions on conceptual framework

The conceptual framework has undergone many iterations since its initial presentation in Chapter Two. The last and final version of the conceptual framework includes the recommendations received from the focus group session conducted in Chapter Five. The framework in Figure 6.1 is the final conceptual framework for this research.

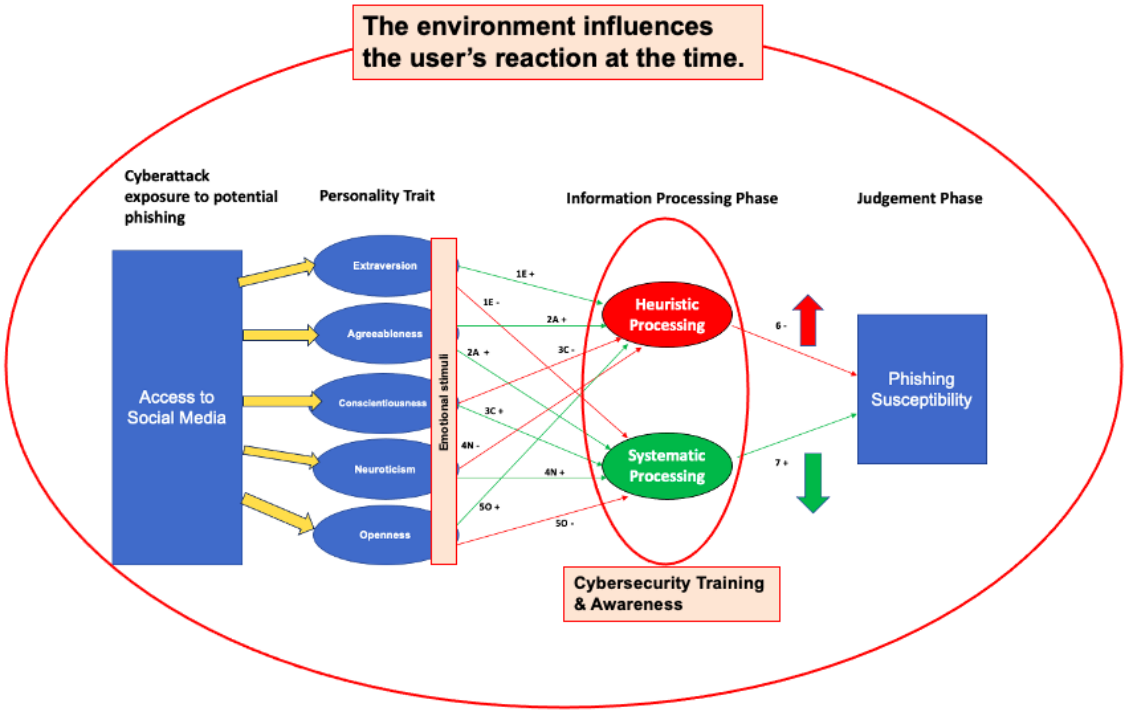


Figure 6.1: Final conceptual framework

The conceptual framework can be understood as flowing from left to right:

a) A user is first exposed to a cyberattack potential threat when they access social media.
b) Based on their type of personality trait (yellow arrows), a user is influenced by their emotional stimuli.
c) This result can have a positive (+) or negative (-) impact on the user's ability to process information.
d) When a user applies heuristic or systematic processing, the role of cybersecurity training and awareness is a key component to determine if they understand what cues to look for in a phishing message.
e) This approach will essentially determine whether the phishing threat has succeeded.
f) In this entire phishing lifecycle, the environment, and the context in which a user is at the time, ultimately influences a user's reaction to how they carry out points A to E explained above.

6.4.1 Contextual contributions

The framework contributes to the body of knowledge in understanding a user's phishing lifecycle and their probability of getting phished. Various factors, such as the context in which a user is, the level of cybersecurity training and knowledge they have been exposed to and the user's emotional stimuli before applying information processing, all matter. Therefore, to ultimately understand how personality traits and information processing proceed to play a pivotal role in phishing, it cannot be done outside of these additional contextual constructs.

6.4.2 Theoretical contributions

The adaptation of a conceptual framework contributes significantly to future research studies with the same phenomena. The framework can be used to measure other variables that have previously not been considered in seminal literature by theoretically applying relevant hypotheses and a matrix to determine how different environments and different levels of digital literacy influence phishing susceptibility.

6.4 Recommendations

The rationale of this research study was to benefit two major stakeholders, namely South African businesses that already have a presence on social media and want to expand their

digital businesses to social media platforms, as well as the social media users affiliated with businesses on social media. The following recommendations are made for each stakeholder:

6.4.1 Recommendations for social media users

- Ensure you are exposed to some cybersecurity awareness and education.
- Keep abreast of security news, the latest cyber trends and digital technologies, and what they mean for you as an active social media user.
- Understand what privacy controls are available and ensure you have applied them to your applications.
- Update your software applications regularly; older versions tend to be prone to security breaches.
- Frequently update passwords and use a password safe if there are too many passwords to remember.
- Practice self-awareness and mindfulness. When you are mindful, aware, and present in the moment, factors such as what is happening around your environment will not affect your reactions prematurely.
- Lastly, always use social media with a pinch of salt. Do not take everything online at face value.

6.4.2 Recommendations for South African businesses

Organisations are responsible for keeping consumers safe and protected on all platforms that interface with the consumer, including informal platforms such as social media. The same vigour and drive invested in workforces should be replicated for consumers across all industries.

- Inclusivity is important. Organisations should have a rigorous strategy on how lower LSM consumers can be educated on cybercrimes. Only relying on sending communications and pop-up messages through an app is not sufficient and marginalises people experiencing poverty because there is a large population who are not exposed to digital platforms. For instance, how can an individual based in an informal settlement with WhatsApp access but no banking app be educated on how to stay alert from criminals?
- Organisations should have a solid security architecture framework, internally and for external applications.
- Organisations should limit data leakage by managing how much information users can provide to businesses on social media.

- Even though verification can now be bought, organisations should ensure all social media platforms for the business require verification. That way, users can track the consistency across the businesses.
- Organisations should create incident report lines. In the interviews, participants were asked if they reported phishing attempts to the relevant businesses and most said they would not even know where to report them. Organisations should ensure consumers understand processes on how to report fraud.
- Organisations should be transparent with consumers. They should be open and honest about breaches and scams; that way, users will know what is happening in the organisation and that something is being done to resolve problems.
- Organisations should leverage technologies and software that can identify spam messages to consumers.
- Organisations should be proactive in reporting and having fake accounts with similar business names removed on social media.

6.5 Limitations of the study

Qualitative studies are often criticised for their sampling size being too small and the evaluation of the study possibly being too subjective (Rodolfo et al., 2011). The intended purpose of opening participation of this study to the entire South Africa, as opposed to a specific province or city, was to recruit as many participants as possible because it would be difficult to assume that a specific region experiences more phishing attacks. This approach still did not yield the desired outcome, as the study only managed to secure 11 participants.

Eleven participants are an insubstantial sample to determine the prevalence of angler phishing. Despite using snowball sampling and actively recruiting on social media, it was daunting to find people who would be comfortable admitting to being scammed. The researcher was cognisant that there is also a large population who are not habitually active on social media for various reasons, including a lack of data, among others. This does not prevent them from potentially being or becoming victims of phishing.

Another acknowledged limitation was the research instrument not having adequate questions to measure information processing, compared to other studies that provided different scenarios to ignite stimuli from participants. Participants could have been biased in their answers to convey a certain image to the researcher.

Lastly, it could have been beneficial to focus on measuring the extent of angler phishing on one specific social media platform, for instance, WhatsApp or Facebook.

6.6 Suggestions for further research

The users in a phishing incident are only one aspect of an entire phishing lifecycle. There are also businesses whose profiles get impersonated and financial institutions that receive fraud reports, among others. As a future research suggestion, it could be beneficial to consider interviewing different fraud department heads, to gain the perspective of fraud departments who have these crimes reported to them. It is also worth exploring how they determine which victims receive refunds and which do not.

As previously stated, to reach a larger sample of participants, this study did not focus on specific demographics and industries. Future studies can look at more purposive sampling, such as Generation Z's who are on the latest social media platforms, and perhaps look at specific social media platforms such as TikTok and phishing, or Instagram and phishing. Additionally, it could be beneficial to focus on a specific industry; for instance, financial institutions or telecommunications fraud.

Future studies could also measure other factors, such as culture, and the role of government laws in cybersecurity policies and regulating social media platforms to protect consumers.

REFERENCES

Aichner, T., Grü, M., Maurer, O., & Jegeni, D. (2021). *Twenty-Five Years of Social Media: A Review of Social Media Applications and Definitions from 1994 to 2019*, 24(4). https://doi.org/10.1089/cyber.2020.0134

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes,* 50(2), 179-211.

Allen, M. (2021). *Social Engineering: A Means to Violate A Computer System Social Engineering A Means To Violate A Computer System*. SANS Institute

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. John Wiley and Sons Inc. https://doi.org/10.1049/ise2.12073

Amichai-Hamburger, Y., & Vinitzky, G. (2010). Social network use and personality. *Computers in Human Behavior*, 26(6), 1289–1295. https://doi.org/10.1016/j.chb.2010.03.018

Amichai-Hamburger, Y., Wainapel, G., & Fox, S. (2002). "On the Internet No One Knows I'm an Introvert": Extroversion, Neuroticism, and Internet Interaction. *Cyberpsychology & Behavior,* 5(2).

Anthony, A. (2023). *Cyber Resilience Must Focus On Marginalized Individuals, Not Just Institutions*. https://carnegieendowment.org/2023/03/13/cyber-resilience-must-focus-on-marginalized-individuals-not-just-institutions-pub-89254

Benjamin M. (2018, May 11). Why are so many countries banning Telegram? *Dog Town Media*. https://www.dogtownmedia.com/many-countries-banning-telegram/

Bhagattjee, P., Govuza, A., & Westcott, R. (2021, June 9). *Regulating the Fourth Industrial Revolution - South Africa's Cybercrimes Bill is signed into law*. Cliffe Dekker Hofmeyr.

Blythe, M., Petrie, H., & Clark, J. A. (2011). *F for fake: Four studies on how we fall for phish. Conference on Human Factors in Computing Systems - Proceedings*, 3469–3478. https://doi.org/10.1145/1978942.1979459

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1 478088706qp063oa

Busetto, L., Wick, W., & Gumbinger, C. (2020). How to use and assess qualitative research methods. *Neurological Research and Practice* 2(1). BioMed Central Ltd. https://doi.org/10.1186/s42466-020-00059-z

Business Tech. (2023, March 4). South Africans are the biggest internet addicts in the world. *BusinessTech*. https://businesstech.co.za/news/lifestyle/666999/south-africans-are-the-biggest-internet-addicts-in-the-world/

Carr, C. T., & Hayes, R. A. (2015). Atlantic *Journal of Communication Social Media: Defining, Developing, and Divining*. *Atlantic Journal of Communication*, 23(1), 46–65. https://doi.org/10.1080/15456870.2015.972282

Clarke, V., & Braun, V. (2017). *Thematic analysis. In Journal of Positive Psychology* 12(3), 297–298. Routledge. https://doi.org/10.1080/17439760.2016.1262613

Correa, T., Hinsley, A. W., & de Zúñiga, H. G. (2010). *Who interacts on the Web? The intersection of users' personality and social media use. Computers in Human Behavior*, 26(2), 247–253. https://doi.org/10.1016/j.chb.2009.09.003

Cybercrime statistics. (2022). https://surfshark.com/research/data-breach-impact/statistics

El, Y., Ghouddana, H., & Rojas Barcelona, A. (2022). *Defining tools for phishing campaigns*. (Bachelor's thesis, Universitat Politècnica de Catalunya).

Frauenstein, E. D., & Flowerday, S. (2020). Susceptibility to phishing on social network sites: A personality information processing model. *Computers & Security*, 94, 101862. https://doi.org/10.1016/j.cose.2020.101862

Gestão, R., Tecnologia, &, & Leopoldo, P. (2020). *Qualitative Methods of Analysis: An Example Of ATLAS.TI™ Software Usage Analise Qualitatica: Um Exemplo Do Uso Do*

Software ATLAS.TI™ Analisis Cualitativo: Un Ejemplo De Uso Del Software ATLAS.TI http://orcid.org/0000-0002-7012-0679https://orcid.org/0000-0002-7222-5589http://orcid.org/

Gichuru, M. J. (2017). *The Interpretive Research Paradigm: A Critical Review of IS Research Methodologies*. www.ijiras.com

Guest, G., Bunce, A., & Johnson, L. (2006). How Many Interviews Are Enough? An Experiment with Data Saturation and Variability. *Field Methods*, 18(1), 59–82. https://doi.org/10.1177/1525822X05279903

Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023). From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy. In *IEEE Access* (Vol. 11, pp. 80218–80245). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2023.3300381

Grix, J. (2019). *The Foundations of Research* (3rd Edition). https://books.google.co.za/books?hl=en&lr=&id=A5JKEAAAQBAJ&oi=fnd&pg=PP1&dq=GRIX+2010+PARADIGMS&ots=CSUXZnuIoK&sig=K3TTnkGaGjvIhmmga1NOBHft5QA#v=onepage&q=GRIX%202010%20PARADIGMS&f=false

Kancherla, J. (2020). *Motivational and Psychological Triggers in Social Engineering*. https://ssrn.com/abstract=3750474

Kelley, C. M., Hong, K. W., Mayhorn, C. B., & Murphy-Hill, E. (2012). Something smells phishy: Exploring definitions, consequences, and reactions to phishing. *Proceedings of the Human Factors and Ergonomics Society*, 2108–2112. https://doi.org/10.1177/1071181312561447

Kemp, S. (2023, February 13). *Digital 2023: South Africa — DataReportal – Global Digital Insights*. https://datareportal.com/reports/digital-2023-south-africa

Kinswood, C. (2016, August 22). *Don't Let Angler Phishing Lure Your Customers into a Trap*. Proofpoint. https://www.proofpoint.com/au/blog/dont-let-angler-phishing-lure-your-customers-trap

Kivunja, C., & Kuyini, A. B. (2017). Understanding and Applying Research Paradigms in Educational Contexts. *International Journal of Higher Education*, 6(5), 26. https://doi.org/10.5430/ijhe.v6n5p26

Korstjens, I., & Moser, A. (2018). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice*, 24(1), 120–124. https://doi.org/10.1080/13814788.2017.1375092

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

Leighton, K., Kardong-Edgren, S., Schneidereith, T., & Foisy-Doll, C. (2021). Using Social Media and Snowball Sampling as an Alternative Recruitment Strategy for Research. *Clinical Simulation in Nursing*, 55, 37–42. https://doi.org/10.1016/j.ecns.2021.03.006

Lestraundra, A. (2023). *The Rise of Paid Verification on Social Media*. HubSpot. https://blog.hubspot.com/marketing/paid verification#:~:text=With%20the%20advertising%20challenges%20social,offer%20is%20to%20be%20determined.

Lincoln, Y., & Guba, E. (1985). *Naturalistic inquiry*. Sage Publications. Lincoln YS, Guba EG. Naturalistic inquiry. California: Sage Publications.

Longtchi, T., Montañez Rodriguez, R., Al-Shawaf, L., Atyabi, A., & Xu, S. (2022). *Internet-based Social Engineering Attacks, Defenses and Psychology: A Survey A Preprint*.

Luo, X., Zhang, W., Burd, S., & Seazzu, A. (2012). *Investigating phishing victimization with the Heuristic Systematic Model: A theoretical framework and an exploration*. https://doi.org/10.1016/j.cose.2012.12.003

Manyam, S. (2022). *Artificial Intelligence's Impact on Social Engineering Attacks*. https://opus.govst.edu/capstones/561

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

Moerane, P. (2016). *A study of graduates' experience of unemployment in Durban, South Africa*. (Masters dissertation, University of KwaZulu-Natal).

Moore, K., & McElroy, J. C. (2012). The influence of personality on Facebook usage, wall postings, and regret. *Computers in Human Behavior*, 28(1), 267–274. https://doi.org/10.1016/j.chb.2011.09.009

Moran, M. (2023, January 17). *Social Media Statistics (How Many People Use Social Media?)*. https://colorlib.com/wp/social-media-statistics/

Noble, H., & Heale, R. (2019). Triangulation in research, with examples. Evidence-based nursing, 22(3), 67–68. https://doi.org/10.1136/ebnurs-2019-103145

O'Hagan, L. (2018). *Angler phishing: Criminality in social media. Proceedings of the 5th European Conference on social media, ECSM 2018*, 190–197. https://books.google.co.za/books?hl=en&lr=&id=b09mDwAAQBAJ&oi=fnd&pg=PA190&dq=angler+phishing&ots=Al8wIopCwa&sig=8WpADxkiJgEO9IqOmVeCW_dqHAA&redir_esc=y#v=onepage&q=angler%20phishing&f=false

Ollmann, G. (2002). *The Phishing Guide Understanding & Preventing Phishing Attacks*. September 2002.

Parrish, J. L., Bailey, J. L., & Courtney, J. F. (n.d.). A Personality Based Model for Determining Susceptibility to Phishing Attacks. *Little Rock: University of Arkansas*, 285-296.

Petrosyan, A. (2023, May 22). *Worldwide digital population 2023*. Statista. https://www.statista.com/statistics/617136/digital-population-worldwide/#statisticContainer

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

Proofpoint. (n.d.). *Q4 2016 & Year in Review: Threat Summary*. Retrieved April 15, 2023, from https://www.proofpoint.com/sites/default/files/proofpoint_q4_threat_report-final.pdf

Proofpoint. (2016, August 30). *Fraudulent Social Media Accounts Phish For Banking Credentials | Proofpoint*. https://www.proofpoint.com/us/threat-insight/post/fraudulent-social-media-accounts-continue-phish-banking-credentials

Proofpoint. (2022). *A year in review*. https://www.proofpoint.com/uk/resources/threat-reports/state-of-phish

Prosek, E. A., & Gibson, D. M. (2021). Promoting Rigorous Research by Examining Lived Experiences: A Review of Four Qualitative Traditions. *Journal of Counseling and Development*, *99*(2), 167–177. https://doi.org/10.1002/jcad.12364

Rodolfo, B., Mason, M. C., & Nassivera, F. (2011). *Green Marketing and Renewable Energy: Evidence on Motivations and Behaviour in the Aquacultural Market*. www.davidpublishing.org

Ryan, T., & Xenos, S. (2011). Who uses Facebook? An investigation into the relationship between the Big Five, shyness, narcissism, loneliness, and Facebook usage. *Computers in Human Behavior*, 27(5), 1658–1664. https://doi.org/10.1016/j.chb.2011.02.004

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet,* 11(4). MDPI AG. https://doi.org/10.3390/FI11040089

Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). *A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures.* In *Applied Sciences (Switzerland),* 12(12). MDPI. https://doi.org/10.3390/app12126042

Specialised Security Services. (2023). *The Ant Ranch Ponzi Scheme*. https://mikebh.link/e48647?mc_cid=0384a2fe15&mc_eid=UNIQID

Sultan, A. (2019). *Improving Cybersecurity Awareness in Underserved Populations*. (White paper, Center For Long-Term Cybersecurity. San Francisco)

Sutherland, E. (2017). Governance of Cybersecurity - The Case of South Africa. *The African Journal of Information and Communication (AJIC)*, *20*. https://doi.org/10.23962/10539/23574

Tredger, C. (2023, June 15). Digitisation, social media fuelling rampant fraud in SA. *Information Technology Web*. https://www.itweb.co.za/article/digitisation-social-media-fuelling-rampant-fraud-in-sa/KzQenMjyB9B7Zd2r

Van Manen, M. (2017). But Is It Phenomenology? *Qualitative Health Research,* 27(6), 775–779. SAGE Publications Inc. https://doi.org/10.1177/1049732317699570

Vasquez, M. H. (2018). *The financial crimes management of account takeover fraud* (Masters dissertation, University of Texas at Austin).

Wang, J., Li, Y., & Rao, H. R. (2017). Coping responses in phishing detection: An investigation of antecedents and consequences. *Information Systems Research*, *28*(2), 378–396. https://doi.org/10.1287/isre.2016.0680

Wang, Z., Sun, L., & Zhu, H. (2020). Defining Social Engineering in Cybersecurity. *IEEE Access*, *8*, 85094–85115. https://doi.org/10.1109/ACCESS.2020.2992807

Wood, B. D., & Vedlitz, A. (2007). Issue definition, information processing, and the politics of global warming. *American Journal of Political Science*, 51(3), 552-568.

YouMail. (2023, April 25). Survey Reveals Scale of Brand Imposter Risks to Consumers. *YouMailPS*. https://blog.youmailps.com/survey-reveals-scale-of-brand-imposter-risks-to-consumers

Zhuo, S., Biddle, R., Koh, Y. S., Lottridge, D., & Russello, G. (2023). SoK: Human-centered Phishing Susceptibility. *ACM Transactions on Privacy and Security*, *26*(3). https://doi.org/10.1145/3575797

APPENDIX A: Ethical Clearance

Graduate School of Business Administration
University of the Witwatersrand, Johannesburg

Wits Business School Ethics Committee
Constituted under the University Human Research Ethics Committee (Non-Medical)

Ethics Clearance Certificate

Ethics protocol number: WBS/DB2520298/309
This certificate is only valid with a legitimate ethics protocol number and signed by the Researcher (below).

Project title	Angler phishing attacks on social media users in South Africa
Investigator / Researcher	Ms Kemisetso Mogashoa
Nature of Project	MM (Digital Business)
Decision of the Committee	Approved, provided stakeholders and participants are guaranteed confidentialty.
Issue Date of Certificate	9/11/2023
Expiry date	Date of submission of the project / research report
Chairperson	Dr Pius Oba ☎ +27 11 717 3976 +27 82 733 6587 pius.oba@wits.ac.za

Declaration by Researcher

One copy must be signed by the Researcher and returned to the Chairperson of the Wits Business School Et Committee.

I fully understand the conditions under which I am authorized to carry out the abovementioned research a guarantee to ensure compliance with these conditions. Should any departure to be contemplated from the research procedure as approved I undertake to resubmit the protocol to the Committee.

Signature

13/09/2023
Date:

APPENDIX B: Participant Information Request

Dear Sir / Madam

I hope this finds you in good health,

My name is Kemisetso, I am a Masters candidate in Digital Business at Wits Business School, student number is 2520298 at the University of the Witwatersrand, Johannesburg. My supervisor is Prof Nixon Ochara I am conducting a research study about Angler Phishing attacks. The study title is Angler phishing attacks on social media users in South Africa.

I am inviting you to take part in an interview if you have experienced Angler Phishing attacks. If you decide to take part, your participation in this research study will last about 60 minutes.

With your permission, I would like to record the interview for reference purposes. This data will be stored in my iCloud and One Drive for the remainder of the study and/or deleted after 5 years. Only the researcher and mandated stakeholders at the university will have access to the data.

The interview will be confidential and anonymous. When I share the results of the research study, I will not include your name or anything else that could identify you. With your permission, other researchers may use the data collected from this research study, but your name and any personal information will not be used or passed on.

If you decide to take part in the research study, it should be because you want to volunteer. You do not have to take part. You can stop being in the study at any time. You do not have to answer any questions if you do not want to. You will not get any direct benefits if you choose to join the research study. You will not lose any services, benefits or rights you would normally have if you decide not to join. Taking part in the research study will not cost you unless travel or data is required to have interviews in person or online You will not be paid for being in this research study. Your travel/data costs to attend the interview will be reimbursed to a maximum of R100.

The risks for this research study are no more than what happens in everyday life / some of the questions asked may make you feel sad or upset. If this happens, I will stop the interview recording and continue another time.

This research study will be written up as a research report. The report will be available on the university library website. If you would like to receive a summary of this report, I will be happy to send it to you.

If you have any questions during or afterwards about this research study, feel free to contact me or my supervisor on the details listed below. If you have any concerns or complaints about the ethical procedures of this research study, you are welcome to contact the University Human Research Ethics Committee (Non-Medical), telephone +27(0) 11 717 1408, email hrecnon-medical@wits.ac.za.

Yours sincerely,

Kemi

Researcher:
Kemisetso Mogashoa, 2520298@students.wits.ac.za , 0658901588

Supervisor:
Professor Nixon Ochara, Nixon.Ochara@wits.ac.za, 072 170 4560

APPENDIX C: Consent Form

Title of project: Angler phishing attacks on social media users in South Africa

Name of researcher: Kemisetso Mogashoa

I, …….., agree to participate in this research project.

I agree to the following:

(Please circle the relevant options below)

The research study was explained to me. I understand what this study is about.	YES NO
I understand that I can volunteer to take part in the study	YES NO
I agree that the interview/focus group/other activity may be audio recorded	YES NO
I agree that direct quotations from my interview/focus group/other activity may be used by the researcher in their research report/ manuscript/book chapter	YES NO
I agree that my participation will remain anonymous (my name or other identifying data will not be used by the researcher in their research report/manuscript/book chapter)	YES NO
I agree that other researchers may use the information I provide in my interview/focus group/other activity (depending on their own ethics clearance being obtained) but my name and any personal information will not be used or passed on	YES NO

…… (signature)
…… (name of participant)
…… (date)

…… (signature)
…… (name of researcher/person seeking consent)
…… (date)

APPENDIX D: Research Instrument

Concepts	Definitions	Interview Questions
Social media	Social media are Internet-based channels that allow users to opportunistically interact and selectively self-present, either in real-time or asynchronously, with both broad and narrow audiences who derive value from user-generated content and the perception of interaction with others (Carr & Hayes, 2015)	1. How many social media accounts do you have? 2. How many hours per day do you usually spend on social media? 3. Which social media account would you say consumes most of your time? 3. What type of content do you usually engage with? Engage in this context meaning, liking of posts, commenting, sharing etc. 4. Do you generally follow South African businesses who have social media accounts?
Openness	*Openness to experience* is the desire to seek out new experiences without anxiety and an appreciation of different ideas and beliefs (Parrish et al., n.d.). They have a vivid imagination and prioritise learning (Frauenstein & Flowerday, 2020).	1. Do you frequently explore new websites, forums, or online communities? 2. Have you ever clicked on a link from an unknown or known source which you thought was reliable out of curiousity? 3. How open are you to exploring new online platforms and technologies?
Conscientiousness	People who exhibit *Conscientiousness* are upright, reliable and diligent. They tend to follow the rules and are law-abiding citizens (Frauenstein & Flowerday, 2020).	1. Do you carefully review messages on social media before taking any action? 2. What do you do to verify the sender's legitimacy when you receive messages or comms from an unfamiliar source?
Extraversion	Is the personality trait associated with enthusiasm (Frauenstein & Flowerday, 2020). They tend to be sociable, energetic, talkative, thrive off energy and have dominating personalities.	1. Would you say you generally regard yourself as an over-sharer or as a private person? 2. Are you likely to engage in online communication with strangers or likely to ignore them?
Agreableness	Are people who have a high tolerance, usually compassionate, modest, polite and can be seen as naïve because of their trusting nature. They often believe people are genuinely honest people, which can be a false misconception.	1. Do you tend to trust people, both in online and offline interactions? 2. How would you describe your approach to engaging with new online connections?
Neuroticicism	People with *Neuroticism* frequently experience unpleasant emotions including pessimism, humiliation and guilt. They typically have low esteem, are anxious and occasionally irrational.	1. Do you find yourself anxious or stressed when receiving unexpected or urgent messages? 2. Have you ever felt overhwhelmed or panick when receiving notifications from your financial insitiution? 3. What do you typically do with messages that require you to take an action of some sort " click here urgently" "update this before xyz"?
Information Processing (Heureustic)	Heuristic processing can be explained as factors embedded within or surrounding a message such as format, length and subject (Luo et al., 2012). This can also be referred to as the visual quality of the message as it focuses on aspects such as logos, grammar, context and instructions in the message (Frauenstein & Flowerday, 2020).	1. Are you most likely to trust a business on social media if it has a verification tick? 2. Are you likely to trust a business on social media if the logo of the business is the legitimate logo associated with that brand? 3. Researcher will share an image with participants and ask them to spot the difference between the two url's.
Information Processing (Systematic)	Systematic processing is concerned with the message content and the validation of it thereof (Luo et al., 2012). It is no doubt that systematic processing therefore requires more effort and cognitive conscious to accurately process messages.	1. Would you say you usually skim posts by business accounts, or do you take your time to thoroughly go through the message and it's contents thereof? 2. Are you more likely to check the legitimacy of a message and it's content if it is relation to something that is of interest to you or sentimental to you? 3. Would you reckon a spelling mistake is a valid reason to not trust the legitimacy of a message?
Phishing susceptibility	The likelihood that a person would fall prey or become a victim to cybersecurity threats.	1. In your own simplified words, are you familiar with the word phishing and do you know any examples of a form of phishing? 2. If you reported a query via social media to a specific business and the business is likely to ask you to share your details via direct message (name, surname, account detail for resolution) would you normally ask what the purpose of sharing these are, or you would go ahead and provide them? 3. Have you ever reported a susciptious message to the relevant business/organisation? 4. Have you ever received cybersecurity training or awareness education on how to manage threats on social media? 5. How confident are you in your ability to identify a phishing message/attempt on social media? 6. Can you explain what two-factor authentication is? 7. What do you do to keep up with security controls for your applications?
Total		30 questions

APPENDIX E: ATLAST.ti Coding Report

ATLAS.ti Report

MMDB Experiences of phishing attacks on social media users

Codes

Report created by Kemisetso Mogashoa on 27 Jan 2024

- **Cybercriminals tactics**

Created: 2024/01/24 by Kemisetso Mogashoa, **Modified:** 2024/01/27 by Kemisetso Mogashoa

Groups:
- Phishing Experiences

- **Cybersecurity knowledge and training**

Created: 2024/01/24 by Kemisetso Mogashoa, **Modified:** 2024/01/27 by Kemisetso Mogashoa

Groups:
- Cybersurity Training and Awareness

Comment:
2024/01/27, 13:20, merged with
User understanding of phishing

- **Information Processing (Heuristic)**

Created: 2024/01/24 by Kemisetso Mogashoa, **Modified:** 2024/01/27 by Kemisetso Mogashoa

Groups:
- Information Processing (Heuristic vs Systematic)

Comment:
This image was shared with participants during the interview and they were asked to spot the difference for heauristic stimulation

---

- **Information Processing (Systematic)**

Created: 2024/01/24 by Kemisetso Mogashoa, **Modified:** 2024/01/27 by Kemisetso Mogashoa

Groups:
- Information Processing (Heuristic vs Systematic)

- **Personality types user resonates with**

Created: 2024/01/24 by Kemisetso Mogashoa, **Modified:** 2024/01/27 by Kemisetso Mogashoa

Groups:
- Personality Traits

Phishing

Created: 2024/01/25 by Kemisetso Mogashoa, **Modified:** 2024/01/27 by Kemisetso Mogashoa

Groups:
- Phishing Experiences

Comment:
2024/01/27, 13:21, merged with
Phishing Consequences

2024/01/27, 13:21, merged with
Phishing platform

2024/01/27, 13:21, merged with
Reasons for getting phished

2024/01/27, 13:21, merged with
Reporting fraud with Bank

Psychological impact on victim

Created: 2024/01/25 by Kemisetso Mogashoa, **Modified:** 2024/01/27 by Kemisetso Mogashoa

Groups:
- Phishing Experiences

Time spent on social media

Created: 2024/01/24 by Kemisetso Mogashoa, **Modified:** 2024/01/27 by Kemisetso Mogashoa

Groups:
- Social media footprint

Comment:
2024/01/27, 17:25, merged with
Engagement with businesses

2024/01/27, 17:25, merged with
Most used social media platform

2024/01/27, 17:25, merged with
Number of social media accounts

User online behaviour

Created: 2024/01/24 by Kemisetso Mogashoa, **Modified:** 2024/01/27 by Kemisetso Mogashoa

Groups:
- Cybersecurity Hygiene

Comment:
2024/01/27, 17:24, merged with
Cybersecurity behaviour

2024/01/27, 17:24, merged with
Responsiveness to unsolicted messages

APPENDIX F: Editing Certificate

Between the lines editing

Leatitia Romero
Professional Copy Editor and Proofreader
(BA HONS)

Cell: 083 236 4536
leatitiaromero@gmail.com
www.betweenthelineseditting.co.za

26 February 2024

To whom it may concern:

I hereby confirm that I edited the dissertation titled: "Angler phishing attacks on social media users in South Africa". Any amendments introduced by the author hereafter are not covered by this confirmation. Participants' verbatim quotes were not edited. The author ultimately decided whether to accept or decline any recommendations I made, and it remains the author's responsibility at all times to confirm the accuracy and originality of the completed work. The author is responsible for ensuring the accuracy of the references and its consistency based on the department's style guidelines.

Leatitia Romero

Affiliations

PEG: Professional Editors Group (ROM001) – Accredited Text Editor
SATI: South African Translators' Institute (1003002)
REASA: Research Ethics Committee Association of Southern Africa (104)