UNIVERSITY *of the*
WESTERN CAPE

Remedies to reduce user susceptibility to phishing attacks

by

Ashley Eventhia Maseko

(Student nr: 3725633)

Research report submitted in fulfilment of the requirements for the degree of

Master of Commerce in Information Systems

in the Department of Information Systems

Faculty of Economic and Management Sciences

University of the Western Cape

Supervisor: Prof. Joel Chigada

April 2023

Abstract

Organisations have been compelled to embrace digitisation, increasing their dependence on the internet and computer systems rather than on in-person interactions. These organisations have had to adjust to new societal norms of teleworking and social distancing. The new adjustments were because of the total nationwide lockdown enacted in response to the global Corona Virus disease (COVID-19) pandemic. Many organisations have adopted teleworking to become more agile, but in the face of escalating cybercrime, it has also exposed them to increased security vulnerabilities. The study's ultimate purpose was to report phishing attacks on financial institutions and offer remedial solutions that can be implemented to reduce user susceptibility. To answer the study's main objectives, a qualitative approach was adopted. Semi-structured interviews and interview schedules were used for data collection. The research discussed the two main theories governing the study: Routine activity and Rational choice theories. The rational choice theory describes the reasoning and motivations that underlie the choices made by offenders, whereas the routine activities theory explains the necessary conditions that must be present for a crime to happen. Thematic analysis was used to better understand the data by using codes to uncover commonalities or themes in the responses of the participants. Additionally, thematic data analysis enabled the researcher to report on solutions that met the objectives of the study. The patterns that emerged laid the groundwork for the discussion and allowed the researcher to make references and substantiate with literature from existing studies. The study revealed that users tend to disregard established protocols when engaging with systems, leading to an increased likelihood of organisations being successfully phished. Based on the findings, the recommendations focused on human centric approaches to effectively reducing the success rate of phishing attacks through coordinated efforts with close engagement between employees and Information Technology personnel.

Key words: Cybercrime; COVID-19; Financial Institutions; Phishing; Phishing attacks; Social engineering; Cybersecurity

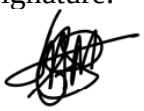
Declaration

I declare that ***Remedies to reduce user susceptibility to phishing attacks*** is my own work, that it has not been submitted for any degree or examination in any other university, and that all the sources I have used or quoted have been indicated and acknowledged by complete references.

This thesis will be submitted for examination after approval by my academic supervisor.

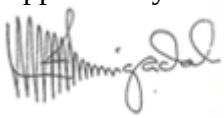
Full name: Ashley Maseko **Date**:21/04/2023

Signature:



.....

Approved by



.....

Professor Joel Chigada

Acknowledgments

The journey that I have been on completing my thesis has been nothing short of amazing and filled with lessons. I learned to believe in myself, and this journey enabled me to draw on my inner strength to keep going. I would like to extend my sincere thanks to my supervisor, Professor Joel Chigada; none of this could have been possible without his forceful, kind, patient, and motivating nature. He was very instrumental in my journey and words cannot express my gratitude to him for his invaluable patience and feedback. A special thanks goes out to the participants who consented to participate in the study as well as management who approved and supported me throughout the completion of my thesis, and more so during the data collection phase.

I am very happy that I never gave up however the biggest motivation for me to keep going was my parents Busi Maseko and Lawrence Maseko, my sister, Euginia Maseko and my son, Ethan Maseko, and niece Lisa Maseko whose encouragement, patience and love inspired me to keep going and strive to the finish line. This body of work would not have been possible without the help of the abovementioned individuals. This project showed me the significance of having a solid support system and how much it can help you stay motivated and accountable even when the going gets tough.

I would be remiss in not mentioning the God factor in all this and the role that prayer played in keeping me going. I thank God for bestowing wisdom on me and surrounding me with love. I would like to acknowledge the management of the financial institution for granting me permission to conduct this study with their employees. To all participants for this study, I thank you for your time, data and insights shared during the interviews. Without your inputs, I would not have completed this study. If there is anyone not mentioned, kindly accept my apologies. Your contributions towards this study are acknowledged.

Table of Contents

List of Tables

List of Figures

List of Acronyms

IDS – Intrusion Detection Systems

RAT – Routine Activity Theory

RCT – Rational Choice Theory

VPN – Virtual Private Network

SSL – Secure Socket Layer

URL – Uniform Resource Locator

SMS - Short Message Service

DNS - Domain Name System

MFA – Multi Factor Authentication

SMB – Small and Medium sized Businesses

IP – Internet Protocol

Chapter 1: Introduction

1.1. Introduction

Social engineering involves threat actors persuading a person or an organisation to dupe them into becoming victims and disclosing classified information. It thrives on deception and threat actors' prey on people using different guises in order to infiltrate their social interactions and obtain sensitive information (Ghasemi, Saadaat, & Ghollasi, 2019). This form of crime can be committed online using computers and the internet or face to face. According to Conteh and Schmick (2016) social engineering attacks have two forms: human and technological deployments. Human deployment entails threat actors wilfully obtaining personal information about a victim and building a relationship with the user. The threat actor employs a trusted party method where the victim is rendered vulnerable and coerced into divulging information. This information then adds to the puzzle that the threat actor, put together so that the information can be used to his/her advantage. Technological deployments known as technical attacks are more straightforward and can be launched via a variety of channels, including websites, email attachments, pop-up windows, and software programs.

Jain and Gupta (2022) define phishing as a type of identity fraud that involves tricking internet users into disclosing personal information such as login credentials, credit/debit card numbers, along with other critical information. Vayansky and Kumar (2018) explain that phishing attacks have a simple modus operandi that ensures that the phisher can conceal their location and operate from a place of complete anonymity, all they do is send an email, email redirects victim to a website, site steals information. According to Aldasoro *et al.* (2020:3) the purpose of imitating trusted senders is so that the criminals can gain the victim's trust.

Threat actors tend to mimic the identities or characteristics of people that the targeted users would likely trust or submit to, or they appeal to the things that would likely trigger the interests or curiosity of human users. For example, a notification that claims a user has won prizes and redirects the user to a fake uniform resource locator (URL) where she or he can enter personal details like login credentials in order to redeem their winnings. It is important to develop strategies that may be implemented to close gaps like these that threat actors frequently exploit. The study will gather data from employees of institutions in the Southern Suburbs in the Western Cape in order to deconstruct the elements involved in the human

deployment form of social engineering. Employees are human users who interact with platforms and systems daily in their place of work.

This study focuses on examining strategies that can be adopted to reduce user susceptibility to phishing attacks and limit losses within institutions in the financial industry. Shahbaznezhad, Kolini, and Rashidirad (2021) state that prior research has concentrated on phishing attacks from a narrow perspective of technical countermeasures, e-mail characteristics, information processing, and securing individual's behaviours to tackle existing gaps. This study identifies the factors that tend to contribute to the prevalence of phishing attacks and how they can be reduced. Additionally, the research explains the theories that underpin this investigation as well as the numerous factors that lead to the rise in phishing attacks. The philosophical approach that will be used to dissect these theories is also explained in detail.

1.2. Background to the study

The effects of social engineering attacks on people and businesses have been the subject of an in-depth investigation by many researchers. When considering the potential defences against attacks like phishing, it is important to understand that individuals' response bias, confidence, detection ability, and perception of repercussions all influence phishing-related decisions (Jampen, Gür, Sutter, & Tellenbach, 2020). According to Downs, Holbrook, and Cranor (2006:79) "before we can address the "people" side of phishing attacks, we must develop a better understanding of why people fall for these attacks and the extent to which people take advantage of available cues that might help them identify fraudulent emails and web sites". Khan *et al.* (2020) states that fintech users are frequently the victims of social engineering, in which hackers use a variety of ways to impersonate a legitimate person and obtain access to personal information such as password recovery. In line with this, the study will also examine phishing with fintech users as the main unit of analysis. Daengsi, Pornpongtechavanich, and Wuttidittachotti (2021) established that the financial sector accounted for ten percent of breaches at a sectoral level. As a result, the losses arising from these breaches affected not only financial institutions but customers and employees as well.

Most correspondence outside of telephonic calls between institutions and clients is done using emails. Emails are an integral part of virtually communicating, making them a plausible

attack vector for phishers when they target users (Baykara, & Gürel, 2018). As a result, it is important to understand the inner workings of phishing emails, including how they are presented, how to spot these emails, what they often ask for, and how they are laid out. The traditional phishing email tone capitalizes on fear, panic, and has requests that lean toward urgent action, causing panic or making the user to feel the need to respond right away. An example given by Iser and Brandtweiner (2022) is where a user receives an email saying that their account has been blocked. In this scenario, the subsequent steps to unblock the account would likely contain a phony link requiring the personal login details which the attackers then use to infiltrate the system.

Anti-phishing strategies, tools, and techniques are used to combat phishing; however, the primary goal is not to lower the likelihood of it happening but rather to significantly lower the success rate. Florêncio and Herley (2006) state that although there are several anti-phishing solutions that address frequently seen phishing attacks, the field is rapidly evolving. Therefore, a strong prevention strategy should be resilient to both predicted and observed attacks. Phishers can manipulate systems in a way that exploits the vulnerabilities of the internet, its users, and the general weak points of a system (Eian, Yong, Li, Qi, & Fatima, 2020). Although, systems change with time, phishers tend to adapt their strategies to target systems users and exploit existing vulnerabilities.

Users who lack sufficient training or security awareness, as well as organisations that do not implement reinforcements to strengthen their systems, are more vulnerable to phishing attacks. Wang, Herath, Chen, Vishwanath, and Rao (2012) investigated how users' attention to visual cues and signs of phishing deception affect their decision-making process. The authors furthermore indicated that phishing emails frequently contain visceral triggers, which means there is a focus on the need for quick action on the part of the user. These are psychological tricks phishers use to get people to process information quickly and superficially causing them to make poor decisions. According to Ghazi-Tehrani and Pontell (2021) phishing is the major method that threat actors use to breach or infiltrate networks for ransomware and is directly responsible for financial fraud.

1.3. Statement of the research problem

The global Coronavirus pandemic provided cybercriminals with an ideal opportunity to exploit cybersecurity vulnerabilities and to launch a slew of cyberattacks on various sectors of society (Minnaar & Herbig, 2021:155). Chigada and Madzinga (2021) state that cyberattacks and threats against financial institutions soared by more than 238 percent (238%) across the globe between February and April 2020. Threat actors are increasingly leveraging Covid-19 messaging to perform phishing and malware attacks and take advantage of less protected business networks (Writer, 2020). According to Wang, Herath, Chen, Vishwanath, and Rao (2012) such attacks make customers less trusting towards email-based correspondence with businesses, heightening customer's overall resistance to online communication and this drives up the cost of doing business online. APWG (2021:3) states that "phishing attacks more than doubled since early 2020". In addition, the APWG and its global research partners recorded between 68000 and 94000 to 260642 phishing attacks in the month of July 2021.

Allianz (2021) states that financial institutions are becoming increasingly vulnerable to cybercrimes and social engineering attacks like phishing due to over-reliance on new technology. "Social engineering has become a significant threat, affecting both the average user and big corporations" (AL-Otaibi & Alsuwat, 2020:6378). This purports that the existential realities of social engineering and the number of businesses and individuals that fall victim are increasing. Networks are not the only potential source of risk in an organisation. Users also play a pivotal role in enabling or deterring business infiltration, network, or system compromise by threat actors. Shirsat (2018) found that although there are numerous frameworks for exploring and analysing phishing as a type of social engineering, there isn't much literature that addresses the topic of phishing from a broader viewpoint. This limited viewpoint has created a gap in which not enough research has been done on the remedies that organisations can adopt to reduce user susceptibility to phishing. Phishing attacks have increased because of enabling factors within the remote working structures of employees. Today, large, and small businesses more than ever rely on computer systems, mobile devices, and the internet to work, communicate, process payments, and do business. Having said that, the more people work remotely online, the more opportunities there are for threat actors to exploit systems and prey on unsuspecting users. This has become a serious challenge for many internet users.

According to the Monetary Authority of Singapore (2021) the rising popularity of remote working has altered the overall control environment in which employees work. In a dispersed remote working environment, risk management tends to be more difficult than in an office setting where employees are co-located. This report by the Monetary Authority of Singapore (2021) suggests that poorly regulated employees' remote access to sensitive information increases the danger of financial institutions being compromised. This is when employees have more access to systems than they require to execute their duties (Borkovich & Skovira, 2020). Many institutions and individuals have been compromised because of this over-access combined with a lack of adequate user education about phishing and anti-phishing techniques. According to a report by Accenture (2020:7) South Africa has the third-highest number of cybercrime victims across the globe. This ranking is attributable to various factors like: a lack of adequate investment in cybersecurity, unfledged cybercrime legislation and law enforcement training and the public having poor understanding of cyber-threats.

1.4. Research question

The primary research question of the study:

What remedies can be adopted to reduce user susceptibility to phishing attacks?

1.5. Research objectives

The main objectives of this thesis are:

i. To establish the solutions that can be put in place to manage the prevalence of phishing attacks.
ii. To determine the extent to which human beings contribute to the success of phishing attacks.
iii. To determine how insufficient technical and organisational security measures expose financial institutions to phishing attacks.
iv. To establish the interventions financial institutions can put in place to mitigate the risks caused by phishing attacks.

1.6. Structure of dissertation

The section gives an overview of the process used to choose the research methodology, paradigm, and sampling techniques that governed the study. Additionally, each chapter describes how these research elements impacted how the study was designed, structured, and

executed. Holden and Lynch (2004:397) assert that, *"research should not only be "methodologically led," but that the methodology chosen should also be in line with the researcher's philosophical position and the social science phenomenon being studied"*. A qualitative research methodology was used in this study and the third chapter shed lights on the consequences if this approach for this study. The application of this approach makes it possible to investigate and interpret intricate social constructs while devoting considerable time exploring and comprehending human behaviours without focusing on statistical or numeric analysis (Pacho, 2015). According to Alase (2017) with this qualitative approach the researcher is able to apply their interpersonal skills and sound judgement to explore the study in a way that adds value. The study adopted an interpretive research paradigm. The interpretive paradigm seeks to comprehend reality as it is through the emotional experiences of people. Furthermore, *"the interpretivist approach employ methods that focus on meaning rather than measurement, like participant observation or interviewing, which is based on the arbitrary relationship between the researcher and the subject"* (Antwi & Hamza, 2015:218). This made the methodology suitable for the study given its capacity to offer insider insights that are derived from real life experiences of individuals influenced by their cultures, and belief systems. In qualitative research, sample sizes are commonly small to allow for a thorough case-oriented analysis of the sample (Vasileiou, Barnett, Thorpe, & Young, 2018). It is important to fully understand the subset chosen in order to ensure sample adequacy, relevance, and confidence that it accurately represents the entire population. Sixty employees made up the population, and fourteen people were sampled from it. The convenience sampling approach was adopted along with a qualifying criterion that is explained in detail in chapter three.

The five chapters that make up this thesis comprise of the following:

Chapter One: Introduces the research by stating the problem the questions and objectives that guide the research. This chapters also provides justification for the study, and the background information on phishing as a form of social engineering.

Chapter Two: Introduces the literature that underpins the study. Routine activity theory and rational choice theory are the two theories that the study uses to explain rational choice and how decisions are made that either contribute to or deter criminal conduct. In addition to discussing the different kind of phishing attacks, this chapter thoroughly covers related concepts on cybersecurity, information security and other security breaches. This

examination also enables a greater comprehension and justification of the theories in terms of how they relate to the research problem. Gaps in existing frameworks are also examined.

Chapter Three: Provides an explanation of the research methodology chosen and how it connects to the research questions. The chapter also discusses the chosen research design, participant selection criteria, data collecting, documentation, and analysis procedures, as well as the sequence of events from the commencement of data collection to the analysis and application of the findings to the study's overarching goals.

Chapter Four: Thematic analysis of data is the focus of this section. The findings are presented throughout the chapter in terms of the qualitative information gathered. The chapter highlights the significant conclusions from the data gathered, using themes to ensure that interpretations are organized into meaningful and comprehensible parts that truly reflect the responses.

Chapter Five: This chapter derives conclusions from the study's findings while also basing the conclusion on the purpose of the study, research objectives, research questions. Additionally, this chapter also explains the implications of the findings, gives follow up recommendations and discusses the limitations and contributions of the study.

1.7. Chapter summary

This chapter has provided a synopsis of the thesis by highlighting some of the previous research on phishing attacks and user susceptibility. In doing so, the chapter describes briefly what social engineering is and what phishing is, how it affects users, and the complexity of threat actor tactics and how these constantly evolve. The chapter also provided a clear picture of why phishing attacks have been on the rise and the environments that allow such attacks to thrive. In presenting this information the study also stresses the need for anti-phishing strategies that partner both human element and system reinforcement. The effects of inadequate end user education and other forms of reinforcement are examined in connection to how these factors raise attack susceptibility and success rates. The existing gaps in the literature are also discussed as they are material to this investigation, along with previous studies done by other researchers on phishing. Phishing attacks have become a worldwide phenomenon that thrives on the flaws and vulnerabilities of systems and people.

Chapter 2: Literature Review

2.1. Introduction

This chapter discusses existing research by providing an overview of previous studies on the impact of phishing attacks on many users and organisations. The chapter describes the theoretical underpinnings of the study that can be employed to understand cybercrime and the factors that influence whether online crimes occur. The study unpacks the theoretical framework that will serve as the foundation for the investigation covered in this thesis. To highlight the scenarios in which such attacks typically flourish, the first section of this chapter will discuss the "who, when, where, what, why, and how" elements that relate to cybercriminal operations. These elements are explained in order to give an overview idea of how phishing works. Two criminology theories guide this study, and these are the Routine Activity theory and the Rational Choice Theory. The Routine Activity Theory theoretical framework is discussed at length in this chapter along with the key role players in the occurrence of a crime. Rational Choice Theory explains threat actors as rational beings that decide for or against committing a crime as influenced by the perceived benefits.

The third section addresses the overview of the different types of phishing attacks. The fourth section will assess the extent to which humans contribute to the success of phishing attacks. The fifth section will discuss the effect of inadequate organisational and technical security measures on institutions when it comes to phishing. The sixth section will include the recommendations on countermeasures that can be implemented to reduce the prevalence of phishing attacks. The seventh section speaks to the phishing detection approaches that organisations can adopt. The eighth section identifies gaps in existing literature.

2.2. Theoretical works guiding the study

“A theoretical framework is a structure that guides research by relying on a formal theory, the framework is constructed by using an established, coherent explanation of certain phenomena and relationships” (Eisenhart, 1991: 205). A theoretical framework provides a well-supported rationale for conducting a study and assists the reader in comprehending the researcher's viewpoint. According to Simon and Goes (2011) the purpose of the theoretical framework is to assure the reader that the study is factual and credible, rather than based on intuition or speculation. The current study is guided by the Routine Activity and Rational Choice theories, which are utilised to understand crime through the perspective of everyday activities

and evaluative choices. The theories will be used to gain a deeper understanding of how a lack of adequate security reinforcements allows for social engineering attacks like phishing to continue thriving during Covid-19. The research investigates the strategies used by motivated criminals to improve the success rate of their attacks. It will also look at how the right targets (inexperienced users) make financial institutions more vulnerable, and how the lack of skilled guardianship raises the risk of being compromised.

2.2.1. Routine Activity Theory (RAT)

Horgan, Collier, Jones, and Shepherd (2021:3) describe the RAT as a school of thought that holds a relationship between "location, time, and human behaviour" which is a useful means of better understanding online victimisation and cybercrime dynamics. The interconnections between these elements influence where, when, and whom the attack is directed towards. Horgan, Collier, Jones, and Shepherd (2021) also propose that three elements come together in this theory: a motivated perpetrator, a suitable target, and the lack of a capable guardian. Jakobsson and Myers (2006, cited in Chaudhry, Chaudhry, and Rittenhouse 2016) state that phishing scams consist of three elements which describe the modus operandi for most attacks: lure, hook and catch. The motivated offender uses lures and hooks that are appropriate for the target. The absence of a capable guardian has an impact on the offender's ability to successfully catch and compromise the target. “The core premise of RAT is that the potential for crime to succeed exists in a social setting where offenders feed on everyday norms, a sequence of routine behaviours that eventually take on a pattern” (Herbig & Warchol, 2011:5). Furthermore, the theory does not consider the offenders' individual history as potentially linked to the motivation for certain actions. It instead favours examining the structural factors that may help to explain how crime is distributed throughout society.

Offenders also decide whether to commit a crime based on the suitability of a target and the presence or absence of a capable guardian who can intercept or prevent the crime from occurring (Nickerson, 2022). There is a high prevalence of coronavirus-themed phishing attacks that utilise fear to ensnare weak individuals or system users while exploiting the teleworking set-up to cause disruption in the workplace (Ahmad, 2020).

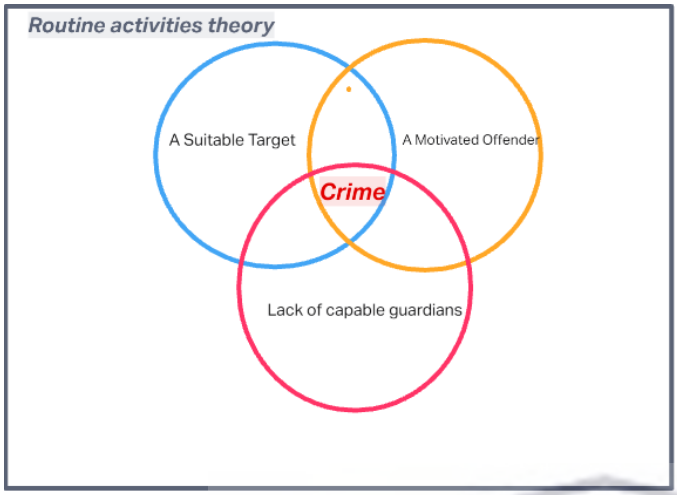


Figure 2.1: The Routine activities theory model by Abt (2017)

The point at which the three elements of the Routine activity theory converge, is when a crime occurs. This is illustrated by figure 2.1, an extract from Hirschfield, Johnson, and Bowers (2001:6).

According to Felson (1987:913) a perpetrator is driven for a variety of reasons. Zipf coined the phrase "Principle of Least Effort" in the 1950s to describe how people typically seek for the quickest, least time-consuming, and most straightforward ways to do tasks. “In order to make the least amount of effort, one must avoid wasting calories, time, or trip distance. If offenders travel minimal distances and often carry out illegal activities while enroute to other ones, then their routines will set the stage for the illegal opportunities which come their way. Criminals are more likely to take advantage of the targets that are convenient, offer little to no resistance, and are easy to find, using lazy reasoning and taking easy action, this then leaves no challenge. Zhu, Zhang, Wang, Q.A., Li, and Cai (2018) define how humans interact with one another in space. “RAT is not concerned with individual characteristics but rather the situational and structural dimensions conducive to victimization” (Howell, Burruss, Maimon, & Sahani, 2019: 539).

Pratt and Turanovic (2016:337) posit that at the point of convergence of the three elements (i.e a motivated perpetrator, a suitable target, and an absent capable guardian that is when a crime can occur). If any one of the elements aren’t present a crime cannot occur, so the prevalence of the crime has more to do with convergence leading to opportunity, and very little to do with chance on its own. The researchers also discuss how crime thrives in "routines" and suggest that with RAT, victimisation and crime are driven more by common

daily activities like leaving the house and going to work than by social pathology or risky behaviour. A routine is a set of repeated actions. In this theory, we establish how routines, opportunity and converge makes the crime. Numerous investigations have been carried out to support the principles of the routine activity theory; these studies serve as the cornerstone of the current study.

2.2.1.1. Ten principles of opportunity and crime

Neelima and Chennapalli (2022:55) define "opportunity as an occasion or situation that makes it possible to do something that you want to do or have to do or presents the possibility of doing something". There are ten principles defined by Felson, and Clarke (1998:9). Some of these principles intertwine with the routine activity theory, and the offender takes advantage of the window of opportunity depending on the suitability of the target and the degree of susceptibility, particularly in cases where the capable guardian is not present. According to the proverb "Opportunity makes the thief," committing a crime necessitates more than just the existence of a willing offender (Madero-Hernandez, & Fisher, 2012:1). In addition, the researchers add that, "even the most motivated offender cannot commit a crime unless an opportunity to carry out illegal activity presents itself".

- *Opportunities play a role in causing all crime* – without opportunity and a platform to commit a crime, a crime cannot occur. Madensen (2016:384) states that "opportunity can lead to crime in two different ways. The first necessary condition for crime is opportunity, which is an encounter, a situation, or an environment that is then identified and exploited. Secondly, opportunities may potentially become catalysts for criminal activity; attractive opportunities to commit crime may persuade law-abiding people to engage in actions they would typically consider to be unacceptable".
- *Crime opportunities are highly specific* - Felson and Clarke (1998:11) hold that crime should not be explained from a generic one size fits all perspective, as it is a concept that cannot be explained by a single element. The opportunities for crime are influenced by a variety of factors, making them very particular to each type of offense and criminal subset.
- *Crime opportunities are concentrated in time and space – "Crime has a tendency to concentrate in time, space and other dimensions along which it occurs"* (Farrell, 2015:233). Additionally, elements like the uneven distribution of people and things in varying spaces and times may create conditions for crime to occur at specific time and

places. Consequently, the term "crime hotspots" is coined to characterize locations very likely to have higher crime rates than other. According to Farrell (2015:235) another concept created to explain the crime concentration theory is “crime spree or crime spate” which typically refers to more than two comparable crimes in a short period of time, implying they are serious close repetitions.

- *Crime opportunities depend on everyday movements* – Crime opportunities depend on people engaging in regular, everyday behaviours, some of which may result in a prospect that threat actors purposefully seek to exploit after having discovered it. These opportunities are shaped by everyday movements, according to Olofinbiyi and Singh (2020:225) explain that as these opportunities shift *“offenders and their targets also shift in accordance with their activities such as trips to offices, schools, social/recreational settings”*.
- *One crime produces opportunities for another* – Any covert crime puts persons at risk of committing another unlawful conduct. When several criminal acts result from a single conduct that is carried out, both the actual crime and the effort put in to hide the crime may result in even more criminal activity.
- *Some products offer more tempting crime opportunities* - As most products get older, the danger of theft decreases due to their falling worth (unless they become antiques). Cars are an exception, as their rates of theft rise with time (Clarke & Newman, 2005). The level of temptation for a crime opportunity for one product may differ from another depending on the level of offender interest and motivation which determines the extent to which the offender pursues the product.
- *Social and technological changes produce new crime opportunities* – As technology develops new products, there are also new opportunities for crime, particularly when those products are valuable enough to be stolen, have a large market, or are in high demand.
- *Opportunities for crime can be reduced* – Making sure the car is locked, the luggage are secured, the machine is locked, and all other activities that minimize the potential for effective targeting or susceptibility all contribute to reducing the opportunity for crime. The strategies used must be adjusted for each specific situation.
- *Reducing opportunities does not usually displace crime* - There are various approaches to lowering the likelihood of crime however they only serve to

disperse criminality rather than to prevent it. According to Felson and Clarke (1998) the "displacement" theory states that crime moves about in five different ways:

From one site to another geographically; shifting from one time to another chronologically; shifting from one goal to another tactically. One technique of committing crime can take the place of another; similarly, one form of crime can take the place of another.

- *Focused opportunity reduction can produce wider declines in crime* – In some instances reducing window of opportunity also translates into capping the amount of crime that can take place successfully. Alabi, Adeleke, and Olajide (2021) assert that not all opportunities lead to crime, but every illegal act needs an opportunity. Furthermore, in circumstances where crime is likely to occur, opportunity becomes the deciding limiting factor of crime outcome. Threat actors generally have no control over the environment and the circumstances that allow for crime are sometimes uncommon, unlikely, or avertible.

2.2.1.2. A suitable target

A person or piece of property that the criminal might threaten is a viable target. Felson favours the term "target" to "victim" because it emphasizes the fact that most crimes are committed to gain things, hence the "victim" may not be present when the crime is committed (Felson & Clarke, 1998). The four factors that establish a target's desirability, affecting the likelihood that they would be targeted by the offender are: value, inertia, visibility, and accessibility (Leukfeldt & Yar, 2016). The term VIVA stands for Value, Inertia, Visibility and Accessibility and it is used to examine the primary factors that determine the extent to which a suitable target is likely to be attacked by motivated offenders. These elements affect the likelihood that an attack will succeed at the point of convergence that is defined by the Routine Activity Theory where a motivated offender, a suitable target and a missing capable guardian come together.

- *Value*

For the offender to develop keen interest in a target there must be something perceived to be possessing a presumed value. The value of information comes from what it can do for the offender, which is why, as Wall (2007:36) points out, offenders focus on gathering information to reap its benefits by extracting its value.

- *Inertia*

As described by Cohen and Felson (1979: 588) “refers to an object’s physical properties about size, weight and shape which defines the ease with which it can be removed”. According to Buil-Gil, Lord, and Barrett (2021) the concept of inertia in relation to cybercrime refers to the amount of data included in electronic files and their technical specifications, which provide some resistance to the target's ability to take or duplicate the information. The use of encryption may be seen as another form of inertia since this measure makes it more difficult for criminals and threat actors to steal or compromise sensitive data from infected computers and files.

- *Visibility*

A good target is one that the offender can easily locate without exerting too much effort (Schreck, 2017). The researcher further explains that those who draw attention to their wealth, for instance will be more visible or noticeable to the potential robbers than those who do not. The crime cannot be committed if the target is hidden from the offender's view and if the offender is unaware of any nearby targets. As the principle of least effort has already shown, criminals frequently use lazy reasoning since they don't want to exert too much work. Targets that are in plain sight are far easier for motivated offenders to attack than those that must be sought for.

- *Accessibility*

Accessibility makes it simple for an offender to get to the target and then leave the crime’s scene easily. The desirability of a target for theft is directly influenced by accessibility (Shaik, & Oliveira, 2019). According to Jansen and Leukfeldt (2016:81) “accessibility refers to weaknesses in software that can be used by fraudsters to attack customers”. These weaknesses can take many different forms, such as holes in security structures or software setup, systems lacking adequate security reinforcements. Criminals tend to disclose and share information on their platforms, which leaves users of well-known software vulnerable to attacks (Leukfeldt, 2014).

2.2.1.3. A motivated offender

An offender may be motivated by means, motive, or a mixture of the two. The offender has the potential and ability to commit a crime (Kao, Kluaypa, & Lin, 2017). Additionally, the

researchers contend that a motivated offender cannot always carry out their plan, which forces each offender to decide for themselves whether to commit the crime. The decision's outcome varies depending on the circumstances. The rational choice perspective is used to explain how offenders make decisions within the Routine Activity Theory, it outlines the two stages of decision-making that determine the offender's decision to act or not. According to Groff (2007: 83) “making the decision to take part in criminal activity is the first step. A condition of "readiness" to execute the crime is the outcome of this step. The decision to commit a specific crime is made in the second stage, which is influenced by the contextual elements that exist in a particular setting”.

2.2.1.4. The absence of a capable guardian

“Guardianship refers to the capacity of persons or objects to successfully prevent crime” (Madero-Hernandez, & Fisher, 2012:5). Furthermore, the researchers assert that there is an inverse relationship between the degree of guardianship and the vulnerability of targets to exploitation. Targets with less guardianship are thought to be more vulnerable to exploitation. The opposite is true for targets with more guardianship, they would likely be less vulnerable to exploitation. A competent guardian, according to RAT, can be a manager, a co-worker, security cameras, lights, an alarm system, network administrators, security personnel, and Information Technology (IT) auditors amongst many other preventive elements that deter a crime from taking place (Shaik & Oliveira, 2019).

2.2.2. Rational Choice Theory (RCT)

The Rational Choice Theory traces back to the investigations done in the classical school of criminal law where the scientific study of crime was conducted by the philosophers Cesare Beccaria and Jeremy Bentham in the eighteenth and nineteenth century (Moran, 1996). The rational choice theory holds that criminal behaviour is a decision, and those who do it do so much like we do when we decide to engage in any kind of action. According to McCarthy and Chaudhary (2014) the Rational Choice Theory approach is different from many other theories of crime in that it describes how people's preferences influence their decisions rather than attempting to identify the causes of those preferences. This approach also offers an effective method for comprehending criminal decision-making and can be used in conjunction with analysis of the causes of preferences and the accessibility of the tools, or mechanisms, through which preferences are realised.

Decision-making is characterised by the perceived costs, inconveniences, and benefits of engaging in a particular behaviour in a particular situation. If the apparent rewards exceed the perceived losses, crime is seen to be more likely to occur (Wikström & Treiber, 2015). When it comes to decision-making, rationality presupposes that one must take certain factors into account before deciding whether to pursue a given course of action. The decision is then reached that adheres to a particular logic or thought process. The decision or choices is intentional as it is supported by a thorough thought process.

2.2.2.1. Cost Benefit Analysis

The theory's foundation is on rationality which according to McClennen (2010:525) "is simply a matter of the consistent and effective pursuit of whatever ends or purposes the individual has". A cost-benefit analysis provides a clearer explanation of the decision-making process used to commit a crime. Cost–benefit analysis is a process of analysing and comparing one thing over another, it is built on a very basic principle that pros should outweigh the cons, benefits against costs (Hansson, 2007). What a threat actor stands to lose by committing the crime is one of the factors that makes the decision unfavourable. Benefits are what the threat actor stands to gain by committing the crime. The risks anticipated and unanticipated are the probabilities that something may go wrong and the consequences thereof. Threat actors consider all the factors that can result in a favourable outcome, all the factors that can result in an unfavourable outcome, the level of risk and the likelihood of occurrence of the risk factors. According to Feldman and March (1981) formal theories of rational choice suggest that people will only seek out and use information about the potential outcomes of different courses of action if it is accurate, pertinent, and dependable in a way that is consistent with its cost.

2.3. Synthesis of the two Theories

The two theoretical perspectives hold in common a focus on the event. The event refers to the occurrence of the actual criminal act. In the rational choice perspective, the event and the surrounding circumstances are considered from a standpoint of a set of choice-structuring properties. The routine activity perspective considers judgement on how suitable a victim is and the guardian capability implicitly and views these at the very least as natural outcomes of a given social setting. The ability to anticipate repercussions is vital from a routine activity and from a rational choice perspective. "It is the calculation of how capable a guardian is and

how suitable a victim is which drives both individual crime and crime waves, rather than the actual level of suitability and capability" (Pease, 1997). A lack of consideration for the notion that people may differ in their initial inclination to offend is what unites the rational choice theory with the theory of routine activities (Nagin & Paternoster, 1993). Moreover, the incentive to commit crimes can vary over time, although according to the authors theoretical publications rarely mention this, and empirical models do not include criminal inclination as an exogenous variable.

Tillyer (2012:147) asserts that, the two theories have similar theoretical roots, the *"perspectives can be viewed as complementary approaches to understanding crime and deviance in that they emphasize the importance of immediate situational and environmental factors in shaping offender decision-making".* The routine activity theory looks at how criminal opportunities arising at the intersection of the three crucial components needed for a crime to occur. The rational choice theory assumes that decisions are made using a cost-benefit analysis, which either motivates or dissuades offenders from committing crimes, and views crime through the lens of the inherent rationality held by the offender (Shariati & Guerette, 2017). According to Jubaer and Hassan (2021:28) "*routine activities theory is a natural, place-based clarification of wrongdoing, where the behavioural designs and crossing points of individuals in time and space impact when and where violations happen".* The prospective offender chooses a spot for the crime, considered ideal by several variables like perceived benefits, magnitude of risks involved. In certain situations, the crime may not occur. *"The perpetrator's decision may be premeditated or awaiting the opportune time. Or it may be the outcome of a random event, in which case the perpetrator may not carefully consider all factors. Criminals are aware of these different choice factors, but they might not combine them into risks and rewards in a way that maximizes anticipated benefit"* (Westland, 1996). The factors that influence an offender's motivation are addressed by the rational choice theory while the routine activity theory examines the resulting outcomes that stem from the offender's choices.

2.4. Overview of phishing attacks

Phishing is a form of social engineering wherein high-level techniques are used to elicit personal information from users of websites and systems (Dou, Khalil, Khreishah, Al-Fuqah, & Guizani, 2017). According to Andrade, Ortiz-Garcés, and Cazares (2020) the three attack

vectors used by threat actors when carrying out phishing attacks are: web-pages, emails, and SMS. Furthermore, "phishing attacks within the COVID-19 pandemic account for more than eighty percent of reported security incidents" (Kovatcheva, Consoli, & Yordanov, 2021:7164). Basit, Zafar, Javed, and Jalil (2020) posit that phishing attacks have become one of the most significant threats faced by internet users, institutions, and service providers, especially with the teleworking setting during COVID-19. Threat actors tailor different sorts of phishing attacks to different settings in order to successfully prey on victims' fear and vulnerability. According to Peng *et al*. (2019) when evaluating existing research investigations have been done on phishing websites and the operations of phishing. However, a knowledge gap exists because it is unclear how information is shared from beginning to end during the phishing process.

The different types of phishing attacks that impact institutions include email phishing, spear phishing, whaling, vishing, smishing, angler phishing, pharming, clone phishing, and the watering hole phishing attack.

2.4.1. Email phishing

Also known as "deceptive phishing" email phishing is a type of attack wherein threat actors imitate a reputable institution to obtain personal information or login credentials from the end users of a system (Bhavsar, Kadlak, & Sharma, 2018). Employees tend to receive information on COVID-19 and vaccination through their company email communications regularly. This gives threat actors the ability to deceive employees by including links to bogus websites to emails. According to Hu (2022) "fake websites impersonating brands like Pfizer and BioNTech were used in COVID-19-themed phishing attacks".

2.4.2. Spear phishing

Aycock (2007:290) defines spear phishing as a "phishing attack that targets a single organisation. It allows a phisher opportunity to create a more customized phishing message, because more context is known". Threat actors in the financial services industry utilize spear-phishing to target individual workers with extensive account access. They can plant a Trojan and use the infection as a doorway to drain accounts if they can convince those employees to click on a dodgy link (Kitten, 2013).

2.4.3. Whaling

This is a form of phishing also referred to as CEO fraud. According to Techtarget's report in Kalaharsha and Mehtre (2021) whaling is a type of spear phishing wherein threat actors target high profile executives in senior positions such as CEOs and CFOs to obtain valuable company information. The reasoning behind these individuals being targeted is that they are known to have access to sensitive information through the higher office that they hold. The email could also include an attachment or another malicious technique for threat actors to gain backdoor access into the executive's machine by infecting it with malware (Moul, 2019).

2.4.4. Vishing

Voice phishing, often known as vishing, is a type of phishing attack in which an attacker uses a telephone system to trick the receiver of the call into divulging personal information (Lee & Park, 2021). Victims of vishing are at risk of identity theft and/or financial fraud (Griffin & Rackley, 2008).

2.4.5. Smishing

SMS Phishing, commonly known as smishing, is a social engineering attack wherein a fake SMS message is sent to steal the personal information of the mobile user (Ghourabi, 2021). Furthermore, the aim of this form of attack is to launder money from victims using texts that often require users to do something like responding with their credentials or personal data (Kalaharsha & Mehtre, 2021). The contents of a phishing SMS may contain phoney links that take the user to websites that contain harmful applications and user interfaces (Mishra & Soni, 2020).

2.4.6. Angler phishing

"The increased use of social media by legitimate businesses to engage with their customers led to the emergence of angler phishing" (O'Hagan, 2018:192). Angler phishing is a phishing attack that targets those who utilize social media. Threat actors use various social media platforms to impersonate a customer service representative in order to contact and bait disgruntled customers and get personal information or account credentials (Hicks, 2018).

2.4.7. Pharming

Attacks such as "pharming" divert people to fraudulent websites instead of the legitimate websites they were trying to access (Sundaram, & Gayathri, 2020). Lala (2015:20) describes pharming as, *"a type of domain spoofing that is often accomplished by compromising DNS servers or the hosts file on a user's computer, causing the user to be sent to a bogus website while entering the proper URL of the intended website into their web browser"*. When a customer of a financial institution tries to use a payment portal such as Ozow to make a payment, they are led to a spoofed site where they enter their credentials, resulting in their banking information being compromised.

2.4.8. Clone phishing

Clone phishing is a phishing attack in which a phisher takes the content and other information from a legitimate, previously delivered email containing an attachment or a link to make a nearly identical or duplicate email. Furthermore, "to appear legitimate and to convince the receiver to open the link or the attachment, the phisher says that the new email is the updated version of the first or original received email" (Patayo, 2021). A link to the phisher's website is usually included in the phishing email. Such links are sometimes disguised by swapping similar characters such as 0 (zero) for O (capital o) (Chaudhry, Chaudhry, & Rittenhouse, 2016).

2.4.9. Watering hole phishing attack

The "watering hole" attack, which is used by attackers to infect victims with zero-day malware, is a new type of phishing attack in which the attackers choose a website in a certain sector to corrupt. This website will be used to infect employees that access it on a regular basis (Ali, 2015). According to Kim, Bu, and Cho (2018:83) "zero-day attacks are undisclosed attacks of computer software that hackers can exploit to adversely affect computer programs, data, or networks of computers". Watering hole phishing attacks focus on certain organisations, industries, and regions. The phisher utilizes this watering hole to guess which website the group frequently visits and infects it with malware (Krithika, 2017:196).

In the digital age because majority of transactions take place online given the widespread use of websites. According to Athulya and Praveen (2020) phishers exploit this, and they eventually target a victim's credentials, so they can use them to create phony accounts that compromise user security or may prevent users from accessing their accounts. Attackers may be driven to conduct these crimes for a variety of reasons, including money gain, fame, or personal honour (Jain & Gupta, 2022). Additionally, they may even do so to carry out illegal initiatives by assuming other people's identities.

2.5. Human factors contributing to phishing attacks

Human factors refer to the behavioural traits that justify why people act the way they do. Human users of a system must act ethically according to cybersecurity regulations for a system to remain secure (Desolda, Ferro, Marrella, Catarci, & Costabile, 2021). Users of a system are either the staff or the customers. It then becomes critical to comprehend how human factors can lead to system vulnerabilities that an attacker can take advantage of. Phishing attacks have drastically increased since the beginning of the COVID-19 pandemic. According to Shi (2020) in Abroshan, Devos, Poels, and Laermans (2021:345) there has been a *"600% spike in phishing attacks in March 2020 alone"*. Human error is a contributing factor to the success of phishing attacks. Abroshan, Devos, Poels, and Laermans (2021:345) posit that "users are still the weakest security link within companies". Social engineering attacks like phishing thrive when users are unaware of their vulnerabilities and when they lack adequate knowledge on the implications and risks of certain behaviour (Desolda *et al*., 2021). According to Verizon (2021) 44 percent of breaches in the Financial and Insurance industry were caused by internal actors. Most of these mistakes are inadvertent, such as sending emails to the wrong people, which accounted for 55 percent of all error-related breaches. Phishers capitalise on the enormous potential for human error in every institution, where a single mistake like clicking on a phishing email can grant access to the whole corporate network. This is a severe mistake that can compromise an entire institution (Burke, 2021).

Susceptibility refers to the probability of becoming a victim of an attack. According to Petrič and Roer (2022) employees who are susceptible to phishing at work are more likely to reply to phishing emails (whether solicited or not) in a way that compromises organisational assets and networks. This basically means that phishing susceptibility relates to the likelihood of

fulfilling a request contained in a fraudulent message. Many users fall victim to phishing attacks because they are not well-versed when it comes to making online trust decisions. According to (Alghamdi, 2017) it has been proven in prior studies that people who are under stress do not explore all their options while making judgments. They also have a propensity to act irrationally and disregard all viable options (For example, reading an email thoroughly before acting on it rather than responding hastily because of a deadline). As important as it is to educate people about social engineering attacks. House and Raja (2020: 1205) contend that it is also crucial to investigate the factors that lead people to ignore cues that are frequently recognised as typical phishing attempts, such as misspellings, bogus URLs, and requests for personal information. Furthermore, it is important to examine the underlying emotions that influence decision-making since doing so can give researchers key information about how people react to phishing attacks. According to Harrison, Vishwanath, and Rao (2016:5632) "when presented with a deceptive email, people with high communicative suspicion experience higher levels of uncertainty and consequently tend to perceive a lack of information to make a choice. In other words, they perceive a wider disparity between the information contained in the email and the information required to determine whether the email is authentic. Individuals handle the information in the email differently as a result of these variations in their perceptions of information scarcity".

Many factors influence or contribute to human beings becoming susceptible to phishing attacks. According to Frauenstein, and von Solms (2009:257) "some of the reasons include a lack of knowledge of computer systems, lack of security and security indicators, lack of attention to the security indicators, lack of attention to the absence of security indicators, and the sophistication of spoofed sites seem to be the greatest threat". Anawar, Kunasegaran, Mas'ud, and Zakaria (2019) suggest that knowledge and experience play a pivotal role in decreasing the susceptibility of users to phishing. There are many systemic factors that contribute to the success of phishing attacks. The absence of adequate procedures for internal control contribute to systems becoming easily compromised by phishers (Woods, 2021).

Phishing attacks tend to thrive in environments where there is absence of protocols, or a rule book designated for policy awareness. According to (Alghamdi, 2017) when their targets are unaware of the company's policies, phishers find it incredibly enticing. Additionally, in certain cases, users don't know which channels to use to file complaints about account

maintenance and fraud investigations. Customers that are not knowledgeable about a company's policies and are inept are more likely to be targeted by phishers.

2.5.1. Dimensions of user susceptibility to phishing

The three factors that influence the human mind and eventually determine output behaviour, are cognitive thinking (what one knows, understands, or thinks), affective emotions (what one feels, attitude and convictions), and conation (volition, reasons for acting) (Huitt, 2012). It is important to understand the emotional triggers that lead to cognitive biases and results in actions that are irrational and not well considered. No matter how many firewalls, encryption tools, certificates, multi-factor authentication systems, or other technical safeguards an organisation installs, infiltration will still happen if the individual behind the keyboard falls for a phish (Hong, 2012). Organisations frequently rely on employees to function as the first line of defence in spotting phishing emails and safeguarding company assets. However, strategies like social engineering that prey on human emotions make it difficult to rely only on this line of security. The ability to recognise phishing emails, report them, and refrain from actioning them is important.

Human beings perform certain actions based on the judgement they apply when confronted with certain decisions. According to Green and Dorey (2016:26) there are: Conformists: individuals that stay secure by following what everyone else is doing, they conform, or follow other people because they believe that there is "probably a reason why that should be done". Selfish individuals incline towards looking out for and helping themselves than anyone else. They have the "I trust me, and I do not trust you to keep me alive, so I will do what is best for me" approach to decision making. Consistent persons feel more secure repeating the same behaviour rather than taking the risk of doing something atypical because they have the belief that if something has previously worked, it must be safe to do again. Rule of thumb thinkers: "I will take a decision based on the first thing I see because it is likely to be the nearest thing to me and therefore the most important to my safety" (Green & Dorey, 2016:27).

These types of individuals mentioned are prone to exhibit different responses when confronted with a phishing email each with different motivations. Conformists will typically click on the fake link if they see other people acting on the phishing email in the same way. Selfish people use their discretion to do what makes sense for themselves even if it is not

necessarily what everyone else is doing. These selfish individuals may choose to click or to not click and even in some instances to report the email to relevant persons for it to be flagged. Consistent people will follow a uniform way of handling phishing emails; if they didn't click on the last one, they are probably not going to feel comfortable clicking on any additional emails that might look similar. But if they clicked before and nothing happened, they would probably think the same thing again. Rule of Thumb thinkers, on the other hand, treat phishing emails according to the first set of instructions they recall or consider for how they should handle such emails; if nothing comes to mind, the second-best idea would be to inquire about the rules that already exist for handling such kind of emails.

Since smartphones, computers and the internet have become so widely used, the speed at which information is transported, processed, and communicated has increased substantially. "The internet is a decentralised structure that offers speedy communication, has a global reach and provides anonymity, a characteristic invaluable for committing illegal activities" (Alazab, Layton, & Broadhurst, 2013:58). According to Green and Dorey (2016:1) all these changes create a reality where, "the speed with which information is communicated exceed our capacity for reflection and judgement and this does not make for balanced and proper forms of expression. There is need for a restoration to the sense of deliberateness and calm". This allows people to think through what they do when handling instruction and to be able to easily identify the tactics threat actors conceal in innocently looking but dubious phishing emails.

2.6. Ineffective organisational measures

A phishing attack not only results in financial loss, but it also leads to data breaches (Lichtfuss & Berryman, 2021). Furthermore, data breaches result in reputational damage and business disruption. "A data breach is a cyber-attack in which sensitive, confidential or otherwise protected data has been accessed or compromised" (Hanna, Ferguson, & Beaver, 2021). According to Elmisery and Sertovic (2021) beyond the reputational and financial implications of data breaches, data being compromised allows threat actors the platform to be able to use the leaked data for various nefarious purposes.

According to Okereafor and Adelaiye (2020:63) the following are the generic impacts of cyber-attacks, which also relate to phishing:

i. Effect on data confidentiality

Phishing attacks lead to data breaches and the unlawful exposure of sensitive client information. When phishing attacks succeed, firms become in violation of the Protection of Personal Information Act (POPIA). The purpose of POPI Act is to protect the personal data of people at the hands of governmental and private entities. This act necessitates a heightened awareness of how personal information should be handled, and it exists to protect data from being accessed by unauthorized individuals by regulating how it is distributed (Buys, 2017).

ii. Effect on data integrity

Data integrity refers to the "accuracy and consistency of data throughout its lifecycle" (Ahmad, Kumar, & Hafeez, 2019:306). When data is compromised or altered as a result of a cyber-attack, its validity and usefulness is impacted (Okereafor & Adelaiye, 2020:63).

iii. Effect on data availability

Some systems rely on the availability of data to work properly. Such programs may stop working or perform erratically if data becomes unavailable. This downtime caused by data inaccessibility limits the system's ability to be used for its intended purpose, posing substantial dangers to workflow and operations that rely on it (Thomas, 2018).

iv. Effect on revenue loss

Theft of corporate information, theft of financial information, theft of money, and disruption of critical trading activities are all common consequences of cyber-attacks. Businesses that have had a cyber breach will typically incur financial costs for restoring impacted systems, networks, and devices, as well as implementing appropriate security measures (Pochuyko, 2018).

Another way that phishers readily infiltrate organisations is through poorly designed user interfaces (UIs) that have significant security flaws and are not properly protected. A user interface is a front facing means by which a user interacts with a system. According to Sridevi (2014) computer-based system or product's user interface is perhaps its most crucial component. If the interface is poorly designed, the user's ability to maximize or derive value from the system is impeded. A poor interface may make an application that has otherwise

been well-designed and solidly implemented fail. Regardless of the architectural security measures that have been implemented, the overall security of a computer system can be compromised if its communication channels are deliberately interfered with (Malisa, 2017). Furthermore, user interface attacks are also more likely when there isn't a secure end-to-end channel that is permitted and private between the user and the program they are using.

2.7. Interventions to reduce phishing attacks

Despite the existence of numerous anti-phishing technologies, phishing persists because zero-day attacks are not adequately detected (Orunsolu, Sodiya, & Akinwale, 2019). A cyberattack that takes advantage of a flaw that has not yet been made public is known as a zero-day attack. Phishers frequently target systems before programmers can patch them and commonly when anti-virus software is unable to recognise the true nature of the attack (Bilge, & Dumitras, 2012). According to Sumner, Yuan, Anwar, and McBride (2021) the three key areas of reducing the occurrence of phishing attacks are through, phishing detection approaches, education, and training, and establishing level of user susceptibility. The authors argue that the two ways to detect threats are manually or automatically. Automatic approaches frequently use browser add-ons to block phishing websites, but manual detection relies more on user intervention and requires users to be astute enough to recognise attacks. The three-dimensional classifications by Frauenstein and von Solms (2009) described in figure 2.7 further illustrate these automatic and manual approaches.

Organizations can lessen their exposure to risk by making sure that all risk sources are successfully addressed. To do this, they must be aware of, monitor, and respond rapidly to risks as they arise. Furthermore, a risk mitigation plan for a business is considered successful if it helps the organisation to handle issues and ensure that they do not trigger adverse occurrences (ChePa, Jnr, Nor, & Murad, 2015). Adopting multidimensional approaches to email security and the implementation of solutions like Mimecast Targeted Threat Protection can help organisations contain the success rate of phishing attacks (Sidler, 2017).

There are three dimensions that must be addressed for institutions to protect their information assets successfully against phishing attacks. These dimensions are explained by the model defined by Jain and Gupta (2022).

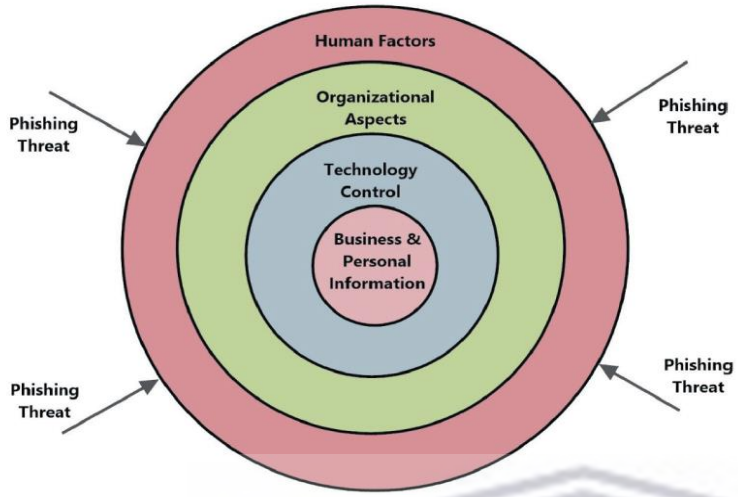


Figure 2.7: Anti-phishing model for institutions by Jain and Gupta (2022)

i. Technological dimension

The technological dimension involves the installation of anti-phishing software, email filters and regular updating of software and operating systems. A practical implementation of this dimension involves the installation of antivirus programs, setting up signature updates, and keeping an eye on the antivirus status on all machines and equipment. Anti-phishing software is a collection of computer tools that seek to detect phishing content on websites and in e-mail messages (Singh & Imphal, 2018:65). Spam filters detect unsolicited, unwarranted, and unwanted emails that flood the inbox of a system user. According to Raulot (2019) spam filters act as the first line of defence in preventing phishers from sending false emails to end users, ensuring that such emails never even reach the user's mailbox. This technical measure should be used in conjunction with web filters so that, in cases where the spam filter misses an email, the system is able to ban the user when they click on a malicious link associated to that email.

Certain phishing emails are so carefully crafted, that they can slip through the cracks and go undetected, making it to the user's mailbox. Having both filters in place becomes a dual form of system protection. Systems and software must be regularly updated with the necessary updates, and security layers. Outdated systems give rise to a gap that threat actors can exploit (Kannan, 2017). Secure Sockets Layer (SSL) is a form of encryption on communication that is done on the internet, between a website and a system user (Oakes, Kline, Cahn, Funkhouser, & Barford, 2019). Using an SSL Certificates, helps in the securing of incoming

and outgoing traffic to a website, the encryptions prevent third parties from intercepting the data being transferred between the website's server and the client's browser.

ii. Human dimension

The human dimension involves employee education and training. Cybersecurity training and workshops are vital since they aim to raise employee awareness and ensure that employees become competent enough to protect the company's information assets (Kim, Lee, & Kim, 2020). Lack of security behaviour by Staff is a key concern in this dimension. Unwanted staff behaviour needs to be treated seriously. According to Jain and Gupta (2022) the norms and procedures of the organisation should be enforced to prevent employees from breaking them or assisting an attacker in carrying out hostile activities against the organisation. Securing email accounts with strong passwords also makes it harder for threat actors to compromise systems, but organisations must make sure that password changes are mandatory and scheduled to occur every ninety days at least (Wadhwa & Arora, 2017).

iii. Organisational dimension

The organisational dimension speaks to the adoption of policies and procedures to successfully manage and mitigate phishing attacks. According to Jensen, Dinger, Wright, and Thatcher (2017) a rule-based strategy can be used to train employees how to behave or which rules to follow to prevent the company from falling victim to phishing attacks. Two factor authentication and verification methods are important in avoiding phishing attacks. Grosse and Upadhyay (2013) state that attackers also attempt to infiltrate systems by attacking password security causing user passwords to fail. Attackers do this by either using a proxy to access the real authentication server or by collecting users' passwords, two-factor codes, and security questions and answers. However, if password managers are properly linked with the device and browser, they can help ensure that only the right websites utilise passwords. However, be that as it may, users still need to guard against clever attacks. Better user-interfaces are also helpful in protecting system users (Hong, 2012). Users can easily report or access key information relating to system protocols. It makes detecting anomalies in system performance quicker and users can quickly pick up phishing emails easier. Encryption of important and sensitive company data can also reduce the success rate of phishing attacks. According to Panda (2016) encryption is an algorithm that plays a crucial part in ensuring

that information is made secure by encrypting data and encoding it so that only the holder of the corresponding password or key may decode or decrypt such files. This maintains the integrity of organisation information by improving data privacy and confidentiality.

Phishing simulations can be used to reduce the success rate of phishing attacks. These simulations allow institutions to assess the efficacy of the training provided. “Phishing simulations are intended to teach users how to recognise "teachable moments" which occur when they make a mistake” (Jayatilaka, Beu, Baetu, Zahedi, Babar, Hartley, & Lewinsmith, 2021). Lahcen, Caulkins, Mohapatra, and Kumar (2020) state that some companies use computer programs to replicate real-world scenarios, these become illustrated in the form of phishing exercises. This is beneficial because it makes users more cognisant of the dangers of phishing. “Another method for combating phishing attacks is to use machine learning to detect phishing emails automatically” (De Bona, & Paci, 2020). While Gordon, Wright, Aiyagari, Corbo, Glynn, Kadakia, Kufahl, Mazzone, Noga, Parkulo, and Sanford (2019) posit that sending simulated phishing emails to a group of employees is one way to raise awareness and offer training, and you can then send educational material to the individuals who click or enter their credentials on the test email.

2.8. Phishing detection approaches

Four categories were used to classify the review of previous studies on phishing detection methods. These categories are Blacklist Based, Content Based, Heuristic-Based, and Fuzzy-Based Approaches as described by Zuraiq and Alkasassbeh (2019).

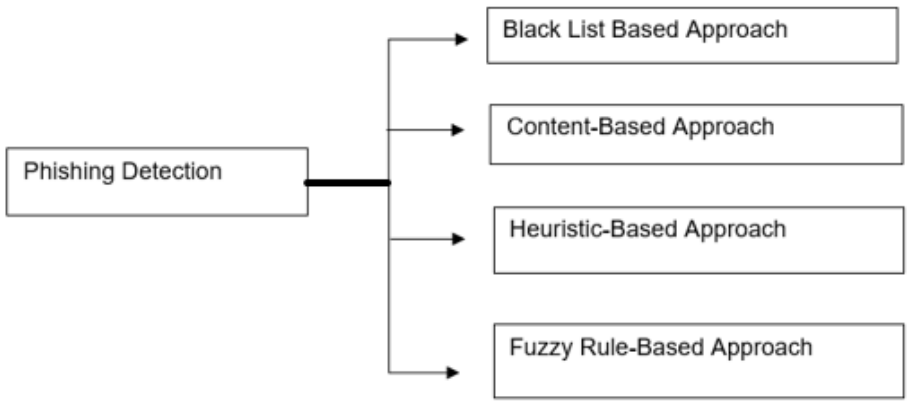


Figure 2.8: Phishing detection categories

Categories defined by Zuraiq and Alkasassbeh (2019)

- *Blacklist based approach*

A blacklist is a list that is contained in toolbars and search engines that comprises all phishing URLs and IP addresses that have been flagged as suspicious (Ma, Saul, Savage, & Voelker, 2009). Users are automatically prevented from accessing a particular website when they receive messages with any of the links on this list. Blacklisting is a technique for detecting and preventing phishing threats; it refers to automatic blacklists that are frequently installed as browser plug-ins and are used to review each URL entry (Zouina & Outtaj, 2017). Blacklists include well-known phishing websites that were obtained through means like user voting. Any attempt by the user to connect to any of the hazardous websites on the blacklist is then rejected.

- *Content-based approach*

The Content-Based Approach uses weighted word extraction from URLs and HTML contents to identify phishing web pages. These phrases might include brand names that phishers use in various parts of the URL to make it seem legitimate (Zuraiq & Alkasassbeh, 2019).

- *Heuristic based approach*

The heuristic-based technique analyses the website's contents. According to Apandi, Sallim, and Sidek (2020) within this method, there are three sub-approaches: visual content (focuses on website design), textual content (focuses on a website's keywords), and surface level content (focuses on website's URL).

- *Fuzzy rule-based approach*

According to Zuraiq and Alkasassbeh (2019) the Fuzzy Rule-Based Approach where logic is the foundation of rules. Fuzzy logic is used to assess the level of phishing in various web pages based on a specified set of principles. Therefore, the URL will be identified as a phishing webpage and given a score if it meets the necessary requirements.

2.8.1. Fuzzy Logic

In 1965, Professor Lotfi Zadeh coined the phrase "fuzzy logic" which according to Abdul-Hussein, Mohammed, and Kadhim (2022:545) "is a branch of mathematics that was developed from fuzzy set theory, where evaluation is an approximation rather than precise values". Since then, this reasoning has been applied to the real-time detection and identification of phishing websites using a range of characteristics and qualifying criteria. Bhagwat, Patil, and Vishawanath (2021) assert that fuzzy logic and data mining algorithms play a crucial role in identifying and testing phishing websites. The fuzzy rules can resolve the ambiguities that are inherent in the detection process of such websites. "Fuzzy logic offers a more logical method of handling quality factors as opposed to exact values" (Prasad & Rohokale, 2020:34).

Phishing detection using fuzzy logic method focuses on applying wisdom to identify the significant characteristics that distinguish between real and phishing URLs (Nivedha, Gokulan, Karthik, Gopinath, & Gowshik, 2017:21). Furthermore, "the fuzzy based methodology provides efficient and high rate of phishing detection of URLs". Human users receive a phishing email, and they have the choice of clicking links or not, and whether to enter their credentials or not. At this point, the users apply a 'yes', I should do it because or 'no' I should not do it because decision, which is supported by a particular justification. The fuzzy system is a rule-based system that analyses data using fuzzy logic, a set of if-then rules. According to Nordin, Ismail, and Omar (2020) this fuzzy system uses a different approach from conventional logic, which mimics the manner in which people make decisions reduced to either a 'Yes' or 'No'. Consequently, fuzzy logic therefore mimics human thinking since it can deal with ambiguous situations and replicate human cognitive decision-making.

There are several characteristics discussed by Bashir, Agbata, and Emmanuel Ogala (2020:209) that can be used to distinguish between phishing websites, their associated emails, and legitimate websites. According to Aburrous, Hossain, Thabatah, and Dahal, (2008:2) "these characteristics and the fuzzy logic approach allow for the use of linguistic variables to explain important phishing indicators and the associated website phishing probability". Threat actors frequently hide the IP Address and use misleading or confusing URLs. Redirect pages are made to redirect users to other pages where they can be tricked into giving over their information. Long, suspicious URLs that contain partial truths are used to trick users

into not checking the authenticity of the claimed identity. According to Nivedha, Gokulan, Karthik, Gopinath, and Gowshik (2017:21) the length of the URL, the number of slashes in the URL, and the dot in the host component of the URL are the main indicators of a phished URL. Additionally, details like misspelled words and the lack of Secure Sockets Layer (SSL) certifications point to the website's illegitimacy.

2.9. Gaps in the existing literature

According to Dewis and Viana (2022) phishing and spam detection is not a new research area; however, detection solutions developed to tackle these types of emails have extensively focused on machine learning approaches. The measures can't be used effectively when applied independently of one another. The research perspective needs to be balanced so that the technical measures are employed along with a significant amount of human participation. "Despite having sophisticated technical methods to combat phishing emails, attackers are still finding their way to get into user's inboxes and eventually their targeted systems" (Sharma, 2021:2). The human aspects that make people vulnerable to phishing attacks are still largely unexplored, neither have enough studies been conducted on this aspect. Zhuo, Biddle, Koh, Lottridge, and Russello (2022:13) posit that, in order to successfully increase users' detection performance, this research gap needs to be filled. This creates a need for additional human-centred phishing research. Future studies should compare security culture-raising initiatives and the extent to which organisations embrace policies that promote an environment of increased security. According to Ertan, Crossland, Heath, Denny, and Jensen (2020) this is one of the potential research paths that needs to be explored in the future, as well as how employee behaviour outside of the office influences the internal security culture of an organisation. It is crucial that additional research be done in the future to fully understand users' cognitive biases, visceral triggers, and mental capacities that affect their potential to reconcile information and distinguish false from true. Phishers capitalise on the possibility of human understanding error, while user susceptibility stems from flawed and uninformed decision making.

The likelihood that users will become less susceptible to phishing is high if these research gaps are filled. The presence of these gaps that have been identified presents an opportunity for further research to be done to close the gaps and gain a better understanding of phishing. Future researchers have an opportunity to focus on achieving an equal amount of research

effort which adequately emphasizes both human and technology aspects of containing phishing attacks. This will consequently result in improved users' awareness.

2.10. Chapter summary

This chapter provided a review of the literature that underpins the study. The routine activity and rational choice theories where discussed, and it was established that RAT explains how cybercrime takes place. It is evident that RAT focuses on the convergence of a suitable target, a motivated offender, and absence of culpable guardianship. The rational choice approach covers elements that influence the decision or thought process of the offender. According to this theory, crime is not a random act but rather comprises of a rational process that is followed which affirms the decision to commit or not to commit a crime. The chapter furthermore explores the types of phishing attacks that people frequently encounter when using various systems. The study investigates the factors that contribute to users falling victim to phishing attacks. Further, the study examined the behavioural traits and characteristics of users who typically succumb to phisher tactics, user triggers, and motivations for how users handle emails. The thesis also examines how institutions are affected by inadequate organisational and technical measures and the interventions that may be used to contain the success rate of phishing attacks. Phishing attacks can only be mitigated, but not prevented, and the mitigation can only be achieved through an increased amount of collaboration and involvement from users. Organisations also need to have a sufficient level of technical agility to ensure that systems, and processes are always up to date with the necessary patches.

Chapter 3: Research Methodology

3.1. Introduction

This chapter used the research onion illustrated in Figure 3.1 to explain the research methodology. “Research methodology is a way to systematically solve the research problem. It may be understood as a science of studying how research is done scientifically” (Kothari, 2004:8). The methodology is used to examine the many approaches typically used by a researcher to analyse a research problem, as well as the reasoning behind them. These steps and justifications are carried out with the aid of a research onion. The research onion allows an extensive description of the main layers or stages that must be addressed to formulate an effective methodology (Melnikovas, 2018). According to Sinha, Clarke, and Farquharson (2018:366) the analogy of the onion is used because "onions contain layers, and researchers need to peel the research onion to its core, to unearth layers of meaning that enable the comprehension of phenomenon being examined”. This chapter includes the research philosophy, approach, design, methodology, data collection and analysis techniques used, participants, and ethical considerations.

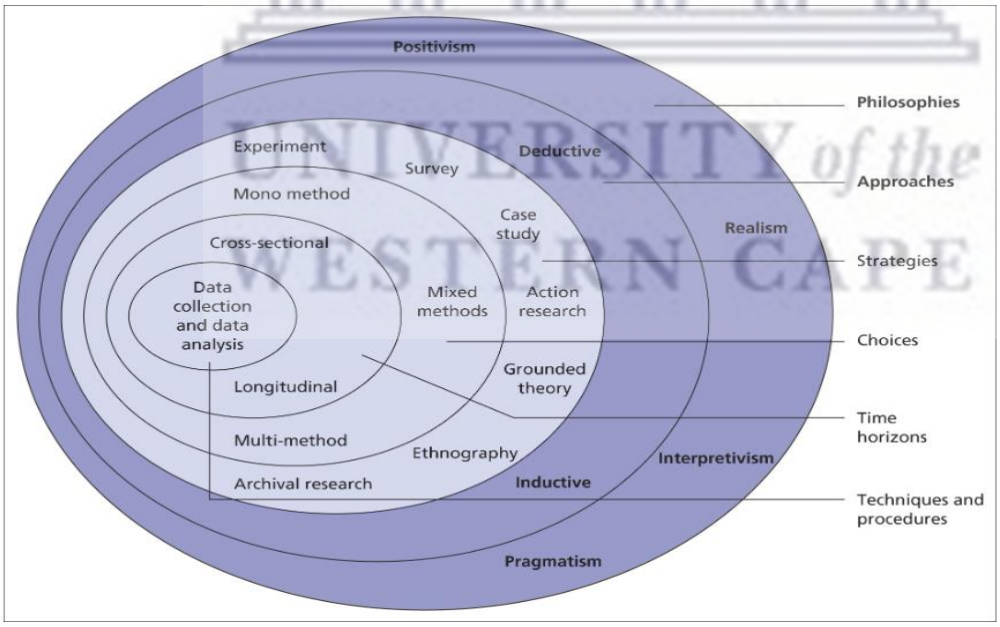


Figure 3.1: The research onion by Saunders, Lewis, and Thornhill (2018)

3.2. Research philosophy

A research philosophy expresses the viewpoint of the research on the way the data is collected, interpreted, and analysed (Al-Zefeiti & Mohammad, 2015). The philosophy

outlines sets of beliefs or viewpoints that serve as the foundation for an investigation. The philosophy that was chosen by the researcher informed the research's assumptions and point of view, as well as the design, strategy, and execution of the study Ontological and epistemological branches of philosophy were used in this study in order to describe the essence of the study coherently and comprehensively. Ontology describes the genesis of all research, from which one's epistemological and methodological stances naturally flow (Grix, 2002). According to Don-Solomon and Eke (2018:2) *"ontology describes the researcher's view of the nature of reality or being on the societal organisational phenomenon studied"*. Ontology aids in the foundational understanding of what actually exists when a phenomenon is being studied. On the other hand, Crotty (1998, cited in Al-Ababneh, 2020:78) purports that, *"epistemology is the study of knowledge and embodies a particular view of what knowledge entails and how we come to know what we know. The nature of knowledge, its possibility, scope, and general foundation are the topics covered by epistemology"*.

The approaches that underpin these philosophical views are, interpretivism, positivism, realism, and pragmatism. The Interpretivist school of thought holds the view that reality is subjective and can be better understood through one's experiences (Alturki, 2021). The belief is that how one looks at things is shaped by where they come from and their social surroundings. Positivists unlike Interpretivists believe that reality is objective and can be confirmed using quantifiable characteristics that can be empirically or scientifically confirmed (Majeed, 2019). Hypothesis testing is done to prove or disprove a phenomenon. "Realism is an ontological approach that focuses on the existence of things, structures, and mechanisms scientifically at different levels of reality. Realists examine causation in terms of the characteristics of things, how they interact, and the causal capabilities (and limitations) of those objects, the leading metaphors are mechanisms in reality than events or specific phenomenon" (House, 1991). According to pragmatism, one needs experience to give an event meaning. So, rather than depending on unchanging truths, the aim of pragmatic research is to use human experience as the main source of information and understanding of the world (Allemang & Dimitropoulos, 2022).

The study adopted the interpretivism philosophical research paradigm, which contends that people's experiences and perceptions have a significant impact on how they interpret reality. As a result, the definition of what is considered truth and knowledge becomes highly subjective and is significantly influenced by culture, history, and other external factors that

affect how people perceive things (Ryan, 2018). This paradigm was appropriate for the study because it clarified what phishing is from the perspective of those who are exposed to and may have encountered it. Additionally, with this approach participants were able to discuss their understanding of phishing as influenced by situations they have encountered at work or in general. According to Tuli (2010) "interpretive researchers prioritize first-hand knowledge, accurate reporting, and quotes from real conversations from insiders' perspectives over testing the laws of human behaviour, they use data collection techniques that are sensitive to context, allowing for rich and detailed descriptions of social phenomena by encouraging participation".

3.3. Research design

The term "research design" refers to the specific approach that the entire study adopts from beginning to end to answer the research questions and achieve the research objectives (Creswell & Poth, 2016). Sovacool, Axsen, and Sorrell (2018:18) posit that "the important distinction between a research method and research design is that the former pertains to a technique for collecting or analysing data, whereas the latter describes how such a method or set of methods are actually executed in a given study". There are three approaches that can be adopted within a study these are: quantitative, qualitative, and mixed method approaches (Creswell, 2014). "The quantitative approach describes a study strategy that uses deductive reasoning to support or refute theories by demonstrating their hypotheses. Because the data being analysed are quantified and therefore have a numerical structure, statistical methods are used in the analysis (Atmowardoyo, 2018:197).

A qualitative approach "*makes discoveries using inductive reasoning with less concern for the generalizability of the findings and more concern for deeper comprehension of the research problem in its unique context"* (Savai, 2016:71). According to Morse and Nichaus (2016:14) "A mixed method design is a scientifically rigorous research approach, led by an inductive or deductive theoretical drive and comprises of a qualitative or quantitative core component with qualitative or quantitative supplementary components". The qualitative research approach was chosen for this study because of its ability to generate findings with rich, in-depth data that can capture the participants' perspectives. The researcher is able to understand user behaviours and associated justifications for specific patterns of conduct using natural language rather than using quantitative methods. According to Verhoef and Casebeer

(1997:65) *"The goal of qualitative research is the development of concepts that help clarify phenomena in natural, rather than experimental, settings, giving due emphasis to the meanings, experiences and views of all the participants being studied"*.

3.4. Research approach

According to the research onion in Figure 3.1 above, there are three approaches namely: inductive, deductive, and abductive. Melnikovas (2018) distinguishes the inductive approach as a type of research that begins with observation and data collection, then moves to description and analysis to form a theory. Whereas the deductive approach unlike the inductive approach begins with an existing theory and then introduces a question or set of hypotheses, followed by data collection to confirm, or reject the hypotheses. "The deductive method entails formulating a theory and hypothesis, as well as devising a research strategy to test the hypothesis. The inductive method entails gathering data and then developing a theory based on the data analysis" (Malalgoda, Amaratunga, & Haigh, 2018:905). The abductive approach refers to a reasoning process in research that focuses on exploring less explored phenomena in new settings. This approach uses facts and findings as a foundation for developing a theory (Järvi, Kähkönen, & Torvinen, 2018). According to Rahmani and Leifels (2018) the facts of the abductive method are explained based on a single experience or observation that serves as a beginning point for linking more experiences and observations to form a hypothesis. To uncover the most likely explanation, an abductive approach typically begins with a startling fact and moves between induction and deduction (Melnikovas, 2018:34). This study adopted an inductive approach and a qualitative methodology to perform the research. The use of an inductive approach was well-suited for this investigation because it facilitated the generation of novel insights and a deeper exploration of the impact of phishing attacks on financial institutions. By capturing the firsthand experiences, beliefs, and attitudes of the participants, this approach served as the foundation for devising practical solutions to mitigate user susceptibility to phishing attacks. Furthermore, it provided a platform for identifying patterns, themes, and cause-and-effect relationships that might not have been discernible through quantitative methods. Consequently, the study was able to reveal the intricacies of phishing attacks within the financial industry, leading to more meaningful and impactful findings.

3.5. Research strategy

This layer of the research onion comprises strategies like surveys, case studies, action research, grounded theory, ethnography, and archival research. According to Omotayo and Kulatunga, (2015:7) “the suitability of these methods depends on the research objectives and the philosophy which has been adopted for the investigation”. Surveys are a quantitative data collection method that uses questionnaires and other cost-effective data collection tools to gather information from a sample of cases (De Vaus, 2016). Draugalis, Coons, and Plaza (2008) assert that even in cases where cost-effective methods of data collection are used, it is crucial for researchers ensure that survey designs maximise response rates. For published survey research to be considered seriously, it must comply with a defined criteria of scientific rigor. This is supported by Holtom, Baruch, Aguinis, and Ballinger (2022:1561) who suggest that future survey research should use validity evaluation frameworks to ensure response rate transparency and the representativeness or generalizability of the study's findings. “Case studies provide the researcher the chance to conduct an empirical investigation into a current phenomenon while using a variety of sources of evidence” (Kulatunga, Amaratunga, & Haigh, 2007:484). Action research is a practical, hands-on method used in real-world situations with the specific goal of solving problems. It draws on qualitative research (Grady 1998). Gubrium, Holstein, Marvasti, and McKinney (2012:347) state that “the term "grounded theory" refers to a methodical approach for building theoretical analyses from evidence that includes explicit analytic procedures and implicit rules for data collection.”

Ethnography is a process for collecting qualitative data that is used to better understand individuals through close observation. Ethnography uses participant observation and interviewing techniques to closely examine and understand the social world through the lens of culture. Moreover, the goal with ethnography is to comprehend a particular group's culture from the viewpoint of the group members. The group culture will provide understanding of the group members' behaviours, values, emotions, and mental states. To fully comprehend the social context and members of the social group's perspectives, ethnographers use a variety of techniques. Archival research draws on information that already exists in archives. Iovino and Tsitsianis (2020) assert that archival research is more likely to use longitudinal data since it allows for the observation of changes in each phenomenon over time.

This study adopted a grounded theory research strategy because it allowed the study to better understand meaning that lies in social interaction which can be answered with close examination of participants and their behaviours. According to Noble and Mitchell (2016:34) the grounded theory approach is *"used to uncover things such as social relationships and behaviours of groups, known as social processes"*. This approach appeared to be the most effective way to evaluate users awareness of phishing attacks, their capacity to lessen susceptibility, and, ultimately, their aptitude for using technology wisely to identify suspicious email activity.

3.6. Methodological choice

A research methodology is either qualitative or quantitative in nature. According to the research onion illustrated by figure 3.1, there are three choices for conducting research: mono-method, mixed method, and multi method. These choices follow either a quantitative or a qualitative research process. Quantitative studies have a numerical focus and employ numerical or measurable methods of data collection, such as graphs when investigating a phenomenon (Basias & Pollalis, 2018). Qualitative research focuses on language, uses non-quantifiable data collection techniques like interviews, and produces non-numerical conclusions through non-numerical data processing (Alturki, 2021). The main distinctions between qualitative and quantitative research are the procedures and techniques, which focus on either verbal words or numerical data. How data is interpreted or understood is an important cornerstone for qualitative research. This is explained by Aspers and Corte (2019:147) who purport that qualitative research can be viewed as a "multi-method, comprising the gathering and application of numerous empirical resources and techniques. It emphasizes both the emotional as well as the objective aspects of behaviour: What people say and do in particular settings and organisations, as reported by individuals, including their attitudes, motivations, behaviour, events, and circumstances".

A researcher employs a mono-method approach if they only use one research method, which could be either qualitative or quantitative, unlike a mixed-method strategy, which combines both qualitative and quantitative research (Phair & Warren, 2021). *"The multi-method approach uses two qualitative and quantitative data collection techniques, such as participant observation and oral history interviews, or two research methods, such as ethnography and case studies, to address the research issues"* (Morse, 2003:11). This study

adopted a monomethod qualitative research method. This approach was chosen for this study because it was better suited to dissect and aid in the understanding of phishing as a form of social engineering. This approach helped in examining the elements and experiences that contribute to increasing user susceptibility. This information was better elicited and understood from the perspective of the users of different systems and through close observation and interpretation.

3.7. Time horizon

The time horizon layer of the research onion refers to the amount of time that the researcher will take to conduct the investigation and collect the data. The time horizons for research are either cross sectional or longitudinal. According to Sahay (2016) a cross sectional design is undertaken when the intention is to solve a problem or answer a question at a particularly short time, whereas with a longitudinal research design the question to be answered or problem to be solved calls for data to be gathered over a longer period. The study used a cross-sectional research time-horizon because data were collected within a short space of time.

3.8. Units of analysis

Units of analysis refer to an entity that forms the focus of the study. In addition, the units of analysis stem from the research question (DeCarlo, 2018). The study concentrated on financial institutions and their employees as they were in a position to offer real-time indication of the cumulative impacts of social engineering attacks like phishing. Financial institutions are business entities that offer financial services and engage in investing money on behalf of clients, some of them furthermore offer loans (Hrdý & Pláničková, 2019). Examples of such institutions include banks, insurance companies, investment companies, and brokerage firms. To properly define the study's scope and create the foundation for its results, the study unpacked financial institutions in relation to insurance companies.

3.9. Data collection and analysis

Data collection and analysis involves gathering and analysing data to comprehend, explain, and draw meaningful inferences about a phenomenon (Bradshaw, Atkinson, & Doody, 2017).

According to Nowell, Norris, White, and Moules (2017) the data collection process, the coding, organising, and analysis have to be described without any ambiguities as clearly to allow the reader to judge whether the final outcome is rooted in the data generated. “Data analysis includes the following core steps: selecting the unit of analysis, creating categories, and establishing themes” (Cho & Lee, 2014:10). Furthermore, researchers should decide which data will be analysed by focusing on a selected material depending on the research questions.

3.9.1. Data Collection

Data collection is a process of gathering information with the intent to corroborate the study. This process allows researchers to find evidence to back up claims and provide a more compelling narrative that is more substantial and not based on uninformed opinion (Best, 2014:5). Best (2014:5) contends that gathering data enables the researcher to shift their perspective from "I know" to "It is known.". To gather information from the participants, interviews were performed over the phone using voice calls, online using platforms like Zoom, WhatsApp, Microsoft Teams, Google meets, and Skype, or in person. Each participant was free to choose how their interview was conducted based on what was most convenient and comfortable for them. In compliance with best practices, the replies were handled in line with the preferences of the participants as stated in the declaration section of the interview schedule. The interview questions were open-ended to encourage more in-depth discussions and participation from the participants. The participants had to explicitly consent for the researcher to record or not record the interview session.

The method of data collection was made flexible and at the participant's discretion. The interviewer had complete control over how the information was gathered. Given the easing of COVID-19 laws and restrictions, a flexible approach was used to provide convenience and make the data gathering process easier. Face-to-face interviews were performed in accordance with the laws and regulations governing social distancing. Interviews were chosen as an ideal beginning point for data collection because of their greater flexibility. In comparison to quantitative methods, qualitative data gathering methods are more flexible.

3.9.1.1. Research instrument

An interview guide was used as the research instrument with which the data was collected. The interview guide comprised of a list of demographic and open-ended questions which

were used. Semi-structured interviews were conducted with each of the participants and the researcher served as the data collector. A semi-structured interview approach usually entails a conversation between the researcher and the participant. According to DeJonckheere and Vaughn (2019) the conversation is aided by flexible interview protocols and enhanced by follow-up inquiries, inquiries for further information, and comments. The questions in the interview guide acted as a road map for the conversation. These questions were designed so that the data collector could begin the first section by gathering information on the participants' demographics like their age, occupation, qualification, and the number of years they had been employed in their organisations. The second segment of the interview guide was made up of six open-ended questions that were intended to initiate discussion about phishing in the workplace, the elements that make employees vulnerable, and any participant recommendations on employee vigilance. The research gathered responses from a small group of participants before expanding the sample size to ensure the instrument's dependability and accuracy.

3.9.1.2. Sources of data

A data source is where data is extracted from. There are primary and secondary sources of data. According to Boslaugh (2007) a data set is considered primary data when it is gathered by the researcher or a member of the team to whom the researcher also belongs. When a researcher uses data sets that were previously obtained by another party for a different goal, it is considered secondary data. The study made use of secondary data sources like websites, electronic books, journal articles and other already existing online materials. A senior manager in the IT division of a financial institution in the Western Cape was asked for permission to conduct this study using the data collected from the company's employees. This request was approved.

3.9.1.3. Sampling

Research population refers to *"the entire group of people, events, or objects of interest that the researcher wants to investigate"* (El-Gohary, 2010:24). Sampling is "the act, process, or technique of selecting a representative part of a population for the purpose of determining parameters or characteristics of the whole population." (Gentles, Charles, Ploeg, & McKibbon, 2015:1983). According to Sandelowski (1995:180) "sample size in qualitative research may refer to a number of people but also to a number of interviews and observations

conducted or numbers of events sampled". The sampling strategy is a deliberate method for ensuring that the sample selected is accurately representative of the population from which it was drawn. According to Swanson and Holton (2005) sampling helps to acquire population parameter estimates from sample data that have the required precision for decision-making while staying within the budget restrictions set on available resources. The sampling strategy that was employed within this study is convenience sampling. Convenience sampling is the process of choosing a sample from the target population based on the people who fit practical criteria, such as being easily accessible, nearby geographically, available at a specific time, or willing to participate (Etikan, Musa, & Alkassim, 2016). Convenience sampling is a form of nonprobability sampling where participants may also be research population subjects who are readily available. This method was chosen because it is the most cost-effective approach that is straightforward and convenient for the researcher to work with accessible respondents, who met the defined criterion. According to Etikan, Musa, and Alkassim (2016:2) *"the main assumption associated with convenience sampling is that the members of the target population are homogeneous. That is, that there would be no difference in the research results obtained from a random sample, a nearby sample, a co-operative sample, or a sample gathered in some inaccessible part of the population".*

The total population comprised of 60 employees wherein the researcher selected only 16 employees to participate in the survey. One of the requirements was for the respondents to be able to read and write responses on the interview instruments along with the supporting documents like the consent forms. This was the most important sample criterion for the study. The consent forms were made available to employees who agreed to participate in the research. The consent forms were used as a guide to explain key information to participants and served as proof that the participants agreed to participate in the study, and that consent was sought before the responses were captured.

3.9.2. Data analysis

Data analysis entails gathering the data, examining it, and making inferences from it. The goal of data analysis is to meaningfully combine the information gathered so that it may be explained, interpreted, and used to reach the proper conclusions (Best, 2014:152). Additionally, the process entails sorting, sifting, and organising through collected data. The form of analysis that will be used within the study is thematic analysis. Thematic analysis

(TA) is a technique for identifying, examining, and reporting patterns (themes) in data. Additionally, “It minimally organises and describes your data set in rich detail” (Braun & Clarke, 2006:79).

Clarke, Braun, and Hayfield (2015:225) state that thematic analysis has a range of different forms which are – Inductive thematic analysis, Deductive thematic analysis, Semantic thematic analysis, Latent thematic analysis, and Descriptive thematic analysis. Inductive thematic analysis refers to analysis that is primarily informed by data, rather than by existent theories and notions. Deductive thematic analysis: on the opposite end of the spectrum, looks at the data through a theoretical lens in order to inform the development of themes and coding while ensuring that the analysis herein goes beyond the data's evident implications. Semantic thematic analysis focuses on the data's clear statements and surface meaning. This form of analysis examines the explicit meanings participants convey to the researcher: the plainly visible ideas and concepts in the data. The focus of latent thematic analysis is on the assumptions, frameworks, or worldviews that underlie the semantic meanings of the data. Latent meanings therefore refer to situations that participants are not consciously aware of expressing; they are meanings that become clearer from the perspective of the researcher. Descriptive thematic analysis refers to analysis where the primary goal is to identify and describe the data's patterned meaning. Semantic thematic analysis was used in the study to evaluate the compiled data and draw conclusions that are indicative of the participants based on their experiences and perspectives.

Thematic Analysis defines six phases that are used to extract the key themes from data. Byrne (2022:1398) asserts that these six-phases enable the researcher to identify and analyse significant themes and, consequently, know how to approach and carry out thematic analysis. Additionally, Byrne (2022:1398) also adds that although the steps follow a sequential and logical flow the analysis process sometimes does not proceed logically through the phases. There may be overlaps. Instead, analysis is iterative and may be repeated, which allows the researcher the ability to alternate between the phases as necessary (Braun, & Clarke, 2020). The study outlines each phase, including what occurs, why it is carried out, and the desired and actionable outcomes.

Phase one: Become familiar with the data

Familiarisation involves building a relationship with the data, becoming more oriented with it. The researcher must read and reread the full data set to get a thorough understanding of the information. This is done so that the researcher can identify pertinent information that may be directly related to the research questions (Byrne, 2022). The outcome of this process was a thorough understanding of crucial elements in the data, which the researcher recorded for later investigation in subsequent phases. The researcher made several clean-ups and rereading on the captured interview notes in order to become intimately familiar with the participant's responses and to ensure that these notes accurately conveyed the feedback given.

Phase two: Generate initial codes

The researcher created initial codes in the second phase using the data generated in phase one. These codes according to Clarke and Braun (2013) must be related to the important features of the study. Additionally, the data is categorized into groups based on similarities or discernible patterns, which are known as initial codes. According to Labra, Castro, Wright, and Chamblas (2020:189) "A code is a type of raw data extracted from interviews and field notes. These include words or phrases that are representative of groups or patterns of data". Moreover, the researchers clarify that there are three different kinds of codes: descriptive (are plainly without any needed clarification), interpretive (data requiring further explanation), and inferential (relates to data that are explicative and indicative). This process produced a predefined set of codes that could be modified if they did not consistently correlate to the themes established in the third phase. All of the participant replies were consolidated by the researcher into a single document, making it simpler to highlight key descriptions, statements or points of interest that were shared in the participant responses.

Phase three: Search for themes

"A theme is a pattern that may be detected in the data that, at the very least, characterizes and arranges the observations and, at the very most, analysis certain features of the phenomenon" (Boyatzis, 1998:4). According to Javadi and Zarea (2016:36)" it is important to take note of the codes defined in phase two because themes are derived from these codes. The list of codes the researcher has should be extensive such that similar codes can be gradually added to a set". At the end of this phase, the researcher compiled information that had been coded and organised it according to relevance to each theme. The researcher marked commonalities,

patterns, and recurrent responses that more than one participant expressed. The researcher marked responses that came up repeatedly across the open-ended question.

Phase four: Review themes

This stage entails examining all the themes within the data set that relate to, are consistent with, and address the study's research questions (Aldulaimi & Abdeldayem, 2020). In some cases, it may be required to merge themes, split a theme into subthemes, or even completely discard certain themes and start the theme development process over. The researcher concentrated on polishing themes at this point, using an elimination process to exclude some themes that were not as frequently recurring, not meaningful, or accurate enough and to earmark meaningful ones for further investigation.

Phase five: Define and name the themes

The names and definitions of the themes must give a clear indication of the range or extent of coverage of each theme. "In this phase topic titles will probably be a little haphazard, possibly lengthy, or maybe simply one word and will only provisionally describe the content and scope of each subject. Furthermore, each theme must be simplified as much as possible before being integrated into a wider narrative about the data as a whole. Overlaps ought to be avoided" (Xu & Zammit, 2020:7). Once the researcher compiled a list of the final themes, each theme was given a distinct name and was then examined separately.

Phase six: Write up the report

The process of writing the report provides one last chance to make modifications that improve the analysis and clearly convey the researcher's interpretation of the data. Terry, Hayfield, Clarke, and Braun (2017) asset that at this point of analysis, the researcher should have begun to shift from a summative posture (considering these themes as collections of codes and data) to an interpretive approach. This can only be done by conveying a story that is based on the data and about the data. The narrative from the story must explain the patterns and varying meanings in the data. At this stage the researcher consolidated the themes and the associated meanings derived from the participant responses. These themes where then used to support the analysis process irrefutably.

3.10. Pilot study

A pilot study is a small feasibility study aimed to evaluate various parts of the methodologies proposed for a bigger, more rigorous, or confirmatory investigation (Lowe, 2019). According to Fourches, Muratov, and Tropsha (2010) before establishing any model it is important to verify the veracity of primary data to the greatest extent possible to ensure validity and reliability. This is the reason why the researcher conducted a pilot study to ensure response reliability and increase the probability of success in the main study. The pilot run began with the distribution of the interview schedules to the four participants who agreed to give feedback on each of the questions' perceived relevance, whether they were simple to understand and engage with, as well as any suggestions for improvements to the instrument. This feedback from the pilot study was used to improve the final instrument that was made accessible to a wider audience.

The goal of this pilot study approach was to leverage stakeholder feedback to improve the research instrument and ensure that all necessary adjustments were made before the instrument was released to a larger audience. Viechtbauer, Smits, Kotz, Budé, Spigt, Serroyen, and Crutzen (2015:1375) state that "one of the goals of a pilot study is to identify unforeseen problems, such as ambiguous inclusion or exclusion criteria or misinterpretations of questionnaire items". This was an internal pilot study because the participants that responded to the pilot pretest where also part of the first participants to respond to and take part in the final interviews. The participants in the pilot study did not respond to the questions in one sitting. They reviewed the questions and completed the feedback document which they then discussed with the researcher. Some of the comments encouraged the researcher to consider making the instrument more relatable by using terminology or phrases in everyday language that people or respondents with backgrounds or jobs unrelated to information technology (IT) would find easy to understand and respond to.

3.11. Trustworthiness

"Trustworthiness is established when findings as closely as possible reflect the meanings as described by the participants" (Lietz, Langer, & Furman, 2006:444). According to Daniel (2019) the idea of trust in research serves as the foundation for both the rigor of the research process and the relevance of the study, as well as the degree of assurance that can be placed in the calibre of the investigation and its results. The criterion established by Lincoln and

Guba (1986) for ensuring reliability of the research are: Credibility, Dependability, Confirmability, and Transferability.

3.11.1. Credibility

Credibility refers to how clearly and accurately the phenomenon is described such that the readers of the study should be able to identify with the research from the perspective from which the researcher describes it (Beck, 1993). In order to ensure the study was credible and free from researcher bias a colleague who the researcher chose because of the nature of his impartiality and unrelatedness to the study was asked to review the data that was collected, the findings drawn from it and the manner in which these were presented. This process in research is referred to as peer debriefing. According to Nowell, Norris, White, and Moules, (2017:3) "peer debriefing offers an external review of the research process, potentially increasing its credibility. It also allows for the comparison of early findings and interpretations to the original data and examines referential adequacy".

3.11.2. Dependability

Dependability is the quality of being able to rely on results to be accurate and consistent over time whereas confirmability is focused on demonstrating that the replies are recorded objectively, accurately, and without the researcher's prejudice or personal interests influencing the research conclusions (Korstjens & Moser, 2017). In order to ensure that the findings in the research were adaptable and could be trusted to have consistency and relevance over time the researcher enriched the data by ensuring that the interviews were not only done with participants face to face but also through video calls. *"Data elicited via video calls have demonstrated substantial richness akin to that gained in face-to-face contexts"* (Keen, Lomeli-Rodriguez, & Joffe, 2022:4). When conducting the thematic analysis of the data that was gathered, the researcher also solicited assistance from peers. To lessen the room for researcher bias and allow for various viewpoints on the major issues raised, results were peer reviewed by two additional researchers. Before any conclusive inferences could be drawn from the findings, this peer review process was able to improve the quality of the findings. The researcher also had to be flexible, and open to other people's views, this strengthened the reliability of the results.

3.11.3. Transferability

Transferability demonstrates that the results can be applied in different settings or how successfully findings from one context can be applied to another (Hellström, 2008). Examples from the interviews were used to illustrate significant themes generated from the study's findings. These examples also served in supporting the findings established by the study. The results and the way they were presented were sufficiently detailed to enable readers to effectively assess how much they could "transfer" or extrapolate the context and inferences drawn from the research to other contexts at their discretion. In order to give the reader as much information about the study as possible the demographic information and geographical parameters of the study were extensively discussed and the information on the population explained to the greatest extent possible. This was done in order to give the reader the ability to assess how well the study's conclusions can be generalized to, or made relevant to, a different context.

3.11.4. Confirmability

To ensure confirmability and eliminate researcher bias, the researcher asked the participants to review their responses before any meaningful inferences were made about them for purposes of the study. This was done to ensure that any conclusions drawn truly represent the views and experiences shared by the participants. In the instance where participants gave consent to have their interview recorded, manual transcription was done to ensure that the researcher was able to clearly decipher interview content and participant intent. To provide an unbiased interpretation of the data and reduce bias or researcher prejudice, the interview responses were categorised into key themes. The interview guide that was adopted included open-ended questions that the researcher used to avoid using leading questions, which could have steered the research in the direction of predetermined answers, during the interview. This was a way in which the researcher ensured credibility.

3.12. Ethical considerations

Ethics were upheld during the entire research process by making sure that the research subjects underwent no harm in any form and that they were aware that participating in the study was entirely voluntary. To maintain and preserve the integrity of the findings and the data collected as part of the study there was strict adherence to the methods outlined in this Chapter as far as data collection and analysis are concerned. Before the start of each

interview, the consent form was read to each participant to ensure that participants understood that their participation was voluntary. The researcher ensured that participants' privacy was protected and that their dignity was given top priority. All forms of communication as part of the study were done in an honest and open manner. All the participants were over the age of 18 and based on their ability to carry out the duties of their current jobs, none of them were showing any signs of mental impairment. Participants in this study had to meet the requirements. To further reduce any potential dangers to confidentiality and privacy, all recorded materials will be deleted five years after final clearance by the University's research committee. The responses from the participants were safeguarded by the researcher and securely stored so that there are no privacy contraventions.

3.13. Chapter summary

The purpose of this chapter was to describe the philosophy that underlies the study and how it influenced the entire research plan. Each aspect of the study was thoroughly synthesized, including how the various pieces of the research onion fit together in terms of the research approach, the strategy, the research design and the methodology, time horizon and the data collection and analysis processes applied. The data was analysed using thematic analysis, which helped derive justified conclusions that thoroughly explained phishing based on real-world examples. The study's trustworthiness was discussed, and the associated steps the researcher took to make sure the study is credible, dependable, and adds real value to the reader. The last section covered was ethics and how the researcher ensured that the research maintained ethical boundaries.

Chapter 4: Presentation and discussion of findings

4.1. Introduction

The objective of this chapter is to analyse the data and discuss the findings. Tables and figures were used to demonstrate the themes and theories discussed in this study. The first section is a restatement of the research objectives that guided the study. The second section used a tabular summary to highlight the participants' demographic data. The demographical characteristics are carefully examined and elaborated as well. The third section was a detailed presentation and discussion of themes which emerged during the interviews. To streamline the data further until distinct patterns emerged from it, direct quotations were used to reference statements. Furthermore, existing literature consistent with these themes was also discussed. The main research objectives were:

i. To establish the solutions that can be put in place to manage the prevalence of phishing attacks.
ii. To determine the extent to which human beings contribute to the success of phishing attacks.
iii. To determine how insufficient technical and organisational security measures expose financial institutions to phishing attacks.
iv. To establish the interventions financial institutions can put in place to mitigate the risks caused by phishing attacks.

The key themes that were identified from the data served as the foundation for the interpretation of the results. Inferences drawn on these themes were confirmed by existing literature from other researchers.

4.2. Demographic characteristics of participants

Research interviews were conducted with sixteen participants who were selected using the convenience sampling strategy. The interviews were conducted face to face and online using platforms such as Microsoft teams and Zoom. According to Vogl (2013) semi-structured interviews are often conducted face-to-face because face-to-face interaction adds value to the conversation by allowing for more accurate interpretation of the respondent's expressions and other observable cues. The choice on the platform where the interview would be conducted was left to the discretion of the participants. Data Analysis according to Graue (2015:8)

describes a phenomenon in some depth by comparing various instances to see what similarities there are or how they differ from each other. Analysis allows researchers to support their viewpoints on the phenomenon being studied. Considering the variations in age, education, positions, and other factors, tabulating the demographic data helps readers in comprehending the data by making it clearer. The data was thematically analysed. The six-step thematic analysis process enabled the researcher to be consistent in defining key patterns or themes and thoroughly refining them until they were accurately reflective of the data. This section includes information about the research population's gender distribution, age, educational background, job position, and years of experience.

Alphabetical letters were used to protect the identities of the participants so that they could stay anonymous. These participants are identified by the letters assigned to them in the participant column; for instance, Participant 1 is denoted by "AB01".

Table 4.1: Demographic characteristics of participants

Participant	Gender	Age	Qualification	Position	Years of experience
AB01	F	25 – 44	Honours	Accountant	>4
BC01	F	25 – 44	National Diploma	Test Analyst	<1
CD01	F	25 – 44	Bachelors	Test Analyst	>4
DE01	M	25 – 44	Bachelors	Intermediate Java Developer	>4
EF01	F	25 – 44	Honours	UI/UX Developer	2 – 4
FG01	F	25 – 44	Honours	Business Analyst	<1
GH01	F	25 – 44	Honours	UI/UX Developer	2 – 4
HI01	F	25 – 44	Bachelors	Digital Communication Developer	2 – 4
IJ01	F	25 – 44	Bachelors	SQL Developer	2 – 4
JK01	F	25 – 44	Bachelors	Business Analyst	<1
KL01	F	18 – 24	Bachelors	Human Resources Administrator	<1
LM01	F	18 – 24	Bachelors	Data Archivist	<1
MN01	M	25 – 44	Bachelors	Automation Tester	2 – 4
NO01	M	25 – 44	Bachelors	Service Desk Agent	2 – 4
OP01	F	25 – 44	National Diploma	Junior Network Engineer	>4
PQ01	M	25 – 44	Bachelors	Junior Integration Automation Consultant	2 – 4

4.2.1. Gender

When looking at this study sixteen participants in total took part in the interviews and from this number four of them were male and the remaining fourteen participants were female.

This research did not place too much emphasis on a specific gender, being the main focus for the study because phishing and social engineering is a cyber crisis that affects people on a global scale regardless of their gender. No assumptions were made regarding the susceptibility of a particular gender; rather, a neutral stance was taken. The gender balance of the participants was not purposefully planned; however, the people who participated, both male and female, were chosen based on availability rather than any gender specific criterion.

According to Iuga, Nurse, and Erola (2016:3) "gender, age, and exposure to educational resources are all user-based factors that have some impact on the likelihood of being successfully phished". These factors are crucial for comprehending patterns of vulnerability and the users who frequently become victims of phishing attacks. Existing studies have produced contradictory results regarding the association between gender and phishing susceptibility. Greitzer, Li, Laskey, Lee, and Purl (2021:3) put forward that historically women have been found to be more susceptible to phishing attacks than men. However, in the same breath studies investigated by other scholars have held a neutral stance where gender was deemed to not be a material determinant of phishing susceptibility. Some studies purport than males are equally as prone to susceptibility as females in certain instances. According to Hamberg (2008:241) "in order to conduct gender-based analyses and determine if gender, is critical to the findings, research must contain a sufficient number of men and women". This is true when gender has material impact on the outcome or the findings, which is not the case for this study. Mughaid, AlZu'bi, Hnaif, Taamneh, Alnajjar, and Elsoud (2022:3821) purport that "most studies showed that women are more likely to fall for phishing attack than men".

4.2.2. Age

Most of the participants in the study were from the 25 – 44 years age bracket. Participants AB01, BC01, CD01, DE01, EF01, FG01, GH01, HI01, IJ01, JK01, MN01 and NO01 within the 25 – 44 years bracket and LM01 and KL01 formed part of the 18 – 24 years age group. According to Dyussenbayev (2017) the age range between 18 and 24 years old reflects the period of youth, and the age range between 25 and 44 years old symbolizes the start and middle of maturity. This demonstrates that the interview subjects were of legal age, of sound mind, and of sufficient reasoning ability to be able to comprehend and be able to respond to the questions posed as part of this study. According to Mughaid, AlZu'bi, Hnaif, Taamneh,

Alnajjar, and Elsoud (2022:3821) “participants’ age linearly predicts their susceptibility to phishing. Additionally, older users are less likely to fall prey to phishing, while younger users particularly between the ages of 18–25 are more vulnerable to phishing attacks”. According to Bolin and Skogerbø (2013:5) “age is a discrete variable that can be aggregated and interpreted in a variety of ways in empirical research. In its most basic form, age refers to traits that particular demographic groupings frequently exhibit”. A study by Gopavaram, Dev, Grobler, Kim, Das, and Camp (2021:7) “found that age and how experienced users are with computers largely has a material effect on how accurately they are able to accurately identify phishing websites”. Furthermore, the researchers found that in comparison to younger people, older participants tend to have lower precision.

4.2.3. Education Level

The qualification rankings referred to in the research instrument include National diploma, Bachelor’s degree, Honours degree, Masters’ degree, and a Doctoral degree. Two of the total sampled individuals BC01 and OP01 hold a national diploma. Ten of the participants from the sample are bachelor's degree holders these are CD01, DE01, HI01, IJ01, JK01, KL01, LM01, MN01, NO01, and PQ01. Four participants namely, AB01, EF01, FG01 and GH01 have honors degrees. Two of the participants have national diploma as a qualification. None of the participants had a doctorate or a master's degree. Education level looks at the years of learning that the participant has successfully undertaken and completed classified using qualifications. According to Gudeva, Dimova, Daskalovska, and Trajkova (2012:1307) “A Qualifications Framework is an instrument for the development, classification and recognition of skills, knowledge, and competencies along a continuum of agreed levels. It is a way of structuring existing and new qualifications”. González Campos (2021:19) purports that there is a positive relationship that exists between a higher level of education and how well an individual can spot a scam email. This indicates that a participant's ability to understand, recognise, and manage phishing emails is influenced to some extent by their level of education.

4.2.4. Participant’s Job Title

The participants were employees in various divisions of the organisation, with the majority of them centred in the IT department. It was important to determine the participants' positions

within the company to determine how likely it was that the participant's role would influence his or her knowledge or comprehension. Some participants had technical IT backgrounds, while others came from non-technical roles. It was critical to ascertain whether users' understanding of the issues this research raised would be impacted in any way by their technical background. Participant AB01 was an Accountant, BC01, CD01 and MN01 were Test Analysts, DE01, EF01, GH01, HI01, IJ01, were Developers with varying areas of specialization. Participants FG01 and JK01 were Business Analysts. Participant KL01 was in the Human Resources Administration space. LM01 was a Data Archivist. Participant NO01 was a Service Desk Agent. Participant OP01 was a Network Engineer and PQ01 was an Integration Automation Consultant. This was an important demographic factor that was used to better understand how well participants comprehend the topics included in the interview guide based on their roles. Understanding their roles was important in order to determine the variation in the level of exposure to phishing attacks. The viewpoints participants shared largely originated from their experiences in the roles that they were in. In some instances, the views were inspired by previous experiences and organisational doctrines.

4.2.5. Years of experience in current position

This demographic characteristic enabled the researcher to determine how long the participants had been in their positions within their organisations. The researcher needed to know this information to determine whether or not the participants' opinions were at all likely to be affected by how long they had worked for the organisation. Participants AB01, CD01, DE01 and OP01 had been employed in their roles for over 4 years. On the other hand, participants EF01, GH01, HI01, IJ01, MN01, NO01, and PQ01 had been employed in their roles for 2 to 4 years. Participants BC01, FG01, JK01, KL01, LM01 had been in their roles for less than 1 year. It was critical that this research be as diverse and inclusive as possible. This increased its generalisability, allowing the findings to be applicable to various contexts. According to Ritchie and Lewis (2013) generalisation speaks to whether the study based on a sample can be deemed relevant beyond the sample and context of the research itself. Additionally, generalisation can be explained in two facets where it can be understood firstly as the qualitative nature of a research study that allows the establishment of findings that can be applied to populations or in other contexts beyond the sample of the study. Secondly generalisation can be understood from the perspective of theory building, this according to

Ritche and Lewin (2013:264) “involves generating theoretical concepts or propositions which can be universally applied”.

Kohfeldt and Grabe (2014:2036) state that “Universalism implies that it is possible to apply generalised norms, values, or concepts to all people and cultures, regardless of the contexts in which they are located”. A diverse set of participants cast the net wider which ensured that the study reflected a variety of viewpoints. This demonstrated that the study could be utilized consistently in many situations and minimized the possibility of researcher bias. Diversity refers to accommodating all genders, age groups, people of various educational backgrounds, people in various positions, and people with various degrees of expertise to ensure that they take part in the research study.

4.3. Thematic Data Analysis

The themes that emerged from the open-ended questions in the second phase of the interview guide are discussed in this section, and they are summarized in Table 4.3.

Table 4.2: Emerging themes

Question	Theme 1	Theme 2	Theme 3	Theme 4	Theme 5
1. How has your institution been impacted by cybercrime, particularly phishing attacks?	Phishing attacks significantly increased	Financial and operational impact	Client privacy violations	-	-
2. How has inadequate training, negligence, and malice contributed to the success of phishing attacks against institutions?	Absence of training increases vulnerability	User negligence of defined protocols	Users mishandling obsolete systems	-	-
3. What are the security measures that your organisation has taken to prevent social engineering attacks from compromising systems?	Training and Phishing simulation	Email monitoring systems	Firewall and System Updates	Cybersecurity Policy revisions	Multi-factor authentication and VPN
4. What are some of the visible inappropriate user behaviors that	Incorrect handling of phishing	User using work machines for	Users leaving their workstations	Password sharing	-

	you have seen in the workplace and believe increase the likelihood of phishing attacks being effective in your organisation?	emails	private uses	with machines not locked		
5.	What lessons has your institution taught you about how to avoid becoming a victim of phishing or other forms of social engineering?	Alertness to URL configuration, emailing rules, and phishing cues	The role of user training	Workstation best practice	-	-
6.	What steps can you suggest to other workers based on your own experience to help them guard against other social engineering attacks like phishing?	Reporting suspicious emails	Workstation cyber-hygiene	Setting up security applications	Self-education	Re-evaluation of password security

4.3.1. Impact of Cybercrime on institutions

The financial industry has seen an increase in social engineering attacks as a result of the COVID-19 pandemic. This question was designed to give the researcher a better understanding of how the participant's organisation had been affected by cybercrime, particularly phishing, from their perspective. The following themes were found in the participant responses to this question:

Theme 1: Phishing attacks significantly increased

"We have experienced a number of emails coming from spammers or email addresses not related to our business activities. Most of these spammers are businesses that we as the employees would not be familiar with" (AB01).

"We unfortunately experienced a lot of phishing emails during this COVID-19 period, and we continue to randomly get these mails" (BC01).

"We have received multiple phishing emails and unfortunately a lot of employees still fall victim" (DE01).

"Phishing attacks have increased have become more common and have impacted organisations in certain instances" (FG01).

The viewpoints expressed above represent the understanding that participants have on the question. As expressed by participants AB01, BC01 and FG01 phishing attacks had increased in their institutions and the COVID-19 pandemic accompanied with it a notable rise of this kind of cybercrime. In support of this perspective, Pranggono and Arabo (2021:1) state that "organisations across the globe have adopted the work-from-home (WFH) business model, increasing attack vectors and threats to corporate data. It is important to note that WFH has replaced normal for individuals all across the world. Additionally, this introduced scenarios where employees were expected to work using their own personal devices and home networks, which are frequently unprotected and lack the necessary standard security reinforcements". This is a pitfall many organisations fall into.

The response from FG01, shows that although such attacks have been on the rise, their impact has only been felt in some and not all instances, this demonstrates that where organisations have adequately trained users and made their systems impenetrable, the likelihood of attacks being successful is minimal to none. Many organisations have gone digital during the COVID-19 era, yet a lot of these organisations ignore the cybersecurity dangers associated with digitisation and take a reactive rather than proactive response to cybersecurity threats (Eian, Yong, Li, Qi, & Fatima, 2020). This indicates that they only consider the seriousness of cybersecurity risks when they have already been the victims of such attacks.

Theme 2: Financial and operational impact

> *"We experienced one of the biggest cyber-attacks during the pandemic. It had a huge financial and resource impact, and we were not as fortunate to have a backup disaster recovery site" (CD01).*
>
> *"The impact on the business was both financial and reputational. We were unable to service our clients for a month as a result of the attack" (JK01).*
>
> *"It has generated a loss of revenue for the business and has stalled business working days as the employees' laptops had to go in for security updates to prevent attacks" (MN01).*
>
> *"We were unable to login to most servers due to user negligence to a point where our terminal machines where targeted and our systems entirely compromised" (OP01).*
>
> *"The Attack mainly affected the daily operation of everyday business as many files were not backed up offline, they became corrupted and thus had to be recreated from scratch" (PO01).*

The participants shared their understanding on the implications of phishing attacks, what it meant for an institution to be compromised, and they gave examples to substantiate their viewpoints. According to Camillo (2017) the cost of breaches includes but are not limited to regulatory penalties, loss of business and reputational damage. Participant CD01 stated that the cyber-attack her organisation experienced resulted in financial and resource impact, especially seeing as the organisation did not have a backup disaster recover site. "A company's reputation can be tarnished, and its business can be destroyed in less than sixty seconds. A server malfunction or hacker can take out critical apps and trigger a disastrous chain of events in just a minute. A company's reputation might suffer irreparable harm from this, which would take months or years to repair" (Stanton, 2005:18). These are the irrefutable facts about the vulnerabilities organisations are subjected to when doing business online.

A disaster recovery (DR) plan is a strategy created to quickly restore all essential business operations in the event of a disaster. This plan includes all the steps necessary to handle emergency scenarios and restore IT infrastructure performance following a cyberattack, or a business disruption (Jorrigala, 2017). Organisations without this DR plan, as is the case in CD01's experience, are prone to experience downtime where operations are halted while recovery is being done. Participant MN01 also spoke on stalled working days where employees had to spend time bringing in their machines to be updated while business as usual (BAU) tasks were halted. Participant JK01 discussed the scenario where clients were not being serviced due to system unavailability. System downtime causes a loss of client confidence and has detrimental financial impact on organisations (Ibrahimovic & Franke, 2017). Business-critical data must be properly backed up and recoverable in the case of a disaster. Disasters cost less when adequately prepared for, with the aid of effective drills that emulate realistic disaster scenarios (Al-Hussain & Al-Shaikh, 2015:189). Furthermore, as part of the preparation, employee' files must be stored and mapped on home directories or shared drives on an organisation's network rather than local hard drives.

Theme 3: Client privacy violation

> *"Breaching of security resulting in the leakage of our member personal information, and some end clients ended up taking legal action" (HI01).*
>
> *"I work in the document and information management team, and we work with very sensitive and extremely private information regarding our clients and investors. The*

company has had to spend hefty amounts annually to train employees on the handling of such information and on cybersecurity in order to reduce room to be compromised" (LM01).

According to participant HI01, her organisation had experienced client privacy violations as a result of a breach that arose from a phishing attack, which resulted in lawsuits being filed against the organisation and clients pursuing legal action. Participant LM01, explained the nature of her position and how, as a result of it, she had access to handling sensitive client information. She also discussed how she had seen her organisation invest financially in user training and system security to lessen the likelihood of users falling prey to social engineering attacks like phishing. Aldawood and Skinner (2019:111) state that, "Social engineering attacks can result in confidentiality losses when private information that is only exclusively accessible to authorized individuals is accessed". Phishing attacks when successfully executed can cause information to lose its integrity since it is exposed to threat actors and so may be subject to modification or manipulation.

4.3.2. Understanding user behaviors that exacerbate phishing attacks

It is important to dissect the user behavior that exacerbates phishing attacks because sometimes all it takes for some attacks to succeed is for users to act in an untoward manner. The purpose of this question was to better understand, from the viewpoint of the participants, the extent to which they believe user negligence, malice, and inadequate training contributes to the effectiveness of phishing attacks in organisations.

Theme 1: Absence of training increases vulnerability

"Where training has not been sufficient, employees easily fall victim to phishing emails by opening emails, clicking on links, or replying to emails they are not supposed to thus endangering the whole business" (AB01).

"Without sufficient training someone can be very susceptible to phishing attacks, since they don't know what to look for, or they don't even know what phishing is or how it works" (GH01).

"Insufficient training of employees on basic cyber security awareness leads to employees answering or open click bait emails from hackers" (LM01).

When participants were asked on user negligence, malice, and inadequate training as concepts pertinent to increased phishing susceptibility. Participants AB01, GH01, and LM01 discussed how they had encountered situations where employees were vulnerable to phishing

because of insufficient training. Participant AB01 explains that all it takes is one click, and the entire organisation is put in danger. Employees cannot be vigilant when they do not know what to look out for and what is at risk. According to GH01 the lack of sufficient training heightens room for susceptibility because users are not adequately informed on different forms of social engineering including phishing. Hassandoust, Singh, and Williams (2019:2) posit that "internet users are now more aware of phishing, but phishing messages have also advanced, necessitating a greater awareness of information security on the part of users in order to keep them safe and secure online". Additionally, training is advantageous as it raises the level of comprehension that users display while working with systems and processes. Training allows users to switch from heuristic rapid processing to a more methodical and deliberate form of decision making informed by their increased understanding of information security (Hassandoust, Singh, & Williams, 2020:8). According to Bakhshi (2017) users' lack of awareness continues to be the key reason why attacks are successful, necessitating remedial action through post-incident training and ongoing IT security training. Training creates a notable impact on user awareness.

Theme 2: User negligence of defined protocols

> *"Security team is always giving out information on how to spot and avoid these emails, but I think users always rush to go through emails and click on the links provided on these phishing emails" (BC01).*
>
> *"Regardless of how much training they receive, users often become susceptible it may not be deliberately but as a result of not exercising due diligence" (JK01).*
>
> *"User negligence has resulted in employees opening emails carelessly and giving out their work emails details and passwords which might give confidential information to attackers" (MN01).*
>
> *"Despite several awareness programs, employees' lack of the knowledge and abilities to adopt internet safety precautions has resulted in our institution becoming a target of phishing attacks. The employee's age or non-ICT background is partially to blame for this" (NO01).*

The abovementioned extracts corroborate the fact that even in instances where employees have access to information on cybersecurity, when they choose to disregard what their organisations prescribe as best practice, they are likely to put those organisations at risk. The security team, in participant BC01's case, always shares information, but because employees scan emails quickly without properly considering what is asked of them, they end up clicking

on fake links. This is corroborated by Mohammad, Thabtah, and McCluskey (2015:5) who note that users are vulnerable to phishing for a variety of reasons, one of which being the fact that users sometimes choose to focus on their main responsibilities while security indicators are viewed as secondary in importance. Security is of the utmost importance, and when users aren't conscious of adhering to the proper conduct, it eventually affects business continuity when organisations are compromised.

The term "due diligence" as described by Jones and Moncur (2020:33) refers to the steps needed to make sure that an activity in this case an email and any accompanying information are secure. Furthermore, where due diligence is concerned it is important to leverage technology solutions that assist users in navigating through processes. This helps to ensure that users are equipped with the necessary information to make educated decisions about who to trust. Users may be more susceptible to fraud if there is a lack of due diligence. "Employee behavioural patterns when responding to phishing mails is influenced by their personality qualities and cognitive abilities. When receiving a target phishing email, employees make decisions about how to respond based on information cues that operate as a bridge between the email and their internal perceptions, which are influenced by their traits and prior knowledge" (Anawar, Kunasegaran, Mas'ud, & Zakaria, 2019:2866).

According to MN01, some employees have a natural tendency to ignore emailing caution by opening emails without considering security, and to reveal their passwords and email addresses. This leak of personal information can be harmful if it falls into the wrong hands. The behaviours exhibited by employees indicated by participant MN01 constitute extreme negligence. Such actions can be classified as purposeful user malice especially where organisations have shared information and defined strict protocols against password sharing.

Participant NO01 classifies some of the employee's lack of knowledge as attributable to age and a lack of a technical or IT background. This is supported by Jampen, Gür, Sutter, and Tellenbach (2020:18) who developed the Suspicion Cognition Aromaticity Model (SCAM) model, which defines five parameters that can be used to better understand elements that influence phishing victimization, and it incorporates experiential, dispositional, behavioural, and cognitive elements. The five parameters are personal cyber-risk perceptions, email processing patterns (both heuristic and systematic), poor self-regulation, and developed email habits.

Theme 3: Users mishandling obsolete systems

> *"Mostly it is user negligence because if you read the phishing email thoroughly, you'll be able to spot one. Most users are just quick to respond" (DE01).*
>
> *"Phishing method have improved over the years and the inadequate training to keep up with the latest phishing techniques as well as old infrastructure exposed us to the greater risk of cybercrime" (PQ01).*

Participant DE01 discussed user negligence and the visual indicators that users overlook while responding to emails hastily. Participant PQ1 discussed the value of training as a strategy to stay abreast with the constantly evolving nature of phishing techniques. This participant (PQ01) then went on to discuss how outdated infrastructure puts businesses at risk of being compromised when at the hands of untrained, malicious, and negligent users who may mishandle it. According to Tweneboah-Koduah, Skouby, and Tadayoni (2017) best practice standards must be established to protect critical infrastructure from cyberattacks.

4.3.3. Security measures against phishing attacks

"Security can be defined as the perceived or actual ability to prepare for, adapt to, withstand, and recover from dangers and crises caused by people's deliberate, intentional, and malicious acts such as terrorism, sabotage, organized crime, or hacking" (Jore, 2019:157). Security measures refers to the preventive steps undertaken to ensure that adequate reinforcements are in place to lower the success rate of phishing attacks. The researcher looked into the security precautions that the participants' organisations had put in place to guard against social engineering attacks like phishing that could compromise systems. The purpose of this question was to determine the degree to which participants understood and were aware of their organisations' efforts to combat various forms of social engineering. It also sought to determine what safeguards had been put in place by the organisations. The several themes that emerged were:

Theme 1: Training and phishing simulation

> *"The company has put in place training programs during the year to teach people how to identify phishing emails. Alongside training, the company also sends random emails similar to phishing to see if any employees would click on the email. Where employees fall victim to these emails, they are obligated to take a compulsory course that teaches them to identify any phishing attacks" (AB01).*

"Training of users to proactively identify phishing emails and we have Awareness Campaigns in place" (DE01).

"Employees are trained to identify cyber threats. Additionally, employees tend to be aware of the kind of sensitive information that would never be requested by a legitimate institution" (EF01).

"There are phishing emails sent to us by the security team just to train or make us aware of such emails. This helps a lot because in a way we are now able to scan through any mail that comes through, and we do not just click random links" (IJ01).

"We have cyber security training every month. Our IT department has advised against clicking any foreign links sent to our work emails and we have blocked all unwanted popups and questionable websites" (LM01).

"Since the attack happened, the security has since improved and the ongoing security course for all the employees to update them with current method of cybercrime" (PQ01).

Ansari, Sharma, and Dash (2022:67) assert that "most users lack awareness on phishing, and this contributes to its effectiveness, leading to phishing attacks continuously increasing". Additionally, users who are knowledgeable are aware of cyber security, how to defend themselves, and how to exercise awareness. This can be a successful method to reduce phishing-based attacks globally. According to Masadeh (2012:63) "training is defined as a structured approach in the workplace designed to modify attitude, knowledge, or improve competence using learning experiences such as knowledge sharing to accomplish effective performance from employees in a specific area". Training helps define the rules on expected conduct which help users take in information and reinforce it through regular practice. This is supported by the feedback from participants AB01, DE01, EF01, IJ01, LM01, and PQ01. Jensen, Dinger, Wright, and Thatcher (2017:599) contend that automatic removal or quarantining of phishing messages and linked URLs is one of the three strategies typically utilized by organisations to prevent phishing attacks, which supports the response provided by participant LM01.

"Organisations utilize and rely on phishing simulations as awareness tools" (Lamas, Loizides, Nacke, Petrie, Winckler, & Zaphiris, 2019:600). Simulated attacks, designed to resemble actual attacks, are used to spot vulnerabilities and threats in an organisation's human defenses (Rizzoni, Magalini, Casaroli, Mari, Dixon, & Coventry, 2022:2). Additionally, these phishing simulations are permitted simulated attacks used to gauge staff members' aptitude for spotting phishing emails. The number of employees who become victims and click on the fake links is reported in the simulation results. Such users are subsequently given remedial training to

educate them and increase their resilience to phishing attacks. This speaks to the compulsory courses referred to by participant AB01.

Theme 2: Email monitoring systems

> *"Users restricted to using only Microsoft Outlook to access emails on their mobile devices. The company rolled out Microsoft Intune" (BC01).*
>
> *"There are systems in place that monitor the emails sent and received by employees. If this system identifies a message (perhaps sent to multiple accounts) with suspicious content, all employees are immediately made aware of the threat" (EF01).*
>
> *"I believe emails are flagged, so that bulk of the attacks don't get through to users. But if a suspicious email does appear users can report it and then any email similar to those will be flagged as well and removed" (GH01).*
>
> *"We have mime cast that can block certain emails that seem dodgy and out of character" (OP01).*

According to Hadjidj, Debbabi, Lounis, Iqbal, Szporer, and Benredjem (2009:124) email communication is exploited for many illegal purposes due to its ease of use and inherent vulnerability. There is very little system security surrounding email communications. Strategies that can be implemented include email filtering, flagging, and monitoring. "Email Profiling is a system used to determine whether an email received is actually from the author who is listed in the email's metadata. In order to accomplish this, email profiler generates behavioral profiles for each sender and assesses new incoming email against these profiles" (Duman, Kalkan-Cakmakci, Egele, Robertson, & Kirda, 2016:410). Feedback from participant EF01 talks to these systems that are used for monitoring emails and detecting suspicious ones. In addition to ensuring access control for organisations, platforms like Mimecast, Microsoft Intune, and other email filters safeguard and preserve the information assets of organisations from nefarious threat actors. This is supported by Williams and Boonthum-Denecke (2017:3) who state that, "many organisations host their corporate email suites on cloud services such as Mimecast this platform enables administrators to monitor conversations and allow for network collaboration".

According to participant BC01 there are risks that organisations try to mitigate by implementing Microsoft Intune when users try to access emails on their mobile devices. Tsalis, Virvilis, Mylonas, Apostolopoulos, and Gritzalis (2015) state that the wide variety of capabilities that smartphones have, have led to the usage of such gadgets becoming more popular with users using them for social networking, email access, online browsing, and

online shopping. However, smartphone security mechanisms are still in their infancy, and it is still unclear how effective they are. Therefore, when using their devices for sensitive online activities, smartphone users face greater dangers than desktop/laptop users (Alzubaidi, 2021). This demonstrates the necessity of email monitoring tools like the one referred to by participant BC01 for online system security.

Theme 3: Firewall and System Updates

> *"We have various firewalls in place. All PCs have been updated and has protection software to attempt to mitigate the risk" (CD01).*
>
> *"Secure and regular changing of passwords methods are in place and Firewalls are also put in place to create complexity for attackers gaining access to systems and software" (FG01).*
>
> *"A Firewall Software has been installed on our computers to give an extra layer of security and the use of OTPs has been put in place as a security measure" (MN01).*
>
> *"We also have roaming firewall in addition to the one we already have for LAN and Wi-Fi to be able to sandbox any malicious websites and block them" (OP01).*
>
> *"We have the OTPs in place on our systems when logging in. Also, log in passwords are changed every 30 days" (KL01).*
>
> *"We are mandated to use strong passwords which have a combination of special characters, numbers, lower and uppercases and must be minimum of 8 characters long. There are also intrusion detection systems which allow system administrators access when violations occur" (NO01).*

Network firewalls and host-based firewalls are the two main types of firewalls. According to Mukkamala and Rajendran (2020:363) "network hardware is used by network firewalls, which aid in securing communication across networks. Firewalls that help filter traffic to endpoints or hosts are known as host-based firewalls". Participants CD01, FG01, and MN01 discussed the presence of firewalls and the role the software played in protecting their organisations' systems. According to Vitak, Liao, Subramaniam, and Kumar (2018) the recommendations by computer security experts to internet users typically includes: updating the software and operating system on their device, utilizing a password manager to save strong and distinctive passwords, and the enabling of two-factor authentication. One-time pins, as described by participant KL01, are a crucial component of multi-factor authentication and are intended to strengthen a system's resiliency and reduce its susceptibility to threats. Passwords have to be regularly changed and made with a certain degree of complexity. Chaudhry and Rittenhouse (2015:30) posit that users frequently select passwords randomly to

make them simple to remember. It is important to use comprehensive password strength and metering tools. The password rules referred to by participant NO01 become crucial at this point.

Theme 4: Cybersecurity policy revisions

> *"There are certain policies in place in our institution which are: Acceptable Encryption and Key Management Policy, Personnel Security Policy, Data Backup Policy, User Identification, Authentication, and Authorization Policy they address cybersecurity issues" (HI01).*
>
> *"We currently have an information security policy, remote access policy, a wireless communication policy, password protection policy, email policy, and digital signature policy" (JK01).*

Cheng, and Wang (2022:192) list the following eight techniques for combating cybersecurity threats: "(1) Strengthening institutional governance for cybersecurity; (2) Revisiting cybersecurity key performance indicators; (3) Explicating cybersecurity policies, guidelines and mechanisms; (4) Training and cybersecurity awareness campaigns to build cybersecurity culture; (5) Responding to AI-based cyber-threats and harnessing artificial intelligence to enhance cybersecurity; (6) Introduction of new and more sophisticated security measures; (7) Paying attention to mobile devices use, using encryption as a daily practice; and (8) Risk management". The third approach backs up the comments made above by participants HI01 and JK01 regarding the role that specific organisational policies play in countering cybersecurity attacks and ensuring that sufficient cyber-hygiene standards are enforced at work.

Theme 5: Multi-factor authentication and VPN

> *"We have Multi factor Authentication to access internal systems" (DE01).*
>
> "*VPN connections are in place when we have to access our systems" (FG01).*
>
> *"The company has enabled two factor authentication method on personal devices when coming to work related tasks" (PQ01).*

Two Factor Authentication, also known as 2FA, two step verification, or multi factor authentication, is a higher level of security that involves dual verification of users before granting them access to a system (Ometov, Bezzateev, Mäkitalo, Andreev, Mikkonen, & Koucheryavy, 2018). It goes beyond requiring a user's username and password and instead requires user-specific information as a passcode to authenticate them (Umarov, 2018). "The

verification code is obtained either from an application operating on the phone or via SMS" (Karapanos, Marforio, Soriente, & Capkun, 2015:485). Furthermore, this soft token authentication approach requires the user to copy the verification code from their phone to the browser.

Rode, Patil, Tare, and Kandane (2022:2937) state that, "virtual private networks are another type of network security that can encrypt connections between end points and networks, typically through the internet. Remote VPN connection frequently uses the IP configuration for secure sockets layer to permit communication between the web and device". VPN allows organisations to offer private intranet access over a public network, with the ability to regulate network traffic whilst ensuring data privacy and access restriction through encryption (Hossain, 2015). Businesses can utilize VPN to set up a secure tunnel for all of their internet traffic, preventing hackers from intercepting their data, as participant FG01 purported. However, using the recommended VPN connection rather than downloading a free VPN is safer for employees.

4.3.4. Human risk factors in the workplace

This segment focuses on the phishing attack risk factors that result from behavioral patterns that attackers take advantage of. Participants were asked to discuss user behaviors that they have observed in the workplace and which they believe would make it more likely for phishing attacks to be successful in their organisation. The aim of the question is to shift attention away from external blame and toward examining internal flaws that foster the effective proliferation of such attacks. The themes that emerged from the responses of the participants were:

Theme 1: Incorrect handling of phishing emails

> *"Replying to phishing emails, clicking on links in unknown emails, Sharing phishing emails with other employees rather than the IT department" (AB01).*
>
> *"The main user behavior that could have led to the organisation being at risk is users clicking on suspicious links or visiting sites that they are not meant to be visiting" (CD01).*
>
> *"Clicking links and not reporting suspicious emails" (DE01).*
>
> *"Staff members using unsecure networks and also clicking on links coming from outside the organisation and not verifying that the link is indeed coming from the company" (JK01).*

> *"Clicking on emails links without scrutinizing the email. Users/employees not verifying the email address or email domain" (MN01).*

Users must have the capacity to pause, reflect, and verify their emails before responding to requests. This approach, as simplistic as it may be, is able to avert a cyber-attack. Participant MN01 highlights situations where other employees responded rapidly to emails without carefully reading them. Younis and Musbah (2020) posit that users would likely be more vulnerable in situations where they don't intuitively understand URLs, while the contrary is true in situations where they do. User having knowledge alone does not offer practical methods for spotting phishing attacks. Users sometimes become victims by reacting to emails that trigger urgency, fear, or pressure with time bound expectations. Wen, Lin, Chen, and Andersen (2019:5) "assert that this urgency tactic used by threat actors leads users to mistakenly believe that visual cues are reliable indicators of an incoming email's authenticity. Furthermore, due to the frequency of these attacks, organisations have established designated IT department teams were phishing emails can be reported. Users are urged to use these channels because they help prevent more people from falling victim by spreading the word to alert other users". As participant AB01 pointed out, when employees share phishing emails with their co-workers rather than the IT department, the risk increases and there is no assurance that these emails would be recognized and handled appropriately.

Theme 2: Use of work machines for personal purposes

> *"Employees signing up to personal sites using their work emails and opening emails from incorrectly spelt email addresses" (BC01).*

> *"Perhaps users are cautious of attacks when using their company email, but they might not be so vigilant when answering personal emails on a company device" (EF01).*

> *"The use of work resources for personal use, for example, using work emails to sign up for a shopping website or gaming site. Searching different personal sites using a work PC" (LM01).*

> *"User negligence/malice when employees use company laptops to access private sites thus exposing the company to phishing attacks for example: Facebook" (PQ01).*

Personal unsecured devices used by employees to access work networks and work machines used for personal purposes bring about risks to the security of an organisation. "Devices that are owned by the company come with security regulations that must be followed, including the encryption of critical data and the usage of passwords. On equipment not owned by the

company, these regulations cannot be easily applied" (Annansingh, 2021:397). Furthermore, the organisation must be aware of who is utilizing the network and what devices are doing so in order for any security strategy to be effective. Users should be provided with a list of programs that are legal and illegal as a reference. When users are redirected to personal websites from work emails, as indicated by participants BC01, EF01, LM01 and PQ01, there are privacy risks because organisations have little control over the information that users share while on those websites, and the Internet Protocol (IP) information of the organisations' information can be compromised.

Theme 3: Users leaving their workstations with machines not locked

> *"Employees leaving their machines unlocked" (BC01).*
>
> *"Employees are not always mindful and do not always lock the laptops leaving them exposed which also poses great risk" (FG01).*
>
> *"There are user behaviors that are risky, and these include: Not locking a pc when going to the bathroom and giving a work pc to family member to use" (HI01).*
>
> *"Employees leaving the laptops unlocked when stepping away is something I have also seen happening" (KL01).*

Users have a propensity to become complacent when it comes to security restrictions, which can result in actions that are either purposeful or unintentional, including leaving desktops and laptops unlocked. This poses a serious danger, especially if inside users collaborate with threat actors to compromise systems and steal data. The process to lock a machine only takes seconds, but users frequently become lazy and forget to do it. Beguin, Besnard, Cros, Joannes, Leclerc-Istria, Noel, Roels, Taleb, Thongphan, Alata, and Nicomette (2019:82) posit that, "even though most employees are aware they must lock their computers every time they leave their desks, regardless of how long they will be gone, many of them still choose not to do so most of the time. It becomes unclear whether or not this is out of neglect or because they deliberately disregard the security advice". Participants BC01, FG01, HI01 and KL01 speak on the issue of users frequently not locking their machines when stepping away. The risks associated with this behavior are explained by Khawandi, Abdallah, and Ismail, (2019:232) who assert that, "desktop lock is one of the solutions that may be used to secure a computer, control access, and lock a computer, preventing unauthorized users from accessing confidential information and resources. The user has the option of locking the computer with

a single click or allowing desktop lock to lock the system automatically at any moment. When screen lock is on, only the currently logged-in user or an administrator is permitted access to the computer".

Theme 4: Password sharing

> *"Employees are sometimes negligent with passwords being shared or left exposed which also poses great risk." (FG01).*
>
> *"Sharing passwords is also a user behavior that is risky" (HI01).*
>
> *"Employees sharing passwords is a risk factor that I have frequently seen happening" (KL01).*

According to Alohali, Clarke, Li, and Furnell (2018:8) the password system is the most widely utilized kind of authentication for securing end-user data and systems. However, there are dangers connected to password reuse, storage, and sharing. Threat actors are able to get access to numerous systems by successfully breaching one system using a shared, saved, or previously used password. It develops a chain effect. "Examples of human errors in the area of information security include sharing the username and password with their co-workers, writing them down on sticky notes that they place on the desk or monitor. The opening of unknown emails and attachments, downloading software from the internet, and leaving systems in login status while unattended" (Safa, Von Solms, & Futcher, 2016:15).

4.3.5. Remedies to reduce susceptibility to social engineering

In this section of the interview, the participants talked about the lessons their organisations had taught them about phishing and other forms of social engineering. This question drew from the knowledge of the participants as gained from the lessons learned at their place of employment. Knowledge has been described by Alavi and Leidner (1999:110) as "a state or fact of knowing" with knowing being a condition of "understanding gained through experience or study; it comprises of what is perceived, discovered or learned". Knowledge is either tacit or implicit and tacit knowledge comes from the gradual knowledge and understanding that an employee gains when working. This knowledge and understanding is then retained and processed by the employee as implicit knowledge in the form of experiences (Jin-Feng, Ming-Yan, Li-Jie, & Jun-Ju, 2017). There were the two classes of knowledge that were used to prescribe remedies and to make suitable recommendations. With the help of these classes of knowledge, we were able to draw meaningful inferences about the

participants' competence from the information they shared. These inferences were reinforced by the participants' feedback, which was influenced by previous experience, intuition, or knowledge gained from company policies or reading documentation. The themes that emerged from the responses were:

Theme 1: Alertness to URL configuration and emailing rules

> *"They have taught us or given us strategies on identifying phishing emails. For example, things like Broken English, Weird Date formats, weird addresses, Compulsory links in emails" (AB01).*
>
> *"We have been taught to avoid providing personal information on email. To look out for fake URL's. Emails with bad grammar and incorrect spelling. If it looks too good to be true, it definitely is" (BC01).*
>
> *"We have always been taught to think before we click, verify a site's secure socket layer (SSL) certificate, keep our browsers up to date with the latest updates, and use antivirus and to never give out personal information" (DE01).*
>
> *"We are taught to not just click on every link sent to our emails" (HI01).*
>
> *"I have learnt from work to scan thoroughly through an email sent by anyone. And also, one can never win a big prize out of nowhere" (IJ01).*
>
> *"Do no click suspicious links. Be careful about websites that do not have valid SSL certificate and start with http instead of https" (NO01).*
>
> *"Always double check the sender email address and if sceptical, call the person and verify that the email id from them. Check the grammar of the email as well" (PQ01).*

Feroz and Mengel (2015) put forward that users must conduct sanity checks before clicking a URL, such as paying close attention to how the website's address is spelt and weighing the potential risks involved in visiting the URL. This is supported by the remarks made by participant AB01 on the pointers her organisation has shared with them on identifying phishing emails. Participant BC01 also addresses the area of grammatical errors as being a typical indicator of phish emails. The fundamental guidelines for responding to emails include validating the sender, contextualizing requests before granting them, scrutinizing email header, and ignoring emails that make promises of instant wealth or prizes (Salahdine & Kaabouch, 2019). Verifiability is confirmed using SSL certificates which participants DE01 and NO01 refer to. The Secure Socket Layer (SSL) protocol uses a digital certificate, and it is a vital piece of technology that protects personal information processed by the browser and delivered to a mail server by using encryption (Arai, 2015).

Theme 2: The role of user training

> *"Our company mitigates risks by ensuring that employees are made aware of the risks and reminding them to always be vigilant" (CD01).*
>
> *"Our company ensures that adequate training is provided, and awareness is a constant reminder to not take phishing attacks lightly. This also ensures that employees are able to report such instances by identifying attacks early on, informing the correct parties, and not sharing any information" (GH01).*
>
> *"Training has been provided to us on how to identify malicious attacks. Additionally, Awareness campaigns have been put in place to create awareness of such attacks" (MN01).*

"People are the weakest link in any cyber environment, it is important to ensure that they receive the proper training to guarantee that they are aware of the different attacks they may encounter in a corporate context" (Sebastian, 2021:5). Furthermore, the establishment of a cyber-aware staff culture is essential because it serves as a vital technique for lowering the likelihood of being compromised successfully. Awareness allows for vigilance and employees are able to identify and handle phishing emails correctly. Participant CD01 described how her organisation uses awareness as a risk mitigation technique, whereas participant GH01's organisations employed awareness together with a considerable level of user training. Participant MNO1 backed up his assertion by detailing how his organisation held ongoing initiatives to educate employees about cybersecurity and cybercrime.

Theme 3: Workstation best practice

> *"The company trains us to avoid clicking on links from people who are outside the organisation and to double check our machines when we come back to our desk because the attackers can plug a USB on a machine and copy data as you work" (JK01).*
>
> *"The company I work for sends out emails almost weekly to remind us of how we can avoid becoming a victim of Phishing. In which some of the advice is that we must lock our laptops when stepping out and we must never share our passwords with anyone" (KL01).*

"We are taught to always stay alert to suspicious emails and links. Always lock your PC and never leave it unattended" (LM01).

Cyber hygiene promotes ethical conduct, and from the participants' feedback it is evident that different companies have different methods for enforcing rules. According to participant JK01, her organisation urges them to exercise extra caution when it comes to the links they receive and to pay attention to their computers whenever they step away from them and then return to them. This is because information can sometimes be erased or stolen through the insertion of infected flash drives that enable users to remotely access an employee's computer.

4.3.6. Recommendations to mitigate phishing attacks

This section of analysis makes important recommendations based on participant responses. Based on their personal experiences, the participants discussed some of the measures they would advise other workers to take to safeguard themselves against different social engineering attacks. The responses were also influenced by the lessons employees received from their workplaces. The following themes emerged:

Theme 1: Reporting suspicious emails

"Do not share emails from unknown sources, read emails carefully before clinking any links, forwarding any suspicious emails to the IT department immediately to alert them to potential phishing" (AB01).

"Don't open emails or links from untrusted or suspicious sources. If something seems suspicious it probably is. Ask for advice or assistance if you are unsure or suspect a cyber threat. Legitimate institutions will never ask for sensitive information like one time pin" (EF01).

"If you are not sure about something, it is better to ask the security department in your organisation" (HI01).

When an email is reported to the IT security team or other designated personnel, information can be shared with staff members more quickly, reducing the number of others who might be misled by the same email. To make communication more seamless and simpler, it is crucial for users to have open lines of communication with members of the security IT teams. This is corroborated by participant HI01, who stated that her company has an open-door policy that welcomes inquiries at any time, making it simpler to report emails.

Theme 2: Setting up security applications

> *"Be Wary of Pop-Ups. Install an Anti-Phishing Toolbar" (DE01)*
>
> *"Setup two factor authentication, when possible, set up an authenticator app like Microsoft Authenticator" (GH01).*
>
> *"Use two factor authentication method on all sites" (PQ01).*

"Pop-up windows on computers show advertisements or entire web sites in front of the one that is currently open. Pop-ups are advertisements that users see above other material in their own windows" (Wijaya, & Yulianti, 2020:34). These pop-up advertising windows generally won't close unless the user makes a conscious effort to close them, and occasionally these pop-ups are linked to malware, which, when clicked, downloads the malware (Mishra, Butakov, Jaafar, & Memon, 2020). This affirms the point of view held by participant DE01 who suggested individuals be wary of pop-up windows and use programs like the anti-phishing toolbar. According to Adebowale, Lwin, and Hossain (2020:2) "anti-phishing toolbars are created to prohibit users from accessing phishing web sites where their private information would be requested and then provided to criminals". Participant GH01 discussed the role and importance of users having verification applications like Microsoft authenticator on their devices to allow for dual verification. According to Khaskheli, Sherbaz, and Shaikh (2022:19) "Microsoft authenticator is a multifaceted application for cell phones that produces time sensitive codes utilized during the Two-Step Verification process". The aim of the dual verification process is to add an additional layer of security. According to Naidu (2022:4307) having this extra layer makes it harder for an unauthorized person to access a target like a real region, registered machine, employer, or data set. For instance, the attacker might successfully guess the passcode but lack the token needed to authenticate the user. Without the user's phone, which this token is typically connected to, the attacker will not be able to access the system. This is why the recommendation made by participant PQ01 for two factor authentication is very important.

Theme 3: Workstation cyber-hygiene

> *"Always lock my machine even when stepping away for a few seconds and avoid using public Wi-Fi connections" (BC01).*
>
> *"Avoid leaving your work laptops at friends' houses. Always lock your laptop when you step out, even at home. Avoid using people's USBS or charging their phones*

using your work laptop because that may put the company's information at risk" (KL01).

"Public Wi-Fi is unsafe and known for having security vulnerabilities, these shortcomings not only pose a significant risk to individual devices but also a much greater risk to organisational data assets, with potentially catastrophic financial consequences for the organisations" (Chigada & Madzinga, 2021:5). Participant BC01 echoed this view, stating that she believed that it was crucial to refrain from using public or free wi-fi networks that are usually found in restaurants or public areas. Participant KL01 gave advice regarding the value of maintaining work equipment and the need for users to be watchful of insertions of USB drives onto their machines. Even when working remotely or moving with their business laptops from one place to another, employees must always be vigilant. When inserted into machines, USB drives present a significant danger. According to Tischer, Durumeric, Foster, Duan, Mori, Bursztein, and Bailey (2016:307) *"a USB drive's firmware can be modified by an attacker to turn it into a network interface capable of intercepting sensitive data or into a USB human interface device that automatically runs malicious code. In the same manner, file previews are created immediately upon connection, and installed application flaws can make an attack possible"*.

Theme 4: Self education and training attendance

"Keep Informed About Phishing Techniques" (DE01).

"Scan through your emails. Google that company that you received an email from, if need be, and go and search for that person on LinkedIn if need to verify information" (IJ01).

"I would recommend that all staff members attend the training that the company gives, and the risk team monitors if staff members adhere to the training requirements" (JK01).

"Do those security training courses offered at work, they are very important and minimize the risk of getting hacked" (LM01).

"Workshops and quizzes will help educate our users as to how to manage themselves online" (OP01).

"The security awareness team should use a variety of communication channels and methods to regularly disseminate security information in order to engage the workforce and reinforce training concepts. Employees need a reason to care about security. The hope is that compliance with these training requirements will result in long term positive impacts on

security behaviours" (Haney & Lutters, 2020:92). Participant DE01 addressed the importance of employees taking personal initiative to keep informed on phishing along with the techniques that phishers use. Participant IJ01 highlighted the significance of employees using due diligence actions, such scanning emails and confirming senders before fulfilling requests. "Awareness training is required to ensure that staff are more aware of the potential implications of their behaviour in the workplace" (Blythe, Gray, & Collins, 2020:120). Participant JK01 emphasized the value of training while also outlining the steps risk teams in an organisation must take to guarantee compliance. Participants LM01 and OP01 made the point that employees should make a conscious effort to participate and fully complete the security training sessions provided at work. These courses are crucial in lowering the potential for vulnerability.

Theme 5: Re-evaluation of password security

> *"Use a password manager to generate complex passwords, that way you can't fall victim to an attack where they use a known password of yours. Don't reuse passwords" (GH01).*
>
> *"Change your password as soon as you notice that one of the other employees might know it. Ensure the cell phone that's used to send one-time pins is yours. Avoid having simple passwords such as where you were born, family member's name or name of your school" (KL01).*
>
> *"Don't click on email links that you don't know where they're from. Always verify the email domain. When prompted, never enter your password on links or attachments. Regularly change your password using characters, numbers, and symbols" (MN01).*

Passwords have been used for identification verification and this has become a very popular practice in recent years. According to Anand, Susila, and Balakrishnan (2018:1208) "using separate passwords would address the security issue, but users forgetting passwords would still be a problem. Using password manager and storing all important passwords will reduce the chance of passwords being lost or misplaced". Participants GH01, KL01, and MN01 brought up three noteworthy issues with passwords. They all agreed that it was crucial for users to avoid using the same passwords more than once and to avoid creating passwords with easy-to-crack combinations. *"Security experts often recommend using password management tools that both store passwords and generate random passwords. However, research indicates that only a small fraction of users use password managers with password*

generators" (Pearman, Zhang, Bauer, Christin, & Cranor, 2019:319). When users recycle or reuse the same password across different systems the risks that come with being compromised become higher. Bojinov, Bursztein, Boyen, and Boneh (2010:295) "put forward that, users prefer to use predictable and related passwords across multiple websites because they feel uneasy using random, independent, or impersonal passwords. Furthermore, the risk is increased if the attacker has prior knowledge about the user. With this information, an attacker can successfully guess the correct password from the collection by searching for victim-related keywords in the password storage and crossing their fingers that those keywords appear as part of a password".

4.4. Chapter summary

The results in this chapter brought up a number of significant issues that provided an indication of participants' current levels of comprehension of phishing. With the help of these findings the researcher was able to make a clear cause and effect analysis which can assist readers in getting to know the wide range of factors that influence a given outcome. Knowing what other actions cause organisations to be effectively compromised by phishing attacks. Fortunately, the outcomes and themes that arose from the analysis corroborated the views held by extant literature. Firstly, the topic of discussion was the actual effects of cybercrime. Participants talked about how their organisation had previously fallen victim to cybercrime. Secondly, participants emphasized the crucial part users can play in working with organisations to avoid phishing attacks, particularly when threat actors aim to target the human line of defence of an organisation. Thirdly, the participants candidly discussed their opinions on the current level of security in their company. This made it easier to understand the background of the participants' and their amount of security measures that they are exposed to in their workflows and processes. The fifth and sixth themes were centred on recommendations and likely interventions that participants had to put forward for managing and mitigating user risks.

Chapter 5: Conclusion, Recommendations, and Implications of the Study

5.1. Introduction

In this chapter the conclusions were drawn in light of the study's objectives, research questions, and findings. There will also be an explanation of the ramifications of these findings, the recommendations that follow, and the intended contribution to previous research, existing organisations, and system users. The study sought to determine the remedies to reduce users' susceptibility to phishing attacks. In addition, the aim was to identify important elements that lead to susceptibility. The study examined existing issues from a process and systematic viewpoint and how these contribute to organisations being susceptible to phishing attacks. In order to help relevant stakeholders, make well-informed decisions about how to reduce the high success rate of phishing attacks. The "who" part examined the users who affect and are also affected by social engineering, and the "how" part outlined the possible actions that could be taken to move towards a resolution of the identified issues.

The first section of the chapter provides a conclusion on the literature review. The second section summarises the conclusions from the primary study looking at three perspectives: the aims of the study, the biographical analysis and lastly the research objectives. The third section discusses the recommendations as uncovered by the data analysis and extant literature. The study's implications for future research and policy are discussed in the fourth section.. The fifth section addresses the limitations and contributions of the study. The chapter ends by emphasizing how the research's findings were positioned to add value to scholarly discourse and demonstrating how the research project was conceptualized through to its successful conclusion.

5.2. Conclusion from literature review

The study's literature review, which was covered in Chapter two, discussed what had been written about phishing before, looking at the theories that support and explain social engineering, particularly phishing. A literature review, according to Ramdhani, Ramdhani, and Amin (2014) is an impartial, comprehensive synopsis and critical analysis of pertinent

research with the objective of informing the reader about the body of existing literature in a specific field, prevailing theories, and identifying gaps that offer an opportunity to lay the groundwork for further investigation. The literature review also established from previous studies that users' state of emotions when engaging with systems have an impact on their decisions and the rationality of their choices at a given moment. It then becomes necessary for organisations to uncover detrimental conduct exhibited by internal users that translate into risk. Phishers thrive on manipulation. *"The goal of social engineering techniques is to alter the cognitive and emotional conditions of the victim so that instead of operating mindfully victims will tend to rely on heuristics to make a judgement"* (Naidoo, 2020: 308).

The theoretical framework that underpins the study includes two theories. Routine activity and Rational choice theories govern the study. The theories' approaches are interconnected, and pertinent to the study and are able to explain how crime occurs. Additionally, the theories enable the research to establish the factors or environmental settings that influence the occurrence of untoward behaviour and present an opportunity to offend. According to Campedelli, Aziani, and Favarin (2021:708) *"the routine activity theory postulates that offenders and victims–or targets–usually meet during everyday non-criminal activities"*. There are ten principles of opportunity that explain factors that make regular environments more conducive for criminal behaviour by turning them into places where it takes little effort to conduct crimes. Users with low vigilance and a high propensity to succumb to visceral triggers make daily work environments more appealing for victimization, particularly in areas without guardianship. In addition to assuming that people have a cause for acting the way they do, rationality also assumes that the people's actions at that time were as rational as possible in light of what was believed, desired, or achievable (Hindmoor & Taylor, 2017:216). These assumptions underpin rational choice theory and serve as important indicators for interpreting human behaviour. The study established that a cost benefit analysis is used as a decision-making scale that informs the decision of an offender on whether to perpetrate a crime or not, and whether a target chooses to open a phishing link or not.

In-depth study has been done in the past on the types and evolving nature of phishing attacks. This has been a crucial step in updating the literature to reflect the attack vectors threat actors employ against unwary users of different systems. The study discussed some of the most common ones explained by (Khan *et al*., 2020). *"The evolving nature of phishing attacks*

requires viable and improved methods for its detection as there is no silver bullet for phishing elimination" (Alsariera, Adeyemo, Balogun, & Alazzawi, 2020:142532).

"An interchange between a deceiver and a target receiver occurs, but the decisions made by the receiver ultimately determine whether the deception is successful" (Proctor, & Chen, 2015:722). The study was able to show from the literature review the influence that people can have on enabling or deterring an attack. Criminals are aware that while it may be impossible to penetrate complex systems, people are the most readily comprisable target for infiltration. Therefore, it is essential to understand these behaviours in order to address the personality flaws that different people introduce. This is so that organisations can define the proper reinforcements that can be put in place to govern expected user conduct more especially when it comes to managing email infrastructure and online communication.

According to Md, Jaiswal, Daftari, Haneef, Iwendi, and Jain (2022:1333) "*Phishing is responsible for 90% of data breaches. Approximately 1.5 million new phishing websites are created each month. The average financial cost of a data breach is $3.86 million (IBM), and these figures only cover the year 2019; as the pandemic continued, phishing instances exploded in the following year, 2020"*. Phishing has significant implications on businesses and the harm it causes can include reputational consequences, theft, irreparable financial loss, breaches of privacy, and legal violations that may result in lawsuits.

Organisations and employees can collaborate to increase knowledge and decrease vulnerability. According to Mansfield-Devine (2016:15) *"companies should inform employees of the risks and vulnerabilities and teach situational awareness. Having the entire workforce involved in the process can go a long way towards improving company defences"*. Change can be successfully ensured to produce results across three dimensions: the human, organisational, and technological dimensions. The human component examines the behavioural modifications that must be made in order to inform, guide, and enhance users' digital literacy. On an organisational level, the literature looked at the benefits of changing cybersecurity policies, setting up simulation training, and making sure that system users are sufficiently informed to make wise choices when working online. Regarding the technological component, the literature looked at the most effective methods to use tools like software updates, apps, and other information systems resources to lessen users' susceptibility to phishing attacks. *"The existing body of knowledge on phishing detection can be summed up as follows: Assist users in developing their capacity to identify fake websites. Create*

phishing detection methods for automated phishing website detection or warning. Recent research has focused a lot of attention on and advanced phishing detection methods" (Yang, Zhang, Wang, Li, Li, & He, 2021:1). Blacklisting, content-based, heuristic-based, and fuzzy rule-based phishing detection techniques are all covered in the literature discussed in chapter two.

5.3. Conclusion from primary study

The study adopted a qualitative approach and used semi-structured interviews and ethnography to establish and report on findings in a descriptive manner. The researcher adopted an interpretivist approach, which is a sociological form of research which focuses more on analysing beliefs, cultural settings, individual values to explain a phenomenon. Semi-structured interviews where held with sixteen participants who were respondents for the study. Note taking was done during the session wherein results where consolidated onto a single table. The consolidated responses were used to find patterns, draw insightful conclusions, and then these patterns were refined into succinct themes. Literature from previous studies was used to support the themes that emerged from the data collected. The researcher made sure that concerns about the validity of the results were addressed and observed in the manner in which the data was gathered, examined, and reported. According to Elo, Kääriäinen, Kanste, Pölkki, Utriainen, and Kyngäs (2014:2) in order to establish credibility, researchers must make sure that those taking part in research are accurately identified and described. For this reason, the study thoroughly unpacked the demographic details of the participants and the criterion that was used in the selection process of these participants. The ethical issues were respected and discussed. The accuracy of the data was assured, and ethical standards were upheld.

5.3.1. Conclusions reached in relation to the aim of the study

The research assessed the remedies to user susceptibility to phishing attacks. This aim was accomplished because the study was able to pinpoint the issues related to user susceptibility. Theoretical frameworks were employed to develop better comprehension of user behaviour. In addition, the opinions of academics from earlier studies on phishing and social engineering were used to support and defend the viewpoints expressed in this research. The next step in the data gathering process involved talking to system users in an effort to bridge the gap

between the study's theoretical viewpoint and the facts and experiences of the outside world. The study's recommendations were guided by the data analysis process, which allowed the study to effectively meet its objectives and provide an answer to the research question.

5.3.2. Conclusions on biographical analysis

There were sixteen participants in this research, 12 of whom were female and 4 of whom were males. The interviews were not performed in a single sitting but rather at a time and place that the participants selected, either in-person or virtually. This flexibility allowed participants to participate in the research at a time and place where they felt most comfortable and able to give their full attention. A sizeable percentage (63%) of the individuals held bachelor's degrees and fell into the 25 to 44 age range. Although participants weren't chosen based on their level of education. However, the education factor did play a significant role in ensuring that the information was relayed with a higher level of comprehension. This resulted in the collection of rich data that resulted in highly informative findings. This was very beneficial because it allowed the researcher to obtain rich data. This data was strengthened by examples that participants shared to explain their answers in greater detail and indicated how well they understood the questions raised in the interviews.

5.3.3. Conclusions reached in relation to research objectives

This section summarizes the findings and demonstrates how they met each of the objectives that were defined at the inception of the study.

Objective 1: To establish the solutions that can be put in place to manage the prevalence of phishing attacks

The first objective was drawn from the title of the study. The aim of this objective was to establish solutions that could be adopted to various settings in order to manage the prevalence of phishing attacks. Notably, phishing attacks have significantly increased, making it more crucial than ever to create and implement practical solutions that are SMART, or smart, realistic, attainable, realistic, and time-bound. According to Harvey and Kumar (2020:266) *"anti-phishing solutions are important because one of the top vectors for infection is spear-phishing"*. The first and the second question from Chapter four significantly aided the researcher in achieving this objective. An in-depth understanding of what "is" was required for the research in order to define what "should be". In order to understand the potential

solutions, the researcher needed to gather information about the participant's experiences with cybercrime and how it has affected them in their organisations.

The purpose of the first question was to gauge participants' perceptions of how cybercrimes like phishing had affected their organisations. The participants' responses to this question then revealed three significant themes that arose from the analysis, including the first being that they had noticed a significant increase in phishing attacks in their organisations. Secondly, These attacks were judged to have had financial and operational implications for these organisations. Thirdly, these attacks resulted in instances of client privacy violations or breaches which contravene certain confidentiality regulations.

This sixth question was focused on generating personal recommendations from the participants. The question asked participants to suggest steps other employees could take to protect themselves from other social engineering attacks like phishing. Five themes related to recommendations emerged in the participant replies to this question. One, the participants generally agreed that reporting questionable emails is a must. Two, despite how soon you want to leave and return to your computer, other participants indicated that it is crucial that you act morally and lock your device as a user. Three, some participants emphasized the significance of setting up numerous security applications and other tools that can assist in securing user access. Fourth, participants spoke on the importance of not only attending company-sponsored training but to also engage in self-education to keep informed on social engineering techniques as they have an evolving nature. Fifth, participants finally spoke on the importance of using services like that of password manager to ensure passwords cannot be easily cracked, and to enforce the proper storage of password information. The key issues raised in questions one and six allowed the study to highlight important information and also report on solutions that exist from the views held by the participants.

Objective 2: To determine the extent to which human beings contribute to the success of phishing attacks

The second objective was designed to understand human users and was derived from term "user susceptibility" in the title of the study. The purpose was to investigate the user behavioural flaws that make systems vulnerable to security threats and proliferate the success rate of phishing attacks. Abroshan, Devos, Poels, and Laermans (2021:44930) purport that “the willingness of users’ to take risks in a phishing process impacts how phishable they are. Furthermore, the scholars define phishability as the propensity to fall prey to phishing scams

and become a victim of one". The second objective of the study was addressed using the participants' responses to Questions two and four.

Question two: The second question featured a retrospective question that required participants to consider their experiential knowledge in order to respond. It requested the participant's opinion on the role that insufficient training, carelessness, and malice have played in the effectiveness of phishing attacks against institutions. The first emerging theme emphasized how vulnerability is increased by a lack of training. Second, people frequently disregard the guidelines that organisations have established regarding acceptable behaviour. Thirdly, outdated systems that haven't even been fully upgraded with the right security reinforcements are handled poorly by users.

Question four: This question uncovered detrimental conduct exhibited by internal users that translates into risk. The focus was then on human risk factors, which are the visible inappropriate user behaviours observed in the workplace that increase the likelihood of phishing attacks being effective. Four themes emerged in response to this question. First, participants brought up how their co-workers occasionally handle phishing emails wrongly, passing communications to other users rather than the security team and failing to look out for critical indicators. Second, some users frequently use equipment meant for business usage for personal tasks like internet shopping, streaming, and responding to personal emails. Thirdly, participants observed that when users leave their workstations, they do not lock their machines. Fourth, the issue of password sharing was brought up on multiple occasions as another example of user misconduct. The participants' answers to questions two and four were able to demonstrate their understanding of the role that users play in phishing attacks. The responses from the participants helped in determining how much human beings influence the effectiveness of phishing attacks.

Objective 3: To determine how insufficient technical and organisational security measures expose financial institutions to phishing attacks

The investigation of the controls that financial institutions have in place and their efficacy was the main emphasis of this objective. The purpose of the research objective was to determine how many institutions comprehend cybersecurity and social engineering concepts. Furthermore, looking at how well this comprehension is applied in the workplace. It was clear from the responses to the third question in Chapter four that while organisations do, to a

certain degree, have controls in place, they were not being adequately maintained to maximize the benefit. In some cases, these measures were implemented with a generalized approach, where solutions weren't tailored to particular settings but rather were applied uniformly across all company divisions. For example, the training element. There was no variation in the types of training that the organisation offered, nor any emphasis to the percentage outcome viewed necessary for an employee to obtain to be deemed competent, nor any rule book governing training attendance or nonattendance. Employees should receive unilateral training as needed according to their level of digital savvy and cybersecurity knowledge. Some cybersecurity measures were mentioned by the respondents as being active at their workplace. However, it is important to note that the effectiveness of these measures in preventing or lessening attacks can only be determined by how strictly they are enforced.

The following significant points should be noted as part of the summary from the data analysed regarding the third question from Chapter four:

This question focused on how organisations are set up internally when it comes to security. The question looked at what security measures the organisation had taken to prevent social engineering attacks from compromising internal systems. A variety of themes emerged and these concentrated on the following: 1. Organisations having training and phishing simulations in place. 2. The presence of email monitoring systems designed to contain email threats.3. Firewall and System updates that are designed to strengthen system robustness. 4. Organisations implementing different kinds of cybersecurity policies and having these constantly revised to ensure relevance. 5. The adoption of multi-factor authentication as a form of dual verification for users accessing internal systems and VPN. The outlined measures demonstrate that organisations do have procedures in place, however their efficacy will depend on how strictly they are enforced and how internal users exercise online hygiene.

Objective 4: To establish the interventions financial institutions can put in place to mitigate the risks caused by phishing attacks

This objective centred on the countermeasures financial institutions may employ at work to reduce the risks presented by phishing attacks. This objective looked at measures from the perspective of regular system users, not just institutionally informed measures. Organisations must establish guidelines for how employees interact with different emails and train them to recognise visual cues used by threat actors. These cues are embedded in the emails that users

receive. Emphasis should be placed on the importance of cyber hygiene and ethical behaviour in order to effectively distinguish between ignorant, uneducated, and malicious users.

The fifth question from Chapter four focused on the lessons that the participants' organisations had imparted to them regarding how to avoid falling prey to different types of social engineering, such as phishing. This question was intended to prompt reflection on previously obtained knowledge and to assess the participants' level of comprehension. The responses supplied revealed three themes. Participants first mentioned that they had learned the value of carefully scrutinizing URLs and how they are configured, adhering to emailing rules like authenticating senders, and paying particular attention to indicators that can easily be missed when rushing to respond. Second, the participants mentioned that they had been taught about the significance of training and its role in raising employee awareness. Thirdly, participants also mentioned that they had been taught the value of using work resources ethically and being mindful of their equipment even when they are working on-site in their physical offices.

5.4. Recommendations

The study identified the potential weaknesses that expose organisations, and this section will offer suggestions based on the study's objectives. Furthermore, the following are the actionable steps proposed by the study that can be undertaken to reduce the success rate of social engineering attacks, like phishing:

5.4.1. The implementation of clear reporting lines

Participants and literature converged on the understanding of the importance of escalations. Different workers have different levels of email interpretation or comprehension, so they are likely to have different definitions of what a "suspicious" emails is. Because of this, it is essential for businesses to have specific divisions or personnel in place who can assist staff members and advise them on what is secure and what is not when people are confronted by unfamiliar emails. *Phishing attacks are crafted to look like regular emails, without having unique volume, frequency, or reputation indicators* (Stembert, Padmos, Bargh, Choenni, & Jansen, 2015:113). Threat actors can take advantage of a weakness that arises when users are not sufficiently informed about who to report suspicious or phishing emails to or when a

hierarchical order is not created for this purpose. “The majority of the time, phishing emails that are missed by technological solutions are found as a result of a business employee reporting a suspicious email. Offering a reporting feature should be considered as a potential additional layer in a business's phishing defenses system, primarily because early reports have significant advantages for members of an organisation's incident response team” (Jampen, Gür, Sutter, & Tellenbach, 2020:13). Participants who supported this recommendation spoke about how important they believed it was to have a keen eye for spotting emails and the capacity to handle them effectively by sharing them with the security team. This act helps the designated teams to manage the situation and prevents other users from falling victim to the same email.

5.4.2. Investing in software security applications

Technology is not infallible. However, it plays a very important role in the introducing a layer of security that bridges the gap towards securing processes and in some cases makes up for system weaknesses caused by human users. "To fight email phishing, technological and human-centred strategies are used in parallel. Filtering, firewalls, and blacklists are examples of technologically focused approaches, whereas human-centred approaches typically concentrate on cybersecurity awareness training, frequently on phishing particularly” (Steves, Greene, & Theofanos, 2019:2). Anti-phishing toolbars and multi-factor authentication are recommended for adoption by organisations, as described in the study's findings in Chapter four. Anti-phishing toolbars are a particular kind of browser toolbar made to guard users against phishing. According to Pham, Nguyen, Tran, Huh, and Hong (2018:4) “user computers are protected on the client side by browser toolbars. The browser toolbar will screen URLs from the address bar each time a user accesses a website and then consult a blacklist database. A special warning will be displayed to the viewer if the URL is present in that database”. These toolbars can be integrated onto different search engines. They serve as a form of technical control for phishing defence.

Dasgupta, Roy, Nag, Dasgupta, Roy, and Nag (2017:186) state that,” the purpose of MFA is to authenticate authorized users in order to secure their sensitive data by offering a layered defence and, at the same time, make it more difficult for unauthorized people to obtain access. A robust method of user authentication is one of the advantages of implementing MFA”. Company registered devices should be used to configure these applications to

improve auditability and increase safety, this is a form of mobile device management. Mobile device management, according to Hayes, Cappa, and Le-Khac (2020) is a method of managing or regulating devices through the use of software applications that can implement security protocols, deploy updates automatically, and control what actions are permitted on a device. These precautions are intended to limit level of end user risk, reduce the potential for attacks, and prevent the accidental disclosure of information, including intellectual property.

5.4.3. Investment in education and training

According to Jain and Gupta (2017:1783) *"The main reason behind phishing attacks being successful is the lack of cybersecurity knowledge among the Internet users. Most of the Internet users do not look at the address bar of the website and avoid the security indicator shown by the web browsers".* Participants also agreed with many studies performed by other researchers on the significance of user education and how it can affect the calibre of the choices that users are capable of making. "The awareness of suspicious messages also rises with increased digital literacy. Digitally literate individuals are more likely to recognise phishing emails and can report them more frequently" (Graham & Triplett, 2017:1378). It is important for organisations to ensure that training moves away from being a tick box exercise for employees and becomes a meaningful activity undertaken from a place of understanding than obligation. Employees must invest in their own education and take personal responsibility for learning about social engineering and its effects on the entire organisation. Participants indicated that they found training very important and felt that it could be coupled with a set of additional precautionary steps. Email sender verification is one of these precautions, and it necessitates additional sender validation using any hints from the email to verify an individual before clicking any links or responding to any requests.

5.5. Implications for future research and policy

This study focused on the remedies to reduce user susceptibility to phishing attacks. The findings were tailored to one organisation, from one industry type (financial services). Future study can broaden the scope and examine phishing from the perspective of multiple organisations using a diverse range of other industries, as phishing has grown to be a worldwide phenomenon that affects institutions in all industry types, large and small. Even within the financial services sector, future research can be expanded to include other financial

services pillars. The financial services industry's other pillars—banking, investments, and others—remain unexplored presenting opportunities for future research because this study is primarily concerned with the insurance pillar. Research can also be performed on phishing attacks from the perspective of other industries outside of the financial industry.

5.6. Limitations of the study

A limitation is a shortcoming in the study caused by a variable that was beyond the researcher's control and had the potential to affect the findings and results of the study (Ross & Bibler Zaidi, 2019). There is one limitation in this study that could be addressed in future research, this was the sampling size limitation. In comparison to the population, a small number of individuals were included in the sample. Because of this, it was challenging to draw inferences from and assume that the results from the sample would apply to the population. This made it challenging for the study to extend its findings so that they would still hold true for everyone in the population.. In order for this limitation to have been resolved the study would have had to adopt a mixed method research approach which entails using both qualitative and quantitative research methods which would have enabled a widened sample size. This is the direction that future researchers can undertake to enrich the quality of their findings a improve the level of generalizability. The study's most important aspect was its retrospective review of what went well and its reflection on what might have been done better rather than ignoring it.. It is important for the researcher to acknowledge and take ownership of what can be done better.

5.7. Contributions of the study

The findings of this study will help organisations by increasing awareness on the best ways to improve user astuteness and ability to recognise and respond to attacks in the correct way. This is especially important given the essential role that users play as the human line of defence for organisational systems against phishing attacks. The study's findings will benefit financial institutions by providing practical techniques to limit the success rate of such social engineering attacks. The study investigates the implications of phishing on financial institutions by looking into the complex tactics that threat actors use to infiltrate systems. The study is designed to provide value adding information to financial institutions. This information will help in developing and implementing a practical approach for risk

identification and mitigation for social engineering attacks like phishing. The study found gaps in prior research because human-centred phishing attacks were not adequately investigated. Furthermore, the impact of cognitive biases and visual triggers in influencing susceptibility have not been sufficiently investigated.

In order to lay the groundwork for future research, this study was able to propose approaches that can be improved upon and used as the cornerstones of subsequent investigations. Therefore, the study lays the groundwork for future researchers to explore more solutions to deal with phishing attacks in other critical industries in the economy, as threat actors' strategies continue to evolve and become more sophisticated. Technology alone does not offer sufficient security, particularly because phishers tend to evolve alongside technology and enhance their baiting methods (Vishwanath, Herath, Chen, Wang, & Rao, 2011). The research is able to contribute significantly to the field of Information Systems, particularly in the domain of information security. As a result, it brings about enriched discussions and enhances existing debates on information security and cybersecurity, thereby advancing new knowledge and theoretical perspectives within the broader discipline of Information Systems.

The study's conclusions can be used to support arguments made in academic discussions. People can learn more about what is going on in other organisations when the report is made public. The study will result in findings that embody unconventional solutions that financial institutions can reproduce and easily adopt. This can create teachable moments that other institutions can learn from and put them in a better position to deal with potential threats. This is especially true for businesses in the financial services industry. Financial institutions that apply the basic tenets of cyber hygiene and cybersecurity outlined in this study will be equipped to limit the success rate of phishing attacks. Through extensive research and a rigorous data collection process the study will propose viable and corrective measures that will be impactful to the financial industry. Managers have the opportunity to reexamine their plans and update outdated policies using the study's findings as guidance. Furthermore, they have the power to introduce policies in areas where none presently exist because, in the absence of new regulations, these organisations will continue to expose their information and data assets to risk.

5.8. Conclusion

The study confirmed that susceptibility tends to be influenced by a variety of factors and these range from system vulnerabilities, user flaws and poor adoption of necessary measures from an organisation perspective. However, the human element presents the most challenge as it is comparatively easier for threat actors to try and infiltrate a system using deception as opposed to trying to hack and crack robust systems with layers of security and access controls. This makes it crucial to focus more effort on equipping users to be resistant to the visceral or emotional triggers that phishers thrive on targeting. There are certain behaviours that stem from the users' subconscious mind not being mindful of security when leaving machines not locked or when mishandling work resources. Simulations become necessary in such instances to bring about alertness and introduce remedial training and implications on users who do not comply with expected behaviour. The absence of detailed rules, standards, procedures, and guidelines and guidelines to promote good cybersecurity hygiene leads to poor cyber hygiene in small and medium sized businesses (SMBs).

References

Abdul-Hussein, R.M., Mohammed, A.H. & Kadhim, A.A. 2022. Detecting Phishing Cyber Attack Based on Fuzzy Rules and Differential Evaluation, p.545.

Abroshan, H., Devos, J., Poels, G. & Laermans, E. 2021. A phishing mitigation solution using human behaviour and emotions that influence the success of phishing attacks. *In Adjunct Proceedings of the 29th ACM Conference on User Modeling, Adaptation and Personalization*, pp. 345-350.

Abroshan, H., Devos, J., Poels, G. & Laermans, E. 2021. Phishing happens beyond technology: the effects of human behaviors and demographics on each step of a phishing process. *IEEE Access*, *9*, pp. 44928-44949.

Abt, T.P. 2017. Towards a framework for preventing community violence among youth. *Psychology, health & medicine*, *22*(1), pp. 266-285.

Aburrous, M., Hossain, M.A., Thabatah, F. & Dahal, K. 2008. Intelligent phishing website detection system using fuzzy techniques. In *2008 3rd International Conference on Information and Communication Technologies: From Theory to Applications*, IEEE, pp. 1-6.

Accenture.com. 2020. Insight Into the Cyber Threat Landscape in South Africa | Accenture. [online] Available at: https://www.accenture.com/za-en/insights/security/cyberthreat-south-africa [Accessed 19 March 2022].

Adebowale, M.A., Lwin, K.T. & Hossain, M.A. 2020. Intelligent phishing detection scheme using deep learning algorithms. *Journal of Enterprise Information Management*, p. 2.

Ahmad, S., Kumar, A. & Hafeez, A. 2019. Importance of data integrity & its regulation in pharmaceutical industry. *The Pharma Innovation Journal*, 8(1), pp. 306–313.

Al-Ababneh, M.M. 2020. Linking ontology, epistemology, and research methodology. *Science & Philosophy*, *8*(1), p. 78.

Alabi, O.T., Adeleke, M.A. & Olajide, S.E. 2021. Measuring the influences of opportunity in residential neighbourhood crime. *International Journal of Multidisciplinary Research and Development*, *8*(6), pp. 17-26.

Alase, A. 2017. The interpretative phenomenological analysis (IPA): A guide to a good qualitative research approach. *International Journal of Education and Literacy Studies*, *5*(2), pp. 9-19.

Alavi, M. & Leidner, D. 1999. Knowledge management systems: issues, challenges, and benefits. *Communications of the Association for Information systems*, *1*(1), p. 110.

Alazab, M., Layton, R., Broadhurst, R. & Bouhours, B. 2013. Malicious spam emails developments and authorship attribution. In *2013 fourth cybercrime and trustworthy computing workshop*, IEEE, p. 58.

Aldasoro, I., Frost, J., Gambacorta, L. & Whyte, D. 2020. BIS Bulletin. Available at: https://www.bis.org/publ/bisbull12.pdf [Accessed 04 August 2022].

Aldulaimi, S.H. & Abdeldayem, M.M. 2020. A thematic analysis of leadership behaviours and change management in higher education to boost sustainability. *International Journal of Higher Education and Sustainability*, *3*(1), pp. 34-51.

Alghamdi, H. 2017. Can phishing education enable users to recognise phishing attacks. *Dublin Institute of Technology Arrow at DIT*, pp. 15-16.

Al-Hussain, Z. & Al-Shaikh, R. 2015. Disaster Recovery Drills Considerations: From Planning to Automation. *Academia.edu*, IEEE, p. 189.

Allemang, B., Sitter, K. & Dimitropoulos, G. 2022. Pragmatism as a paradigm for patient-oriented research. *Health Expectations*, *25*(1), pp. 38-47.

Alohali, M., Clarke, N., Li, F. & Furnell, S. 2018. Identifying and predicting the factors affecting end-users' risk-taking behavior. *Information & Computer Security*, p. 8.

AL-Otaibi, A.F. & Alsuwat, E.S. 2020. A study on social engineering attacks: Phishing attack. *Int. J. Recent Adv. Multidiscip. Res*, *7*(11), p. 6378.

Alsariera, Y.A., Adeyemo, V.E., Balogun, A.O. & Alazzawi, A.K. 2020. Ai meta-learners and extra-trees algorithm for the detection of phishing websites. *IEEE access*, *8*, pp. 142532-142542.

Alturki, R. 2021. Research onion for smart IoT-enabled mobile applications. *Scientific Programming*, *2021*, p. 6.

Al-Zefeiti, S.M.B. & Mohammad, N.A. 2015. Methodological considerations in studying transformational leadership and its outcomes. *International Journal of Engineering Business Management*, *7*, p. 2.

Alzubaidi, A. 2021. Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon*, *7*(1), p. 10.

Anand, S., Susila, N. & Balakrishnan, S. 2018. Challenges and Issues in Ensuring Safe Cloud Based Password Management to Enhance Security". *International Journal of Pure and Applied Mathematics*, *119*(12), pp. 1207-1215.

Anawar, S., Kunasegaran, D.L., Mas'ud, M.Z. & Zakaria, N.A. 2019. Analysis of phishing susceptibility in a workplace: a big-five personality perspectives. *J Eng Sci Technol*, *14*(5), pp. 2865-2882.

Anawar, S., Kunasegaran, D.L., Mas'ud, M.Z. & Zakaria, N.A. 2019. Analysis of phishing susceptibility in a workplace: a big-five personality perspectives. *Journal of Engineering Science and Technology*, 14(5), pp. 2865-2882.

Andrade, R.O., Ortiz-Garcés, I. & Cazares, M. 2020. Cybersecurity attacks on Smart Home during Covid-19 pandemic. *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, pp. 398-404.

Annansingh, F. 2021. Bring your own device to work: How serious is the risk? *Journal of Business Strategy*, *42*(6), pp. 392-398.

Ansari, M.F., Sharma, P.K. & Dash, B. 2022. Prevention of phishing attacks using AI-based Cybersecurity Awareness Training. *Prevention*, p. 67.

Antwi, S.K., & Hamza, K. 2015. Qualitative and quantitative research paradigms in business research: A philosophical reflection. *European journal of business and management*, *7*(3), pp. 217-225.

Apandi, S.H., Sallim, J. & Sidek, R.M. 2020. February. Types of anti-phishing solutions for phishing attack. In *IOP Conference Series: Materials Science and Engineering*, IOP Publishing, 769(1), p. 012072.

Applegate, S.D. 2009. Social engineering: hacking the wetware!. *Information Security Journal: A Global Perspective*, *18*(1), pp. 40-46.

Arai, M. 2015. Development and Evaluation of Secure Socket Layer Visualization Tool with Packet Capturing Function. In *MATEC Web of Conferences*, EDP Sciences, 28, pp. 1-4.

Aspers, P. & Corte, U. 2019. What is qualitative in qualitative research. *Qualitative sociology, 42*, pp. 139-160.

Athulya, A.A. & Praveen, K. 2020. Towards the detection of phishing attacks. *In 2020 4th international conference on trends in electronics and informatics (ICOEI) (48184)*, IEEE, Tirunelveli, India, pp. 337-343.

Atmowardoyo, H. 2018. Research methods in TEFL studies: Descriptive research, case study, error analysis, and R & D. *Journal of Language Teaching and Research*, *9*(1), pp. 197-204.

Aycock, J. 2007. A design for an anti-spear-phishing system. *Proceedings of the 7th Virus Bulletin International Conference, Vienna, Austria*, pp. 290-293.

Bakhshi, T. 2017. Social engineering: revisiting end-user awareness and susceptibility to classic attack vectors, In *2017 13th International Conference on Emerging Technologies*, Islamabad, Pakistan, IEEE, pp. 1-6.

Barrett, D. & Twycross, A. 2018. Data collection in qualitative research. *Evidence-Based Nursing*, *21*(3), pp. 63-64.

Bashir, T., Agbata, B.C. & Emmanuel Ogala, W.O.D. 2020. The Fuzzy Experiment Approach for Detection and Prevention of Phishing attacks in online Domain, *East African Scholars Journal of Engineering and Computer Sciences*, pp. 205 – 215.

Basias, N. & Pollalis, Y. 2018. Quantitative and qualitative research in business & technology: Justifying a suitable research methodology. *Review of Integrative Business and Economics Research, 7*, pp. 91-105.

Basit, A., Zafar, M., Javed, A.R. & Jalil, Z. 2020. A novel ensemble machine learning method to detect phishing attack. *2020 IEEE 23rd International Multitopic Conference (INMIC)*, Bahawalpur, Pakistan, pp. 1-5.

Baykara, M. & Gürel, Z.Z. 2018. Detection of phishing attacks. In *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, IEEE, pp. 1-5.

Beck, C.T. 1993. Qualitative research: The evaluation of its credibility, fittingness, and auditability. *Western journal of nursing research*, *15*(2), pp. 263-266.

Beguin, E., Besnard, S., Cros, A., Joannes, B., Leclerc-Istria, O., Noel, A., Roels, N., Taleb, F., Thongphan, J., Alata, E. & Nicomette, V. 2019. Computer-security-oriented escape room. *IEEE Security & Privacy*, *17*(4), p. 82.

Best, S. 2014. Understanding and doing successful research: Data collection and analysis for the social sciences. *Routledge Taylor & Francis Group*, p. 5.

Bhagwat, M.D., Patil, P.H. & Vishawanath, T.S. 2021. A Methodical Overview on Detection, Identification and Proactive Prevention of Phishing Websites. In *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, IEEE, p. 1505.

Bhavsar, V., Kadlak, A. & Sharma, S. 2018. Study on phishing attacks. *International Journal of Computer Applications*, 182(33), pp. 27-29.

Bilge, L. & Dumitras, T. 2012. An empirical study of zeroday attacks in the real world. *Proceedings of the 2012 ACM conference on Computer and communications security*, pp. 16-18.

Blythe, J.M., Gray, A. & Collins, E. 2020. Human cyber risk management by security awareness professionals: Carrots or sticks to drive behaviour change?. In *HCI for Cybersecurity, Privacy and Trust: Second International Conference, HCI-CPT 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark*, p. 120.

Bojinov, H., Bursztein, E., Boyen, X. & Boneh, D. 2010. Kamouflage: Loss-resistant password management. In *Computer Security–ESORICS 2010: 15th European Symposium on Research in Computer Security, Athens, Greece*. Springer, pp. 286-302.

Bolin, G. & Skogerbø, E. 2013. Age, generation, and the media. *Northern Lights: Film & Media Studies Yearbook*, *11*(1), pp. 3-14.

Borkovich, D.J. & Skovira, R.J. 2020. Working from home: Cybersecurity in the age of COVID-19. *Issues in Information Systems*, 21(4), pp. 234-246.

Boslaugh, S. 2007. An introduction to secondary data analysis. *Secondary data sources for public health: A practical guide*, pp. 2-10.

Boyatzis, R.E. 1998. Transforming qualitative information: Thematic analysis and code development. *Sage*, p. 4.

Bradshaw, C., Atkinson, S. & Doody, O. 2017. Employing a qualitative description approach in health care research. *Global qualitative nursing research, 4(1-8)*, p. 4.

Braun, V. & Clarke, V. 2006. Using thematic analysis in psychology. Qualitative Research in Psychology, *ISSN*, 3 (2), pp. 77-101.

Braun, V. & Clarke, V. 2021. One size fits all? What counts as quality practice in (reflexive) thematic analysis? *Qualitative research in psychology*, *18*(3), 328-352.

Buil-Gil, D., Lord, N. & Barrett, E. 2021. The dynamics of business, cybersecurity, and cyber-victimization: Foregrounding the internal guardian in prevention. *Victims & Offenders*, *16*(3), pp. 286-315.

Burke, S. 2021. How to prepare for the onslaught of phishing email attacks. *Computer Fraud & Security*, 2021(5), pp. 12-14.

Buys, M. 2017. Protecting personal information: Implications of the Protection of Personal Information (POPI) Act for healthcare professionals. *South African Medical Journal*, 107(11), pp. 954-956.

Byrne, D. 2022. A worked example of Braun and Clarke's approach to reflexive thematic analysis. *Quality & quantity*, *56*(3), pp. 1391-1412.

Camillo, M. (2017). Cyber risk and the changing role of insurance. *Journal of Cyber Policy*, *2*(1), 53-63.

Campedelli, G.M., Aziani, A. & Favarin, S. (2021). Exploring the immediate effects of COVID-19 containment policies on crime: An empirical analysis of the short-term aftermath in Los Angeles. *American Journal of Criminal Justice*, *46*(5), 704-727.

Chaudhry, J.A. & Rittenhouse, R.G. 2015. Phishing: Classification and countermeasures. In *2015 7th International Conference on Multimedia, Computer Graphics and Broadcasting (MulGraB)*, *IEEE*, pp. 28-31.

Chaudhry, J.A., Chaudhry, S.A. & Rittenhouse, R.G. 2016. Phishing attacks and defenses. *International Journal of Security and Its Applications*, 10(1), pp. 247-256.

Cheng, E.C. & Wang, T. 2022. Institutional strategies for cybersecurity in higher education institutions. *Information*, *13*(4), p. 192.

ChePa, N., Jnr, B.A., Nor, R.N.H. & Murad, M.A.A. 2015. A review on risk mitigation of IT governance. *Information Technology Journal*, *14*(1), p. 1.

Chigada, J. & Madzinga, R. 2021. Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management,* 23(1), pp. 1-11.

Cho, J.Y. & Lee, E.H. 2014. Reducing confusion about grounded theory and qualitative content analysis: Similarities and differences. *Qualitative report, 19*(32), p. 10.

Clarke, R.V. & Newman, G.R. 2005. Modifying Criminogenic Products-What Role for Government? *Crime prevention studies, 18*, p. 7.

Clarke, V. & Braun, V. 2013. Teaching thematic analysis: Overcoming challenges and developing strategies for effective learning. *The psychologist, 26*(2), p. 3.

Clarke, V., Braun, V. & Hayfield, N. 2015. Thematic analysis. *Qualitative psychology: A practical guide to research methods*, *222*(2015), pp. 225-226

Cohen, L. E. & Felson, M. 1979. Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), pp. 588–608.

Conteh, N.Y. & Schmick, P.J. 2016. Cybersecurity: risks, vulnerabilities, and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, *6*(23), p. 34.

Creswell, J. W. 2014. Research Design: Qualitative, Quantitative and Mixed Methods Approaches (4th ed.). *Sage publications,* pp. 107-215.

Creswell, J.W. & Poth, C.N. 2016. Qualitative inquiry and research design: Choosing among five approaches. *Sage publications*, p. 327.

Daengsi, T., Pornpongtechavanich, P. & Wuttidittachotti, P. 2021. Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks. *Education and Information Technologies*, 27(4), pp. 1-24.

Daniel, B.K. 2019. What constitutes a good qualitative research study? Fundamental dimensions and indicators of rigour in qualitative research: The TACT framework. In *Proceedings of the European conference of research methods for business & management studies*, Dunedin, New Zealand, pp. 101-108.

Dasgupta, D., Roy, A., Nag, A., Dasgupta, D., Roy, A. & Nag, A. 2017. Multi-Factor Authentication: More secure approach towards authenticating individuals. *Advances in User Authentication*, pp. 185-233.

De Bona, M. & Paci, F. 2020. A real world study on employees' susceptibility to phishing attacks. *Proceedings of the 15th International Conference on Availability, Reliability and Security*, pp. 1-10.

De Vaus, D. 2016. What is a survey. *Research Methods for Postgraduates*, *5*(3), pp. 202-211.

DeCarlo, M. 2018. 7.3 Unit of analysis and unit of observation. *Scientific Inquiry in Social Work*.

DeJonckheere, M. & Vaughn, L.M. 2019. Semi structured interviewing in primary care research: a balance of relationship and rigour. *Family medicine and community health*, *7*(2), p. 12.

Desolda, G., Ferro, L.S., Marrella, A., Catarci, T. & Costabile, M.F. 2021. Human Factors in Phishing Attacks: A Systematic Literature Review. *ACM Computing Surveys (CSUR)*, 54(8), pp. 1-35.

Dewis, M. & Viana, T. 2022. Phish Responder: A Hybrid Machine Learning Approach to Detect Phishing and Spam Emails. *Applied System Innovation*, *5*(4), p. 73.

Don-Solomon, A. & Eke, G.J. 2018. Ontological & epistemological philosophies underlying theory building: A scholarly dilemma or axiomatic illumination-The business research perspective. *European Journal of Business and Innovation Research*, *6*(2), p. 2.

Dou, Z., Khalil, I., Khreishah, A., Al-Fuqaha, A. & Guizani, M. 2017. Systematization of knowledge (sok): A systematic review of software-based web phishing detection. *IEEE Communications Surveys & Tutorials*, 19(4), pp. 2797-2819.

Downs, J.S., Holbrook, M.B. & Cranor, L.F. 2006. Decision strategies and susceptibility to phishing. In *Proceedings of the second symposium on Usable privacy and security*, p. 79.

Draugalis, J.R., Coons, S.J. & Plaza, C.M. 2008. Best practices for survey research reports: a synopsis for authors and reviewers. *American journal of pharmaceutical education*, *72*(1), p. 4.

Duman, S., Kalkan-Cakmakci, K., Egele, M., Robertson, W. & Kirda, E. 2016. Email profiler: Spear phishing filtering with header and stylometric features of emails. In *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, 1, pp. 408-416.

Dyussenbayev, A. 2017. Age periods of human life. *Advances in Social Sciences Research Journal*, *4*(6), pp. 1 – 6.

Eian, I.C., Yong, L.K., Li, M.Y.X., Qi, Y.H. & Fatima, Z. 2020. Cyber-attacks in the era of covid-19 and possible solution domains, *Preprints*, pp. 1-15.

Eisenhart, M. 1991. Conceptual frameworks for research circa 1991: Ideas from a cultural anthropologist; implications for mathematics education researchers. *Proceedings of the Thirteenth Annual Meeting*, Blacksburg, Virginia, U.S.A, p. 205.

El-Gohary, H.O. 2010. The impact of E-marketing practices on market performance of small business enterprises. An empirical investigation. Doctoral dissertation, *University of Bradford*, p. 24.

Elmisery, A.M. & Sertovic, M. 2021. Modular Platform for Detecting and Classifying Phishing Websites Using Cyber Threat Intelligence. *Electronic Communications of the EASST*, p. 80.

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K. & Kyngäs, H. 2014. Qualitative content analysis: A focus on trustworthiness. *SAGE open*, *4*(1), p. 2.

Ertan, A., Crossland, G., Heath, C., Denny, D. & Jensen, R. 2020. Cyber security behaviour in organisations. *arXiv preprint arXiv:2004.11768*, p. 10.

Etikan, I., Musa, S.A. & Alkassim, R.S. 2016. Comparison of convenience sampling and purposive sampling. *American journal of theoretical and applied statistics*, *5*(1), pp. 1-4.

Farrell, G. 2015. Crime concentration theory. *Crime prevention and community Safety*, *17*(4), pp. 233 - 235.

Feldman, M.S. & March, J.G. 1981. Information in organisations as signal and symbol. *Administrative science quarterly*, pp. 171-186.

Felson, M. 1987. Routine activities and crime prevention in the developing metropolis. *Criminology*, *25*(4), pp. 911-932.

Felson, M. & Clarke, R.V. 1998. Opportunity makes the thief. *Police research series, paper*, *98*(1-36), pp. 10.

Feroz, M.N. & Mengel, S. 2015. Phishing URL detection using URL ranking. In *2015 ieee international congress on big data*, IEEE, pp. 635-638.

Florêncio, D. & Herley, C. 2006. Analysis and improvement of anti-phishing schemes. In *IFIP International Information Security Conference*, pp. 148-157.

Fourches, D., Muratov, E. & Tropsha, A. 2010. Trust, but verify: on the importance of chemical structure curation in cheminformatics and QSAR modeling research. *Journal of chemical information and modeling*, 50(7), p. 1189.

Frauenstein, E.D. & von Solms, R. 2009. Phishing: How an Organization can Protect Itself. *Proceedings of the Information Security South Africa 2009 Conference*, pp. 53-268.

Gentles, S.J., Charles, C., Ploeg, J. & McKibbon, K.A. 2015. Sampling in qualitative research: Insights from an overview of the methods literature. *The qualitative report*, *20*(11), pp. 1772-1789.

Ghasemi, M., Saadaat, M. & Ghollasi, O. 2019. Threats of social engineering attacks against security of Internet of Things (IoT). *Fundamental research in electrical engineering*, pp. 957-968.

Ghazi-Tehrani, A.K. & Pontell, H.N. 2021. Phishing evolves: Analyzing the enduring cybercrime. *Victims & Offenders*, 16(3), pp. 316-342.

Ghourabi, A. 2021. SM-Detector: A security model based on BERT to detect Smishing messages in mobile environments. *Concurrency and Computation: Practice and Experience*, 33(24), p. e6452.

Gill, P., Stewart, K., Treasure, E. & Chadwick, B. 2008. Methods of data collection in qualitative research: interviews and focus groups. *British dental journal*, *204*(6), pp. 291-295.

González Campos, H. 2021. *A study of phishing emails and their ability to mislead recipients depending on age and education level* (Doctoral dissertation, Universitat Politècnica de València), pp. 1-34.

Gopavaram, S., Dev, J., Grobler, M., Kim, D., Das, S. & Camp, L.J. 2021. Cross-national study on phishing resilience. In *Proceedings of the Workshop on Usable Security and Privacy (USEC)*, pp. 1-11.

Gordon, W.J., Wright, A., Aiyagari, R., Corbo, L., Glynn, R.J., Kadakia, J., Kufahl, J., Mazzone, C., Noga, J., Parkulo, M. & Sanford, B. 2019. Assessment of employee susceptibility to phishing attacks at US health care institutions. *JAMA network open*, *2*(3), p. 2.

Grabosky, P. 2001. "Virtual Criminality: Old Wine in New Bottles?" *Social and Legal Studies* 10(2), p. 248.

Grady, M.P. 1998. *Qualitative and action research: A practitioner handbook*. Phi Delta Kappa International, p. 43.

Graham, R. & Triplett, R. 2017. Capable guardians in the digital environment: The role of digital literacy in reducing phishing victimization. *Deviant Behavior, 38*(12), pp. 1371-1382.

Graue, C. 2015. Qualitative data analysis. *International Journal of Sales, Retailing & Marketing*, *4*(9), p. 8.

Green, J.S. & Dorey, P. 2016. The weakest link: why your employees might be your biggest cyber risk. *Bloomsbury Publishing*, pp. 1-28.

Greitzer, F.L., Li, W., Laskey, K.B., Lee, J. & Purl, J. (2021). Experimental investigation of technical and human factors related to phishing susceptibility. *ACM Transactions on Social Computing*, *4*(2), pp. 1-48.

Griffin, S. E. & Rackley, C. C. 2008. Vishing. *In Proceedings of the 5th annual conference on information security curriculum development*, pp. 33–35.

Grix, J. 2002. Introducing students to the generic terminology of social research. *Politics, 22*(3), p. 177.

Groff, E.R. 2007. Simulation for theory testing and experimentation: An example using routine activity theory and street robbery. Journal of Quantitative Criminology, 23(2), pp. 75-103.

Grosse, E. & Upadhyay, M. (2013). Authentication at Scale. *IEEE Security & Privacy, 11(1),* p. 16.

Gubrium, J.F., Holstein, J.A., Marvasti, A.B. & McKinney, K.D. (2012). The SAGE handbook of interview research: The complexity of the craft. *Sage Publications*, p. 347.

Gudeva, L.K., Dimova, V., Daskalovska, N. & Trajkova, F. 2012. Designing descriptors of learning outcomes for Higher Education qualification. *Procedia-Social and Behavioral Sciences, 46*, pp. 1306-1311.

Hadjidj, R., Debbabi, M., Lounis, H., Iqbal, F., Szporer, A. & Benredjem, D. 2009. Towards an integrated e-mail forensic analysis framework. *digital investigation, 5*(3-4), pp. 124-137.

Hamberg, K. 2008. Gender bias in medicine. *Women's health*, *4*(3), pp. 237-243.

Haney, J. & Lutters, W. 2020. Security awareness training for the workforce: moving beyond "check-the-box" compliance. *Computer*, *53*(10), pp. 91-95.

Hanna, K., Ferguson, K. & Beaver, K. 2021. *What is a data breach?*. Available at: https://www.techtarget.com/searchsecurity/definition/data-breach [Accessed 05 August 2022].

Hansson, S.O. 2007. Philosophical problems in cost–benefit analysis. *Economics & Philosophy*, *23*(2), p. 163.

Harrison, B., Vishwanath, A. & Rao, R. 2016. A user-centred approach to phishing susceptibility: The role of a suspicious personality in protecting against phishing. In *2016 49th Hawaii international conference on system sciences (HICSS)*. IEEE, pp. 5628-5634.

Harvey, J. & Kumar, S. 2020. A survey of intelligent transportation systems security: challenges and solutions. In *2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, pp. 263-268.

Hassandoust, F., Singh, H. & Williams, J. 2019. How contextualisation affects the vulnerability of individuals to phishing attempts, *Association for Information Systems Electronic Library*, pp. 1-15.

Hassandoust, F., Singh, H. & Williams, J. 2020. The role of contextualization in individuals' vulnerability to phishing attempts. *Australasian Journal of Information Systems*, *24*, p. 8.

Hayes, D., Cappa, F. & Le-Khac, N.A. 2020. An effective approach to mobile device management: Security and privacy issues associated with mobile applications. *Digital Business*, *1*(1), pp. 1-8.

Hellström, T. 2008. Transferability and naturalistic generalization: new generalizability concepts for social science or old wine in new bottles? *Quality & Quantity*, *42*(3), pp. 321-337.

Herbig, F.J. & Warchol, G. 2011. South African conservation crime and routine activities theory: a causal nexus?. *Acta Criminologica: African Journal of Criminology & Victimology*, *24*(2), p. 5.

Hicks, A. 2018. *Angler Phishing: What is it?*. Available at: https://www.clearviewfcu.org/Learn/about-financial-wellness/Blog/Angler-Phishing-What-is-it#:~:text=Angler%20phishing%20is%20a%20new,personal%20information%20or%20account%20credentials [Accessed 05 August 2022].

Hindmoor, A. & Taylor, B. 2017. Rational choice. *Bloomsbury Publishing*, p. 216.

Hinson, G. 2008. Social engineering techniques, risks, and controls. *EDPAC: The EDP Audit, Control, and Security Newsletter*, *37*(4-5), pp. 32-46.

Hirschfield, A., Johnson, S.D. & Bowers, K.J. 2001. Review of major policy developments and evidence base: crime domain. *University of Huddersfield*, p. 6.

Holden, M.T. & Lynch, P. 2004. Choosing the appropriate methodology: Understanding research philosophy. *The marketing review*, *4*(4), pp. 397-409.

Holtom, B., Baruch, Y., Aguinis, H. & A Ballinger, G. 2022. Survey response rates: Trends and a validity assessment framework. *human relations*, *75*(8), p. 1561.

Hong, J. 2012. The state of phishing attacks. *Communications of the ACM*, 55(1), 76.

Horgan, S., Collier, B., Jones, R. & Shepherd, L. 2021. Re-territorialising the policing of cybercrime in the post-COVID-19 era: towards a new vision of local democratic cyber policing. *Journal of Criminal Psychology*, 11(3), pp. 222-239.

Hossain, A.S.M. 2015. Implementation considerations of IPsec VPN for small and medium-sized companies, Bachelor's thesis, Turku University of Applied Sciences, Turku, p. 8.

House, D. & Raja, M.K. 2020. Phishing: message appraisal and the exploration of fear and self-confidence. Behaviour & Information Technology, 39(11), pp. 1204-1224.

House, E.R. 1991. Realism in research. *Sage Publication*, *20*(6), p. 3.

Howell, C.J., Burruss, G.W., Maimon, D. & Sahani, S. 2019. Website defacement and routine activities: Considering the importance of hackers' valuations of potential targets. *Journal of Crime and Justice*, *42*(5), pp. 536-550.

Hrdý, M. & Pláničková, M. 2019. Meaning and problems of identification of beta coefficient when valuing financial institutions. *Prague Economic Papers*, *2019*(4), pp. 479-495.

Hu, L. 2022. Fake Websites Used in COVID-19 Themed Phishing Attacks, Impersonating Brands Like Pfizer and BioNTech. [online] Available at: https://unit42.paloaltonetworks.com/covid-19-themed-phishing-attacks/ [Accessed 7 April 2022].

Huitt, W. 2012. A systems approach to the study of human behavior. *Educational Psychology Interactive*.

Ibrahimovic, S. & Franke, U. 2017. A probabilistic approach to IT risk management in the Basel regulatory framework: A case study. *Journal of Financial Regulation and Compliance*, p. 178.

Iovino, F. & Tsitsianis, N. 2020. The methodology of the research. In *Changes in European energy markets*. *Emerald Publishing Limited*, p. 93.

Iser, B. & Brandtweiner, R. 2022. Role of awareness to prevent personal disasters: reducing the risks of falling for phishing by strengthening user awareness. *WIT Transactions on The Built Environment*, *207*, pp. 79-88.

Iuga, C., Nurse, J.R. & Erola, A. 2016. Baiting the hook: factors impacting susceptibility to phishing attacks. *Human-centric Computing and Information Sciences*, *6*, 1-20.

Jain, A.K. & Gupta, B.B. 2017. Two-level authentication approach to protect from phishing attacks in real time. *Journal of Ambient Intelligence and Humanized Computing*, *9*, pp. 1783-1796.

Jain, A.K. & Gupta, B.B. 2021. A survey of phishing attack techniques, defence mechanisms and open research challenges. *Enterprise Information Systems*, pp. 1-39.

Jain, A.K. & Gupta, B.B. 2022. A survey of phishing attack techniques, defence mechanisms and open research challenges. *Enterprise Information Systems*, *16*(4), pp. 527-565.

Jampen, D., Gür, G., Sutter, T. & Tellenbach, B. 2020. Don't click: towards an effective anti-phishing training. A comparative literature review. *Human-centric Computing and Information Sciences*, *10*(1), pp. 1-41.

Jamshed, S. 2014. Qualitative research method-interviewing and observation. *Journal of basic and clinical pharmacy*, *5*(4), p. 87.

Jansen, J. & Leukfeldt, R. 2016. Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, *10*(1), p. 79.

Järvi, H., Kähkönen, A.K. & Torvinen, H. 2018. When value co-creation fails: Reasons that lead to value co-destruction. *Scandinavian Journal of Management*, *34*(1), pp. 63-77.

Javadi, M. & Zarea, K. 2016. Understanding thematic analysis and its pitfall. *Journal of client care*, *1*(1), pp. 33-39.

Jayatilaka, A., Beu, N., Baetu, I., Zahedi, M., Babar, M.A., Hartley, L. & Lewinsmith, W. 2021. Evaluation of Security Training and Awareness Programs: Review of Current Practices and Guideline. *arXiv preprint arXiv:2112.06356*, pp. 1-12.

Jensen, M.L., Dinger, M., Wright, R.T. & Thatcher, J.B. 2017. Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, *34*(2), pp. 597-626.

Jensen, M.L., Dinger, M., Wright, R.T. & Thatcher, J.B. 2017. Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, *34*(2), pp. 597-626.

Jin-Feng, W., Ming-Yan, C., Li-Jie, F. & Jun-Ju, Y. 2017. The construction of enterprise tacit knowledge sharing stimulation system oriented to employee individual. *Procedia engineering*, *174*, pp. 289-300.

Jones, H.S. & Moncur, W. 2020. A mixed-methods approach to understanding funder trust and due diligence processes in online crowdfunding investment. *ACM Transactions on Social Computing*, *3*(1), pp. 1-29.

Jore, S.H. 2019. The conceptual and scientific demarcation of security in contrast to safety. *European Journal for Security Research*, *4*, pp. 157-174.

Jorrigala, V. 2017. Business continuity and disaster recovery plan for information security, p. 18.

Jubaer, S.M.O.F. & Hassan, M.N. 2021. The routine activities and rational choice theory: A criminologist reflection. *European Scholar Journal*. 2(7), pp. 19-29.

Kalaharsha, P. & Mehtre, B.M. 2021. Detecting Phishing Sites--An Overview. *arXiv preprint arXiv:2103.12739*, pp. 1-13.

Kannan, M.J. 2017. March. A bird's eye view of Cyber Crimes and Free and Open Source Software's to Detoxify Cyber Crime Attacks-an End User Perspective. In *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*. IEEE, pp. 236.

Kao, D.Y., Kluaypa, B. & Lin, H.C. 2017. The cyberbullying assessment of capable guardianship in routine activity theory. In *Pacific-Asia Workshop on Intelligence and Security Informatics*. Springer, pp. 3-14.

Karapanos, N., Marforio, C., Soriente, C. & Capkun, S. 2015. Sound-proof: Usable two-factor authentication based on ambient sound. *In the Proceedings of the 24th USENIX Security Symposium*, Washington D.C, p. 485.

Keen, S., Lomeli-Rodriguez, M. & Joffe, H. 2022. From challenge to opportunity: virtual qualitative research during COVID-19 and beyond. *International journal of qualitative methods*, *21*, pp. 1-11.

Khan, N.A., Brohi, S.N. & Zaman, N. 2020. Ten deadly cyber security threats amid COVID-19 pandemic, *IEEE*, pp. 1-6.

Khaskheli, G.M., Sherbaz, M. & Shaikh, U.R. 2022. A comparative usability study of single-factor and two-factor authentication. *Tropical Scientific Journal*, *1*(1), pp. 17-27.

Khawandi, S., Abdallah, F. & Ismail, A. 2019. A Survey on the Existing Lock Methods. In *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing*, IEEE, pp. 232-236.

Kim, B., Lee, D.Y. & Kim, B. 2020. Deterrent effects of punishment and training on insider security threats: a field experiment on phishing attacks. *Behaviour & Information Technology*, *39*(11), pp. 1156-1175.

Kim, J.Y., Bu, S.J. & Cho, S.B. 2018. Zero-day malware detection using transferred generative adversarial networks based on deep autoencoders. *Information Sciences*, *460*, pp. 83-102.

Kitten, T. 2013. *Spear-Phishing: What Banks Must Do*. [online] Bankinfosecurity.com. Available at: https://www.bankinfosecurity.com/thwarting-spear-phishing-long-way-to-go-a-5923#:~:text=In%20the%20financial%20services%20sector,a%20gateway%20to%20draining%20accounts [Accessed 9 April 2022].

Kohfeldt, D. & Grabe, S. 2014. Universalism. *Encyclopedia of Critical Psychology. New York, NY: Springer*, p. 2036.

Korstjens, I. & Moser, A. 2017. Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice*, *24*(1), pp. 120-124.

Kothari, C.R. 2004. Research methodology: Methods and techniques. *New Age International*, p. 8.

Kovatcheva, E., Consoli, A. & Yordanov, A. (2021). Training the employees to meet phishing attacks. *14th Annual International Conference of Education*. IATED, pp. 7164-7168.

Krithika, N. 2017. A study on wha (watering hole attack)–the most dangerous threat to the organisation. *International Journal of Innovations in Scientific and Engineering Research*, *4*(8), pp. 196-198.

Kulatunga, K.J., Amaratunga, D. & Haigh, R. 2007. Researching construction client and innovation: methodological perspective, p. 484.

Labra, O., Castro, C., Wright, R. & Chamblas, I. 2020. Thematic analysis in social work: A case study. *Global Social Work-Cutting Edge Issues and Critical Reflections*, *10*(6), pp. 1-20.

Lahcen, R.A.M., Caulkins, B., Mohapatra, R. & Kumar, M. (2020). Review and insight on the behavioural aspects of cybersecurity. *Cybersecurity*, *3*(1), pp. 1-18.

Lala, D.M. 2015. *An investigation into the prevalence and growth of phishing attacks against South African financial targets*. Doctoral dissertation, Rhodes University, 20 Available at:

https://commons.ru.ac.za/vital/access/services/Download/vital:20379/SOURCE1?view=true [Accessed 05 August 2022].

Lamas, D., Loizides, F., Nacke, L., Petrie, H., Winckler, M. & Zaphiris, P. 2019. Human-Computer Interaction–Interact-2019. *17th IFIP TC 13 International Conference, Paphos, Cyprus, Proceedings, Part III*, Springer Nature, 11748, p. 600.

Lee, M. & Park, E. 2021. Real-time Korean voice phishing detection based on machine learning approaches. *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-12.

Leukfeldt, E.R. 2014. Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking*, *17*(8), pp. 551-555.

Leukfeldt, E.R. & Yar, M. 2016. Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Taylor & Francis Group*, *37*(3), pp. 263-280.

Lichtfuss, J., Lee, F. & Berryman, T. 2021. The Classification of Phishing Websites using Supervised Data Mining Techniques, *AIS Electronic Library*, p. 2.

Lietz, C.A., Langer, C.L. & Furman, R. 2006. Establishing trustworthiness in qualitative research in social work: Implications from a study regarding spirituality. *Qualitative social work*, *5*(4), pp. 441-458.

Lincoln, Y.S. & Guba, E.G. 1986. But is it rigorous? Trustworthiness and authenticity in naturalistic evaluation. *New directions for program evaluation*, *1986*(30), pp. 73-84.

Lowe, N.K. 2019. What is a pilot study?. *Journal of Obstetric, Gynaecologic & Neonatal Nursing*, *48*(2), pp. 117-118.

Madensen, T.D. 2016. Opportunities for white-collar crime. The Oxford handbook of white-collar crime, p. 384.

Madero-Hernandez, A. & Fisher, B.S. 2012. Routine activity theory, pp. 1-26.

Ma, J., Saul, L.K., Savage, S. & Voelker, G.M. 2009. Beyond blacklists: learning to detect malicious web sites from suspicious URLs. *In Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining*, pp. 1245-1254.

Majeed, I. 2019. Understanding positivism in social research: A research paradigm of inductive logic of inquiry. *International Journal of Research in Social Sciences*, *9*(11), p. 120.

Malalgoda, C., Amaratunga, D. & Haigh, R. 2018. Empowering local governments in making cities resilient to disasters: research methodological perspectives. *Procedia engineering*, *212*, p. 905

Malisa, L. 2017. *Security of User Interfaces: Attacks and Countermeasures*. Doctoral dissertation, ETH Zurich, p. 14.

Mansfield-Devine, S. 2016. Ransomware: taking businesses hostage. *Network Security*, *2016*(10), pp. 8-17.

Mardiana, S. 2020. Modifying Research Onion for Information Systems Research. *Solid State Technology*, *63*(4), pp. 5304-5313.

Mas.gov.sg. 2021. [online] Available at: https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Monographs-and-Information-Papers/Risk-Management-and-Operational-Resilience-in-a-Remote-Working-Environment.pdf [Accessed 11 March 2022].

Masadeh, M. 2012. Training, education, development, and learning: what is the difference?. *European scientific journal*, *8*(10), p. 63.

McCarthy, B. & Chaudhary, A.R. 2014. Rational choice theory and crime. *Encyclopedia of crime and criminal justice*, pp. 4307-4315.

McClennen, E.F. 2010. Rational choice and moral theory. *Ethical theory and moral practice*, *13*(5), p. 525.

Md, A.Q., Jaiswal, D., Daftari, J., Haneef, S., Iwendi, C. & Jain, S.K. 2022. Efficient Dynamic Phishing Safeguard System Using Neural Boost Phishing Protection. *Electronics*, *11*(19), p. 3133.

Melnikovas, A. 2018. Towards an explicit research methodology: Adapting research onion model for futures studies. *Journal of Futures Studies*, *23*(2), pp. 29-44.

Minnaar, A. & Herbig, F.J. 2021. Cyberattacks and the Cybercrime Threat of Ransomware to Hospitals and Healthcare Services During the COVID-19 Pandemic. *Acta Criminologica: African Journal of Criminology & Victimology*, *34*(3), pp. 155-185.

Mishra, R., Butakov, S., Jaafar, F. & Memon, N. 2020. Behavioral Study of Malware Affecting Financial Institutions and Clients. In *2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress*, pp. 85.

Mishra, S. & Soni, D. 2020. Smishing Detector: A security model to detect smishing through SMS content analysis and URL behavior analysis. *Future Generation Computer Systems*, *108*, pp. 803-815.

Mohammad, R.M., Thabtah, F. & McCluskey, L. 2015. Tutorial and critical analysis of phishing websites methods. *Computer Science Review*, *17*, pp. 1-24.

Moran, R. 1996. Bringing rational choice theory back to reality, *The Journal of Criminal Law and Criminology*, p. 1147.

Morse, J.M. 2003. Principles of mixed methods and multimethod research design. *Handbook of mixed methods in social and behavioral research*, p. 11.

Morse, J.M. & Nichaus, L. 2016. *Mixed method design: Principles and procedures*. Routledge, 4, p. 14.

Moul, K.A. 2019. October. Avoid phishing traps. *Proceedings of the 2019 ACM SIGUCCS Annual Conference*, pp. 199-208.

Mughaid, A., AlZu'bi, S., Hnaif, A., Taamneh, S., Alnajjar, A. & Elsoud, E.A. (2022). An intelligent cyber security phishing detection system using deep learning techniques. *Cluster Computing*, *25*(6), pp. 3819-3828.

Mukkamala, P.P. & Rajendran, S. 2020. A survey on the different firewall technologies. *International Journal of Engineering Applied Sciences and Technology*, *5*(1), pp. 363-365.

Nagin, D.S. & Paternoster, R. 1993. Enduring individual differences and rational choice theories of crime. *Law and Society Review*, pp. 467-496.

Naidoo, R. 2020. A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*, *29*(3), pp. 306-321.

Naidu, D. 2022. Two-factor authentication for effective information security, *International Research Journal of Modernization in Engineering Technology and Science,* 4(6), pp. 4307-4312.

Neelima, K. & Chennapalli, S. 2022. Post-Pandemic Global Inequalities: Causes and Measures. In *Emerging Trends and Insights on Economic Inequality in the Wake of Global Crises*, IGI Global, pp. 40-55.

Nickerson, C. 2022. [online] Simplypsychology.org. Available at: https://www.simplypsychology.org/routine-activities-theory.html [Accessed 7 April 2022].

Nivedha, S., Gokulan, S., Karthik, C., Gopinath, R. & Gowshik, R. 2017. Improving phishing URL detection using fuzzy association mining. *International Journal of Engineering and Science*, pp. 21-31.

Noble, H. & Mitchell, G. 2016. What is grounded theory?. *Evidence-based nursing*, *19*(2), pp. 34-35.

Nordin, N.S., Ismail, M. & Omar, N. 2020. Fuzzy Modelling using Butterfly Optimization Algorithm for Phishing Detection". *International Journal*, *9*(1.5), pp. 355-360.

Nowell, L.S., Norris, J.M., White, D.E. & Moules, N.J. 2017. Thematic analysis: Striving to meet the trustworthiness criteria. *International journal of qualitative methods*, *16*(1), pp. 1-13.

O'Hagan, L. 2018. Angler Phishing: Criminality in Social Media. *5th European Conference on Social Media ECSM*, Queens University, Belfast, UK, p. 192.

Oakes, E., Kline, J., Cahn, A., Funkhouser, K. & Barford, P. 2019. A residential client-side perspective on ssl certificates. In *2019 Network Traffic Measurement and Analysis Conference (TMA)*, IEEE, p. 185.

Okereafor, K. & Adelaiye, O. 2020. Randomized cyber-attack simulation model: A cybersecurity mitigation proposal for post COVID-19 digital era. *International Journal of Recent Engineering Research and Development*, *5*(07), pp. 61-72.

Olofinbiyi, S.A. & Singh, S.B. 2020. The role and place of covid-19: An opportunistic avenue for exponential world's upsurge in cybercrime. *International Journal of Criminology and Sociology*, *9*, pp. 221-230.

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T. & Koucheryavy, Y. 2018. Multi-factor authentication: A survey. *Cryptography*, *2*(1), p. 2.

Omotayo, T. & Kulatunga, U. 2015. The research methodology for the development of a kaizen costing framework suitable for indigenous construction firms in Lagos, Nigeria, *In Proceedings of the Association of Researchers in Construction Management (ARCOM) doctoral workshop on research methodology,* Dublin, Ireland, pp. 1-12.

Orunsolu, A.A., Sodiya, A.S. & Akinwale, A.T. 2019. A predictive model for phishing detection. *Journal of King Saud University-Computer and Information Sciences*, p. 32.

Pacho, T. 2015. Exploring participants' experiences using case study. *International Journal of Humanities and Social Science*, *5*(4), pp. 44-53.

Patayo, C. 2021. A Preventive and Detective Model for Phishing Attack in Small and Medium Size Businesses. *SSRN*, pp. 1-16.

Patton, M.Q. 2005. Qualitative research. *Encyclopedia of statistics in behavioral science*, pp. 1-4.

Pearman, S., Zhang, S.A., Bauer, L., Christin, N. & Cranor, L.F. 2019. Why people (don't) use password managers effectively. In *Fifteenth Symposium On Usable Privacy and Security (SOUPS 2019). USENIX Association, Santa Clara, CA*, pp. 319-338.

Pease, K. 1997. 14 Predicting the Future: The Roles of Routine Activity and Rational Choice Theory. *Rational choice and situational crime prevention: Theoretical foundations*, p. *233*.

Peng, P., Xu, C., Quinn, L., Hu, H., Viswanath, B. & Wang, G. 2019. What happens after you leak your password: Understanding credential sharing on phishing sites. In *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, pp. 181-192.

Petrič, G. & Roer, K. 2022. The impact of formal and informal organisational norms on susceptibility to phishing: Combining survey and field experiment data. *Telematics and Informatics*, *67*, p. 101766.

Phair, D. & Warren, K. 2021. Saunders' Research Onion: Explained simply. *Peeling the onion, layer by layer. Johannesburg: GradCoach*.

Phishing Activity Trends Report Quarter 3. 2021. [online] Available at: https://docs.apwg.org/reports/apwg_trends_report_q3_2021.pdf [Accessed 11 February 2022].

Pranggono, B. & Arabo, A. 2021. COVID-19 pandemic cybersecurity issues. *Internet Technology Letters*, *4*(2), p. 1.

Prasad, R. & Rohokale, V. 2020. *Cyber security: the lifeline of information and communication technology*. Cham, Switzerland: Springer International Publishing, p. 34.

Pratt, T.C. & Turanovic, J.J. 2016. Lifestyle and routine activity theories revisited: The importance of "risk" to the study of victimization. *Victims & Offenders*, *11*(3), pp. 335-354.

Preece, J. 2004. Etiquette online: From nice to necessary. *Communications of the ACM*, *47*(4), pp. 56-61.

Proctor, R.W. & Chen, J. 2015. The role of human factors/ergonomics in the science of security: decision making and action selection in cyberspace. *Human factors*, *57*(5), pp. 721-727.

Rahmani, F. & Leifels, K. 2018. Abductive grounded theory: a worked example of a study in construction management. *Construction management and economics*, *36*(10), pp. 565-583.

Ramdhani, A., Ramdhani, M.A. & Amin, A.S. 2014. Writing a Literature Review Research Paper: A step-by-step approach. *International Journal of Basic and Applied Science*, *3*(1), pp. 47-56.

Raulot, A. 2019. Bypassing phishing protections with email authentication. *Master Security and Network Engineering*, p. 2.

Ritchie, J., Lewis, J., Nicholls, C.M. & Ormston, R. eds. 2013. *Qualitative research practice: A guide for social science students and researchers*. Sage, p. 264.

Rode, K.N., Patil, A.R., Tare, S.V. & Kandane, S.S. 2022. Computer Network Security. *International Journal of Research Publication and Reviews*, ISSN 2582 – 7421, 3(6), pp. 2935 – 2938.

Ross, P.T. & Bibler Zaidi, N.L. 2019. Limited by our limitations. *Perspectives on medical education*, *8*, pp. 261-264.

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

Safa, N.S., Von Solms, R. & Futcher, L. 2016. Human aspects of information security in organisations. *Computer Fraud & Security*, *2016*(2), pp. 15-18.

Sahay, A. 2016. Peeling Saunder's research onion. *Research Gate*, *Art*, p. 4.

Salahdine, F. & Kaabouch, N. 2019. Social engineering attacks: A survey. *Future Internet*, *11*(4), p. 89.

Sandelowski, M. 1995. Sample size in qualitative research. *Research in nursing & health*, *18*(2), p. 180.

Saunders, M., Thornhill, A. & Lewis, P. 2018. Research Methods for Business Students (8th Edition). London: Pearson, p. 130.

Savai, S.F. 2016. Reflection On Ontological, Epistemological And Methodological Perspectives: What Is The Difference Between Qualitative And Quantitative Research?. *International Journal of Innovative Research and Advanced Studies*, *3*(9), pp. 70-72.

Schreck, C.J. 2017. Routine activity theory. In *Preventing Crime and Violence*. Springer, 69, pp. 67-72.

Sebastian, G. 2021. A descriptive study on cybersecurity challenges of working from home during COVID-19 pandemic and a proposed 8 step WFH cyber-attack mitigation plan. *Communications of the IBIMA*, *2*, pp. 2-7.

Shahbaznezhad, H., Kolini, F. & Rashidirad, M. 2021. Employees' behavior in phishing attacks: what individual, organisational, and technological factors matter? *Journal of Computer Information Systems*, *61*(6), pp. 539-550.

Shaikh, A. & Oliveira, D. 2019. Informal it and routine activity theory-a theoretical review. *2019 SoutheastCon*, pp. 1-4.

Shariati, A. & Guerette, R.T. 2017. Situational crime prevention. *Preventing crime and violence*. p. 263.

Sharma, T. 2021. Evolving Phishing Email Prevention Techniques: A Survey to Pin Down Effective Phishing Study Design Concepts, *Illinois Library*, p. 2.

Shirsat, S.D. 2018. April. Demonstrating different phishing attacks using fuzzy logic. In *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*. IEEE, pp. 57-61.

Sidler, V. 2017. *Why phishing attacks are so effective*. [online] Businesstech.co.za. Available at: https://businesstech.co.za/news/industry-news/206328/why-phishing-attacks-are-so-effective/ [Accessed 2 March 2022].

Singh, L.J. & Imphal, N. 2018. A survey on phishing and anti-phishing techniques. *International Journal of Computer Science Trends and Technology (IJCST)*, *6*(2), pp. 62-68.

Sinha, T., Clarke, S. & Farquharson, L. 2018. Shrek, Saunders, and the Onion Myth: Using Myths, Metaphors and Storytelling. In *ECRM 2018 17th European Conference on Research Methods in Business and Management*, p. 366.

Smith, B. & Caddick, N. 2012. Qualitative methods in sport: A concise overview for guiding social scientific sport research. *Asia Pacific journal of sport and social science*, *1*(1), pp. 60-73.

Sovacool, B.K., Axsen, J. & Sorrell, S. 2018. Promoting novelty, rigor, and style in energy social science: Towards codes of practice for appropriate methods and research design. *Energy Research & Social Science*, *45*, p. 18.

Spicer, N. 2004. Combining qualitative and quantitative methods. *Researching society and culture*, *2*, p. 487.

Sridevi, S. 2014. User interface design. *International Journal of Computer Science and Information Technology Research*, *2*(2), p. 415.

Stanton, R. 2005. Beyond disaster recovery: the benefits of business continuity. *Computer Fraud & Security*, *2005*(7), pp. 18-19.

Stembert, N., Padmos, A., Bargh, M.S., Choenni, S. & Jansen, F. 2015 A study of preventing email (spear) phishing by enabling human intelligence. In *2015 European intelligence and security informatics conference*. IEEE, pp. 113-120.

Steves, M.P., Greene, K.K. & Theofanos, M.F. 2019. A phish scale: rating human phishing message detection difficulty. In *Workshop on usable security (USEC)*, pp. 1-14.

Sumner, A., Yuan, X., Anwar, M. & McBride, M. 2021. Examining factors impacting the effectiveness of anti-phishing trainings. *Journal of Computer Information Systems*, pp. 1-23.

Sundaram, A., Priya, V.V. & Gayathri, R. 2020. Age based perpetration of mental stress using pharmed social networking sites on individuals in India. *PalArch's Journal of Archaeology of Egypt/Egyptology*, *17*(7), pp. 1547-1558.

Swanson, R.A. & Holton, E.F. 2005. *Research in organisations: Foundations and methods in inquiry*. Berrett-Koehler Publishers, pp. 50-51.

Terry, G., Hayfield, N., Clarke, V. & Braun, V. 2017. Thematic analysis. *The SAGE handbook of qualitative research in psychology*, *2*, p. 30.

Tillyer, M.S. 2012. Routine activities theory and rational choice theory. In *The Routledge Handbook of Deviant Behavior*, pp. 143-149.

Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E. & Bailey, M. 2016. Users really do plug in USB drives they find. In *2016 IEEE Symposium on Security and Privacy (SP)*, IEEE, p. 307.

Tracy, S.J. 2019. *Qualitative research methods: Collecting evidence, crafting analysis, communicating impact*. John Wiley & Sons, p. 24.

Tran, C. 2020. Recommendations for ordinary users from mitigating phishing and cybercrime risks during COVID-19 pandemic. *arXiv preprint arXiv:2006.11929*, p. 1.

Tsalis, N., Virvilis, N., Mylonas, A., Apostolopoulos, T. & Gritzalis, D. 2015. Browser blacklists: the Utopia of phishing protection. In *E-Business and Telecommunications: 11th International Joint Conference, ICETE 2014, Vienna, Austria, August 28-30, 2014, Revised Selected Papers 11*, Springer International Publishing, pp. 278-293.

Tuli, F. 2010. The basis of distinction between qualitative and quantitative research in social science: Reflection on ontological, epistemological, and methodological perspectives. *Ethiopian Journal of Education and Sciences*, *6*(1), pp. 97-108.

Tweneboah-Koduah, S., Skouby, K.E. & Tadayoni, R. 2017. Cyber security threats to IoT applications and service domains. *Wireless Personal Communications*, *95*, pp. 169-185.

Umarov, F.S. 2018. Using two-factor authentication for personal data. In *International Scientific and Practical Conference World science*, ROST, 1(6), pp. 24-26.

Van Wyk, B. 2012. Research design and methods Part I. University of Western Cape, Available at: https://www.researchgate.net/profile/Ljubomir-Jacic/post/Can_you_provide_any_references_that_support_the_use_of_logic_as_a_research_methodology/attachment/59d63d7dc49f478072ea8829/AS%3A273760551145475%401442281009419/download/Research_and_Design_I.pdf [Accessed 06 August 2022].

Varshney, G., Misra, M. & Atrey, P.K. 2016. A phish detector using lightweight search features. *Computers & Security*, *62*, pp. 213-228.

Vasileiou, K., Barnett, J., Thorpe, S. & Young, T. 2018. Characterising and justifying sample size sufficiency in interview-based studies: systematic analysis of qualitative health research over a 15-year period. *BMC medical research methodology*, *18*, pp. 1-18.

Vayansky, I. & Kumar, S. 2018. Phishing–challenges and solutions. *Computer Fraud & Security*, *2018*(1), pp. 15-20.

Verhoef, M.J. & Casebeer, A.L. 1997. Broadening horizons: integrating quantitative and qualitative research. *Canadian Journal of Infectious Diseases*, *8*(2), pp. 65-66.

Verizon Enterprise Solutions. 2021. *2021 Data Breach Investigations Report (DBIR)*. [online] Available at: https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdfx [Accessed 2 March 2022].

Viechtbauer, W., Smits, L., Kotz, D., Budé, L., Spigt, M., Serroyen, J. & Crutzen, R. 2015. A simple formula for the calculation of sample size in pilot studies. *Journal of clinical epidemiology*, *68*(11), pp. 1375-1379.

Vishwanath, A., Herath, T., Chen, R., Wang, J. & Rao, H.R. 2011. Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, *51*(3), pp. 576-586.

Vitak, J., Liao, Y., Subramaniam, M. & Kumar, P. 2018. 'I Knew It Was Too Good to Be True" The Challenges Economically Disadvantaged Internet Users Face in Assessing Trustworthiness, Avoiding Scams, and Developing Self-Efficacy Online. *Proceedings of the ACM on human-computer interaction*, *2*(CSCW), pp. 1-25.

Vogl, S. 2013. Telephone versus face-to-face interviews: Mode effect on semi structured interviews with children. *Sociological Methodology*, *43*(1), pp. 133-177.

Wadhwa, A. & Arora, N. 2017. A Review on Cyber Crime: Major Threats and Solutions. *International Journal of Advanced Research in Computer Science*, *8*(5), p. 2219.

Wall, D. 2007. *Cybercrime: The transformation of crime in the information age*. Polity Press, 4, p. 36.

Wang, J., Herath, T., Chen, R., Vishwanath, A. & Rao, H.R. 2012. Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE transactions on professional communication*, *55*(4), 345-362.

Wen, Z.A., Lin, Z., Chen, R. & Andersen, E. 2019. What. hack: engaging anti-phishing training through a role-playing phishing simulation game. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pp. 1-12.

Westland, C. 1996. A rational choice model of computer and network crime. *International Journal of Electronic Commerce*, *1*(2), pp. 109-126.

Wijaya, V. & Yulianti, N.M.D.R. 2020. Pop Up Ads Affecting Buying Decision Mediated by Purchase Intention in Online Marketplace (Lazada) in Denpasar. *TIERS Information Technology Journal*, *1*(1), p. 34.

Wikström, P.O.H. & Treiber, K. 2015. Situational theory: The importance of interactions and action mechanisms in the explanation of crime. *The handbook of criminological theory*, p. 164.

Williams, M. & Boonthum-Denecke, C. 2017. Security and Digital Forensics in Cloud Computing. *In Proceedings of 2017 ADMI Symposium*, Virginia Beach, Virginia USA, p. 3.

Woods, E. 2021. *The Real Reason for Successful Phishing Attacks*. [online] Blog.usecure.io. Available at: https://blog.usecure.io/the-real-reason-why-phishing-attacks-are-so-successful [Accessed 2 March 2022].

Writer, S. 2020. *Have you ever wondered what the success rate is for an online scam in South Africa?* [online] Businesstech.co.za. Available at: https://businesstech.co.za/news/internet/418117/have-you-ever-wondered-what-the-success-rate-is-for-an-online-scam-in-south-africa/ [Accessed 22 February 2022].

Xu, W. & Zammit, K. 2020. Applying thematic analysis to education: A hybrid approach to interpreting data in practitioner research. *International Journal of Qualitative Methods*, *19*, pp. 1-11.

Yang, L., Zhang, J., Wang, X., Li, Z., Li, Z. & He, Y. 2021. An improved ELM-based and data preprocessing integrated approach for phishing detection considering comprehensive features. *Expert Systems with Applications*, 165, p. 1.

Younis, Y.A. & Musbah, M. 2020. September. A framework to protect against phishing attacks. In *Proceedings of the 6th International Conference on Engineering & MIS 2020*, pp. 1-6.

Zhu, Y., Zhang, B., Wang, Q.A., Li, W. & Cai, X. 2018. The principle of least effort and Zipf distribution. In *Journal of Physics: Conference Series*. IOP Publishing.1113(1), p. 012007.

Zhuo, S., Biddle, R., Koh, Y.S., Lottridge, D. & Russello, G. (2022). SoK: Human-Centred Phishing Susceptibility. *arXiv preprint arXiv:2202.07905*, pp. 1-13.

Zipf, G. 1950. The Principle of Least Effort Reading. MA: Addison Wesley.

Zouina, M. & Outtaj, B. 2017. A novel lightweight URL phishing detection system using SVM and similarity index. *Human-centric Computing and Information Sciences*, *7*(1), pp. 1-13.

Zuraiq, A.A. & Alkasassbeh, M. 2019. Phishing detection approaches. In *2019 2nd International Conference on new Trends in Computing Sciences (ICTCS)*, IEEE, pp. 1-6.

Appendix 1: Research interviews: Participant consent form

Consent Form University of the Western Cape

Project Title: Remedies to reduce user susceptibility to phishing attacks

Researcher: Ashley Maseko

Please initial the boxes to show your agreement and understanding of what is expected for this study.

1. I confirm that I have read and understood the information sheet explaining the above research project and I have had the opportunity to ask questions about the project. ☐
2. I understand that my participation is voluntary and that I am free to withdraw at any time without giving any reason and without there being any negative consequences. In addition, should I wish to withdraw, I may contact the lead researcher at any time to do so). ☐
3. I understand my responses and personal data will be kept strictly confidential. ☐
4. I give permission for members of the research team to have access to my responses without revealing any part of my identity. ☐
5. I understand that my name will not be linked with the research materials, and that I will not be identified or identifiable in the reports or publications that result for the research. ☐
6. I agree for the **anonymized** data collected to be used in future research. (*Circle the appropriate answer*). Yes / No
7. I hereby agree to be audio recorded. (*Circle the appropriate answer*). Yes / No

---

In terms of the requirements of the Protection of Personal Information Act (Act 4 of 2013), personal information will be collected and processed:

☐ I hereby give consent for my personal information to be collected, stored, processed, and shared as described in the information sheet.
☐ I do not give consent for my personal information to be collected, stored, processed, and shared as described in the information sheet.

_____	_____	_____
Name of Participant (*or legal representative*)	Date	Signature
_____	_____	_____
Name of person taking consent	Date	Signature

(If different from lead researcher)

_____	_____	____ _____
Supervisor	Date	Signature

Copies: All participants will receive a copy of the signed and dated version of the consent form and information sheet for themselves. A copy of this will be filed and kept in a secure location for research purposes only.

Researcher:	**Supervisor:**	**HOD:**
Ashley Maseko Email: 3725633@myuwc.ac.za Contact: +27 63 982 0590	Prof. Joel Chigada Email: jchigada@uwc.ac.za Contact: 021 959 2578	Prof. Joel Chigada Email: jchigada@uwc.ac.za Contact: 021 959 2578

Appendix 2: Information Sheet

UNIVERSITY of the WESTERN CAPE

Private Bag X17, Belville, 7535
South Africa
Tel: +27 (0) 21 959 3680
Fax: +27 (0) 21 959 3522
www.uwc.ac.za

Faculty of Economic and Management Sciences
Department of Information Systems

Research Project Information Sheet/Privacy sheet: Interviews

Project Title:	**Remedies to reduce user susceptibility to phishing attacks**

In terms of the requirements of the Protection of Personal Information Act (Act 4 of 2013), personal information will be collected and processed:

What is this study about?

I am Ashley Maseko, a student completing a Master of Commerce degree in Information Systems at the University of the Western Cape. I am currently conducting research on the remedies that can be implemented to reduce user susceptibility to phishing attacks. I am conducting this study for academic purposes. Even so, the findings from this research may also be shared with the university authorities and also made public.

Why are you being invited to participate in this study?

The study seeks to investigate user behavior in order to formulate well informed remedies and recommendations. You have been identified and invited as a suitable prospective participant in the research because you are an employee within a financial institution in the Western Cape wherein the research is being conducted. The invitation is so that you may take part in interviews with the researcher where you share responses based on exposure and understanding. Employees of financial institutions who are interested and who have been contacted about participating in the study qualify as the study's participants.

What will I be asked to do if I agree to participate?

Should one accept to participate, this interview comprises a few semi-structured questions and may take around 25 minutes to complete. However, it is important to note that If you do not wish to answer any of the questions, you can still choose not to.

Would my participation in this study be kept confidential?

No personal information, such as your name, address, or identity number, is required. All other information about you elicited as part of the study, such as your age, education, work position, and so on, is kept anonymous.

What are the risks of this research?
There are no known risks associated with taking part in this study. This research will not expose you to any harm as a result of your participation.

What are the benefits of this research?
The results of this study will help financial institutions better understand phishing, a cybercrime that takes advantage of system shortcomings and staff vulnerabilities to disrupt business operations. The study aims to put forward findings that will help financial institutions to reduce the success rate of phishing attacks, taking user vulnerability areas into account. When everything else fails in their attempts to hack and crack systems, attackers frequently turn to targeting and misleading users, therefore the study will help organizations reinforce their human line of defense (the human users).

Do I have to be in this research, and may I stop participating at any time?
Your participation in this interview is completely and entirely voluntary. You have the option to withdraw your agreement to participate and have your replies excluded from the study. If you decide to participate in this interview, you may stop participating at any time you want should you change your mind.

What type of personal information will be collected?
Information pertaining to your demographic information will be collected (i.e. age, occupation, highest qualification, and gender) the remainder of the open ended questions in the second section of the interview relate to the subject matter of phishing.

Who at UWC is responsible for collecting and storing my personal information?
Your personal information will be stored by the researcher (Ashley Maseko), who will also be the data collector. The researcher is obligated to protect the personal information collected from participants.

Who will have access to my personal information outside of UWC?

No one outside of the University of the Western Cape will have access to the personal information obtained from participants. Identifiable private information belonging to participants will be stored securely by the University.

How long will my personal information be stored?
The research data will be stored on the university email google drive and it will be disposed of after a period of 5 years.

How will my personal information be processed?

Personal information will be processed (i.e. collected, handled, stored, disclosed and destroyed) fairly, lawfully and transparently. Personal information will be pseudonymised. Personal information will only be processed for specified, explicit and legitimate purposes. This is to assure you that personal data will not be used for purposes that are incompatible with the original purpose for which they were collected.

What if I have questions?

If you have any questions feel free to contact the project leader whose details are as follows:

Contact details of project leader (study supervisor)
Name: Professor Joel Chigada
University of the Western Cape, Department of Info0rmation Systems
Telephone: 021 959 2578
Email: jchigada@uwc.ac.za

Contact details of student
Name: Ashley Eventhia Maseko
Telephone: +27 63 982 0590
Email: 3725633@myuwc.ac.za

NOTE: *This research project has received ethical approval from the Humanities & Social Sciences Research Ethics Committee of the University of the Western Cape, Tel. 021 959 4111, email: research-ethics@uwc.ac.za*

Appendix 3: Interview Schedule

Private Bag X17, Belville, 7535
South Africa
Tel: +27 (0) 21 959 3680
Fax: +27 (0) 21 959 3522
www.uwc.ac.za

Title of Study: Remedies to reduce user susceptibility to phishing attacks

Dear Participant

My name is Ashley Maseko, a Masters student in the Department of Information Systems within the Faculty of Economics and Management Sciences at the University of the Western Cape. I am conducting research on, "Remedies to reduce user susceptibility to phishing attacks". therefore, I invite you to participate in this study. The Ethics in Research Committee of the University of the Western Cape's EMS faculty has authorized and granted permission to proceed with the study. Your participation in this study is completely voluntary, and you can opt out at any time. Your responses will be kept with the utmost confidentiality and will be crucial to the completion of this study. In this study, you will not be asked to provide any personally identifiable or sensitive information. It will take about 15 minutes to complete the questionnaire. You are giving your implied consent to participate in the research study by completing this questionnaire. Please feel free to contact the researcher if you have any queries regarding the study.

SECTION A: DEMOGRAPHIC INFORMATION

In this section, you are requested to mark your answer with an X.

What is your gender?

Gender	
Male	
Female	
Prefer not to answer	

What is your age?

18 – 24 years	
25 – 44 years	

45 years +	

What is your highest qualification?

National Diploma	
Bachelor's Degree	
Honour's Degree	
Master's Degree	
Doctorate	
Other (specify)	

What is your current position/title?

How many years have you been in your current position?

< 1 year	
1 – 2 years	
2 – 4 years	
> 4 years	

SECTION B: INTERVIEW QUESTIONS

The Corona Virus Disease 2019 has accelerated the pace at which digital transformation has been adopted by most organisations. With this shift, came a significant surge in social engineering attacks by threat actors directed towards internet users and service providers. Phishing attacks have been a particularly severe threat to the financial industry. Phishing is a cybercrime that thrives on deception and involves cyber criminals tricking users into divulging confidential information.

1. The financial industry has seen an increase in social engineering attacks as a result of the COVID-19 pandemic. How has cybercrime, particularly phishing attacks, affected your institution?

2. Describe the extent to which insufficient training, user negligence, and malice aid the effectiveness of phishing attacks against institutions based on your work experience and exposure.

3. Describe the security policies in place at your institution to protect systems from being compromised by different kinds of social engineering attacks (like Phishing).

4. What are some of the visible inappropriate user conducts (attributed to negligence, malice, or inadequate training) that you have observed in the workplace that you believe pose a risk of phishing attacks becoming successful in your organisation.

5. Cybersecurity focuses on security key systems from being compromised by threat actors. What lessons has your institution taught you about how to avoid becoming a victim of phishing or other forms of social engineering?

6. What are some of the measures you may recommend to other employees based on personal experience to help them protect themselves from various social engineering attacks like phishing?

NOTE: *This research project has received ethical approval from the Humanities & Social Sciences Research Ethics Committee of the University of the Western Cape, Tel. 021 959 4111, email: research-ethics@uwc.ac.za.*