Combatting social engineering attacks in South Africa: A critical analysis

N van der Linde

orcid.org/0009-0008-8413-0369

Dissertation accepted in fulfilment of the requirements for the degree *Master of Commerce in Forensic Accountancy* at the North-West University

Supervisor: Mr F Triegaardt

Co-supervisor: Prof DP Schutte

Graduation: May/June 2026

DECLARATION

I, Nici van der Linde, hereby declare that the dissertation entitled *"Combatting social engineering attacks in South Africa: A critical analysis"* is my own work, has been text-edited in accordance with the required standards, complies with the requirements for the degree Master of Commerce in Forensic Accountancy, and has not been submitted to any other university.

Signature: 

Date: 24 November 2025

ACKNOWLEDGEMENTS

First and foremost, I give thanks to my Lord and Saviour, Jesus Christ, for granting me the strength, wisdom and perseverance to complete this journey. His grace and unwavering love have sustained me throughout the challenges of this research, and it is through Him that I have been able to achieve this milestone and contribute meaningfully to society.

I would like to express my sincere gratitude to my supervisors, Mr Frans Triegaardt and Prof Danie Schutte, for their expert guidance, encouragement, and constructive insight throughout this process. Your mentorship has been instrumental in shaping not only this dissertation but also my academic growth and professional perspective.

My heartfelt thanks also go to Mrs Jomoné Müller, my language editor, for her meticulous attention to detail and valuable contributions that enhanced the clarity and quality of this work

A special word of thanks is extended to Mrs Petra Gainsford for her generous assistance in formatting the page numbers and refining the Table of Contents for submission. Your attention to precision and commitment to ensure the document meets the highest presentation standards are deeply appreciated.

Finally, to my mom, dad, and sister, thank you for your endless love, support and encouragement. Your belief in me has been my greatest motivation and constant source of encouragement. I am deeply grateful for your patience, sacrifices and unwavering faith in my abilities.

“For God has not given us a spirit of fear, but of power and of love and of a sound mind.”
II Timothy 1:7, NKJV

This Master’s degree marks not an end but the beginning of a greater journey, one guided by faith, purpose and gratitude.

PREFACE

This study was completed in the form of articles. Two separate articles (Chapters 2 and 3) were compiled and prepared in accordance with accredited peer-reviewed academic journal author guidelines.

The details of these submissions, at the time of final compilation, are as follows:

Article 1

This article, titled "*Identifying social engineering attacks: A critical analysis,*" was completed as Chapter 2. It was submitted for publication to the Journal of Financial Crime. The article investigates the operational mechanisms, psychological tactics and behavioural dynamics that define social engineering attacks. It provides a comprehensive analysis of the most prevalent forms of social engineering, including phishing, pretexting and baiting, while integrating criminological insights to explain offender motivation and victim susceptibility. The findings contribute to understanding how human behaviour and cognitive biases are exploited within the broader cybersecurity context.

Article 2

This article, titled "*Identifying social engineering attacks: A critical analysis of legal, psychological, criminological and cybersecurity perspectives,*" was completed as Chapter 3 and submitted for publication to the Journal of Financial Crime. It critically evaluates South Africa's legal, organisational and behavioural capacity to mitigate social engineering threats, focusing particularly on statutory instruments such as the Electronic Communications and Transactions Act 25 of 2002 (hereinafter referred to as the "ECTA") and the Cybercrimes Act 19 of 2020 (hereinafter referred to as the "Cybercrimes Act"). Adopting an interdisciplinary framework, the article synthesises insights from law, psychology, criminology and cybersecurity to identify regulatory gaps and propose comprehensive strategies for enhancing national and institutional resilience against social engineering.

The articles were co-authored by the study's supervisor (Mr Frans Triegaardt) and co-supervisor (Prof Danie Schutte), both of whom provided invaluable academic guidance and critical input throughout the research process. These individuals are affiliated with the Faculty of Economic and Management Sciences, School of Accounting, at the North-West University, and are aware that these articles collectively form part of the final dissertation submitted in fulfilment of the requirements for the degree Master of Commerce.

ABSTRACT

Social engineering has emerged as one of the most pervasive and damaging forms of cyber-enabled crime, exploiting human psychology rather than technological vulnerabilities. In the South African context, the increasing sophistication of these attacks poses serious risks to individuals, businesses and state institutions, resulting in financial losses, reputational harm and public distrust of digital systems. Despite legislative efforts through the Cybercrimes Act 19 of 2020 and the Electronic Communications and Transactions Act 25 of 2002, gaps persist in behavioural awareness, criminological enforcement and organisational preparedness. These shortcomings collectively undermine national cyber resilience and contribute to South Africa's vulnerability to social engineering attacks.

The main objective of this study was to critically analyse how social engineering attacks can be effectively combatted in South Africa through an interdisciplinary framework that integrates legal, psychological, criminological and cybersecurity perspectives. In order to meet this overarching objective, the following areas were critically examined:

- The operational and behavioural foundations of social engineering attacks. This analysis identified the common manipulation techniques, offender motivations and cognitive biases that enable deception-based cybercrimes such as phishing, pretexting and baiting.
- South Africa's legal and institutional response to social engineering. This involved an evaluation of the Cybercrimes Act 19 of 2020 and Electronic Communications and Transactions Act 25 of 2002 to determine their effectiveness in addressing social engineering attacks, as well as identifying enforcement, awareness and policy gaps that impede their implementation.

The study adopted a qualitative research design grounded in an interdisciplinary literature review to evaluate both the human and systemic dimensions of social engineering. The study synthesised insights across the four analytical domains and identified recurring deficiencies in user awareness, reactive law enforcement and the limited integration of behavioural science within cybersecurity practice.

In conclusion, the findings demonstrate that while South Africa has made legislative progress in addressing cyber-enabled offences, the current framework remains fragmented and overly reliant on legal compliance rather than behavioural resilience. The study recommends a national strategy that incorporates behaviourally informed awareness programmes, criminological profiling of offenders, enhanced digital literacy education and cross-sector collaboration to enhance

proactive defence mechanisms. Future research should further explore how interdisciplinary cooperation between law enforcement, academia and the private sector can embed behavioural science principles into national cybersecurity policy.

South Africa can move towards a more sustainable and adaptive model of cyber resilience by adopting this integrated approach, one that not only prosecutes cybercrime but also prevents its human exploitation at scale.

Key terms: Behavioural manipulation, criminology, cyber resilience, cybercrime, cybersecurity, legal reform, psychology, social engineering, South Africa, the Cybercrimes Act

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ABBREVIATIONS

2FA	Two-Factor Authentication
ACFE	Association of Certified Fraud Examiners
AI	Artificial Intelligence
BEC	Business Email Compromise
CISOs	Chief Information Security Officers
CSC	Cybersecurity Culture
CPA	Criminal Procedure Act 51 of 1977
ECSPs	Electronic Communications Service Providers
ECTA	Electronic Communications and Transactions Act 25 of 2002
ICT	Information and Communication Technology
IoT	Internet of Things
IT	Information Technology
MFA	Multifactor Authentication
POPIA	Protection of Personal Information Act 4 of 2013
RSA	Republic of South Africa
SAPS	South African Police Services
SMS	Short Message Service

CHAPTER 1 PURPOSE, SCOPE AND OUTLINE OF THE STUDY

1.1 Background

1.1.1 Conceptualisation and technological evolution of Social Engineering

The art of deceiving people into providing their credentials and then exploiting them to gain access to networks or accounts is known as social engineering, sometimes known as human hacking (Alabdan, 2020:13; Conteh & Schmick, 2016:31; Ivanov *et al.*, 2021:425). Social engineering is a hacker's deceptive or manipulative exploitation of people's tendency to trust, be cooperative or simply follow their drive to explore and be interested (Alabdan, 2020:13, Conteh & Schmick, 2016:31, Ivanov *et al.*, 2021:425). Social engineering is becoming more common as new technology and cyber environments emerge (Cristescu *et al*., 2022:114).

The manner in which business is conducted across industries is constantly evolving due to economic, social, political and technical changes (Salmon-Powell *et al*., 2021:1). Huseynov and Kose (2022:1) state that despite technological advances in information security and organisations' ongoing efforts to increase user awareness of information security, social engineering attacks have become an increasingly severe threat to virtual communities in recent years. Artificial Intelligence (AI) is one such global effect that is transforming the commercial landscape (Salmon-Powell *et al*., 2021:1). Machine learning and AI can make social engineering attacks more effective and aggressive (Cristescu *et al*., 2022:114).

The simulation of human intellect in computers engineered to think like humans and mimic their activities is referred to as AI (Salmon-Powell *et al*., 2021:1). Large-scale, automated and advanced social engineering attacks become possible as a large group of victims can be contacted at the same time to launch attacks (Cristescu *et al*., 2022:114). As a result of these attacks, forensic accounting has grown as an essential practice for accounting companies (Rezaee *et al.* 2018:87).

1.1.2 Forensic Accounting in the digital and cybercrime environment

Forensic accounting practitioners are required to exercise professional scepticism when gathering and analysing evidence, drawing on data science, data management, and information technology (IT) capabilities to transform investigative questions into meaningful analytical outputs (Rezaee *et al.*, 2018:87). Importantly, forensic accounting operates at the intersection of multiple disciplines, including accounting, law, and technology, requiring practitioners to possess cross-disciplinary knowledge and expertise. This multidisciplinary competence enables forensic accountants not only to ask the appropriate investigative questions but also to interpret and

translate complex data into analytically sound and legally admissible findings. Forensic accounting practitioners must further understand the legal boundaries within which they operate and distinguish between technically feasible analysis and evidence that is relevant and permissible for legal proceedings (Harkin & Whelan, 2022:72).

Accordingly, forensic accounting services encompass a broad range of specialised activities, including fraud examination, corruption and bribery investigations, business valuation, expert witness testimony, cybercrime management, cybersecurity advisory services, and litigation support. These services reflect the profession's integrative role in ensuring that technological data, analytical processes, and evidentiary outputs are aligned to support meaningful decision-making and judicial outcomes (Rezaee, Wang & Lam, 2018:87).

Forensic accounting practitioners, including digital forensic analysts and experienced cybercrime investigators, are required to possess advanced technical competencies supported by specialised and continuous training to perform high-end investigations effectively (Harkin & Whelan, 2022:72). According to Rezaee *et al.* (2018:87) forensic accounting practitioners (or forensic accountants) are professionals with multidisciplinary knowledge spanning accounting, technology, and law, whose expertise is developed through targeted education, professional certification, and ongoing skills development. This specialised training equips practitioners to conduct complex fraud investigations, analyse sophisticated digital evidence, and support the detection and prevention of fraud within legally and procedurally sound frameworks (Mansor, 2015:191).

Forensic accounting practitioners must learn a wide range of extremely particular technological challenges (Harkin & Whelan, 2022: 72). Breakthroughs in IT, for example cloud computing, electronic social media and analytics, have provided companies of all sizes with an unprecedented amount of data and information available (Rezaee *et al.* 2018:87). Social networks, mobile communications and the Internet of Things (IoT) generate not just vast amounts of data, but also numerous methods of social engineering attacks (Cristescu *et al*., 2022:114).

1.1.3 Human vulnerability and the escalation of Social Engineering attacks

A social media networking platform allows users to participate and share multimedia content such as text, audio, video, images, graphs and animations via a website or an application (Soomro & Hussain, 2019:9). According to Almadhoor *et al.* (2021:2973) cybercriminals use social media to gain access to other people's personal information and then use it to commit crimes. Therefore, cybercrime is on the rise and as Almadhoor *et al.* (2021:2973) conclude, it is owed to the increased number of social media users, which continues to grow exponentially each day. As a

result, people are readily hacked, making themselves as well as their social media posts prime targets for cyberattacks (Conteh & Schmick, 2016:31).

Social engineering is a method that uses faults in human logic known as cognitive biases to get access to private and sensitive information (Conteh & Schmick, 2016:32). In the online environment, social engineering refers to an attack in which human vulnerabilities are exploited in order to obtain classified information, gain unauthorised access to restricted areas or violate the security objectives of cyber elements such as infrastructure, data and resources (Cristescu *et al*., 2022:114). As a digital network, the internet enables automated data and information processing at near light speed and on an unprecedented scale (Koops, 2011:737). While security technology solutions strive to improve the security of information systems, human factors are a weak link that is exploited during a social engineering attack (Conteh & Schmick, 2016:32).

The foundation of an attack is to convince the surrender of personal information to exploit an individual or an organisation (Conteh & Schmick, 2016:32). As a result, social engineering is a type of cybercrime in which the attacker takes advantage of human vulnerability through social contact in order to breach cybersecurity (Cristescu *et al*., 2022:114). In essence, an attacker uses social engineering as a deception strategy to defeat computer security systems by using human insiders and knowledge (Conteh & Schmick, 2016:32). As mentioned by He *et al.* (2022:92), employees of a company have access to sensitive data and specific procedures, while being able to avoid physical monitoring. This makes an internal attack difficult to detect, with extensive consequences.

It is generally simple to deceive computer users into infecting their corporate network or mobile devices (Conteh & Schmick, 2016:31). Social engineering attacks are more effective against individuals who were not informed of the potential risks and attacks that can be carried out by fraudulent and malicious intent (Venkatesha *et al.*, 2021:78). This is done by luring them to spoof websites, tricking them into clicking on dangerous links and then downloading and installing the malicious software or backdoors (Conteh & Schmick, 2016:31). In contrast to traditional attacks including password cracking and software flaws, social engineering attacks focus on exploiting vulnerabilities from a human perspective in order to circumvent security barriers (Cristescu *et al*., 2022:114).

In recent years, the increasing rate of fraud in corporate organisations has become a significant global concern, making it essential to examine and identify the associated fraud risk factors (Mansor, 2015:191). As a result of the increased fraud rate, Mimecast (2023:2) surveyed 1700 Chief Information Security Officers (CISOs) from various countries as part of the 2022 State of Email Security Survey.

From this survey, Mimecast (2023:4) have reported that 95% of cyberattacks are growing increasingly sophisticated, that two out of three companies were harmed by a ransomware attack and lastly that 97% of companies have been targeted by email-based phishing attacks. Security decision-makers have seen an 84% increase in social engineering attacks over the past 12 months, of which the most widespread is phishing (Mimecast, 2023:9). Following this, a few social engineering attacks are briefly discussed in order to provide a more reliable and precise assessment of this study.

1.2 Social engineering attacks

As mentioned by Ivanov *et al.* (2021:425), social engineering is the use of human characteristics, such as curiosity, to carry out an attack on computer systems without the use of technical means. Hackers approach their victims through a variety of methods and channels, including the use of social media (Huseynov & Kose, 2022:1). Social media influences people's cultural, economic and social lives and has become an essential part of daily existence (Soomro & Hussain, 2019:9).

Social media posts generally cause significant economic problems, requiring businesses and individuals to take costly measures to ensure their safety and reduce the commission of cybercrime (Snail, 2009:2). Due to social media's quick response time, it is not only a communication medium for the community, but also a medium for the criminal community (Soomro & Hussain, 2019:9). The following is a brief introduction of the *modus operandi* of social engineering attacks that are used to target victim.

1.2.1 Phishing

According to Alabdan (2020:1), phishing constitutes a social engineering technique that uses various deceptive methods to manipulate individuals into divulging sensitive information such as email credentials, login details, passwords or financial data. These attacks are intentionally designed to harvest personally identifiable information, including names, residential addresses and identification numbers, by exploiting a victim's trust or sense of urgency, thereby prompting the disclosure of confidential information (Conteh & Schmick, 2016:32). Cybercriminals leverage social media as users expose their credentials, such as birthdates, mobile numbers, friends' contacts, addresses, driving licence details and credit card particulars (Nagunwa, 2014:80). This information is subsequently exploited by the attacker against the victim (Alabdan, 2020:1).

Victims can also be lured to fraudulent websites by clicking on untrustworthy links, which then instil a sense of urgency to influence users into acting in ways that defy good judgement (Conteh & Schmick, 2016:32).

1.2.2 Pretexting

A fabrication scenario is used to confirm and steal personal information from a victim in this type of social engineering assault (Conteh & Schmick, 2016:32). According to Bishnoi *et al.* (2023:683), it is possible to acquire access to private information through deception. The ease with which people share personal information online provides attackers with a valuable resource for identifying groups of targets and potentially approaching victims (Alabdan, 2020:9).

The changing nature of communication has enabled criminals to exploit social media websites for their own malicious purposes (Soomro & Hussain, 2019:10). In a pretexting scam, for example, the offender poses as someone confirming the victim's identification and collects sensitive information under the pretence of needing it to complete the verification process (Bishnoi, A., 2023:683). According to Soomro and Hussain (2019:10), traditional crime is giving way to electronic crime.

Such vigilance is required because hackers directly engage with their targets in interpersonal communication: via phone calls, emails, text messages or even in person (Gehl & Lawson, 2022:91). This strategy necessitates the attacker crafting a credible story that leaves little opportunity for a victim to doubt (Conteh & Schmick, 2016:32). The role must then be meticulously prepared before being put to the test during an interaction (Gehl & Lawson, 2022:92).

1.2.3 Baiting

Baiting is similar to phishing in that it draws a victim with enticement methods (Conteh & Schmick, 2016:32). According to Bishnoi *et al.* (2023:683), an example of baiting is when the attacker conceals the "bait" with a malware-infected USB flash drive. The victim unintentionally installs the virus by connecting the device (Bishnoi, A., 2023:683). Hackers utilise the promise of products to entice users to disclose their login credentials to a specific site (Conteh & Schmick, 2016:32). This type of attack performs malicious actions in the background, undetected by the victims (Salahdine & Kaabouch, 2019:6).

1.2.4 Quid pro quo

This type of threat is comparable with baiting, but it is offered as a technical service in exchange for information (Conteh & Schmick, 2016:32). Attackers convince the victim that they will be receiving something in return (Mattera & Chowdhury, 2021:58). According to Salahdine and Kaabouch (2019:8), these attacks provide complimentary services to the victim in order to entice them. As an example, an attacker may mimic an IT representative and help a victim who is

experiencing technical difficulties (Conteh & Schmick, 2016:32). They necessitate the exchange of information in return for a service or commodity (Salahdine & Kaabouch, 2019:8).

1.2.5 Tailgating

Tailgating and piggybacking are used in these types of attacks to gain access to restricted areas (Conteh & Schmick, 2016:32). In tailgating, an intruder gains access to a restricted area by following closely behind someone using a legitimate access card (Bishnoi, A., 2023:683). The victim assumes an authorised user is holding the door open for them (Bishnoi, A., 2023:683). According to Syafitri *et al.* (2022:39329), hackers merely need to follow activities conducted by members of the organisation, allowing these hackers to freely move through the security perimeter within the organisation.

1.2.6 Vishing

Vishing is a type of phishing that employs the use of voice (Alabdan, 2020:7). Vishing, a voice-based form of phishing, is a social engineering attack in which attackers obtain sensitive information, such as bank account details, from unsuspecting victims over the phone (Alabdan, 2020:7; Bishnoi, A., 2023:683). According to Obuhuma and Zivuku (2020:2), attackers claim to be from trustworthy firms in order to persuade individuals to disclose personal information such as credit card details.

1.2.7 Smishing

Smishing entails sending a short message service (SMS) text message posing as a trusted authority, such as a bank, with an important message (Alabdan, 2020:7). Social engineer attackers use these messages to tempt victims into disclosing sensitive information (Obuhuma & Zivuku, 2020:3). Smishing also involves sending an SMS to a victim that either contains malware directly or contains a link to a website that contains malware (Alabdan, 2020:7).

The abovementioned comparisons only serve to illustrate the vast contrasts in the different types of *modus operandi* of social engineering attacks. Each of these is discussed in more detail in the subsequent chapters.

1.3 Legal framework combatting cybercrime

Cybercrime demonstrates the relevance of cybersecurity and the need to protect citizens while they are online (Kangapi & Chindenga, 2022:1). Identity theft, malicious malware, ransomware, social blackmail and cyberbullying are a few instances of cyber risks and threats (Kritzinger,

2019:27). Dashora (2011:240) defines cybercrime as any crime committed on the internet that makes use of a computer as either a tool or a targeted victim. An increasing number of cyber users are becoming cyber victims due to a lack of cyber safety awareness, knowledge and skills on how to safeguard themselves and their information (Kritzinger, 2019:27).

The Cybercrimes Act 19 of 2020 - creates cybercrime-related offences, criminalises the disclosure of harmful data messages, provides for interim protection orders and further regulates jurisdiction and investigative powers. Aside from the Cybercrimes Act, other relevant South African legislation exists to combat social engineering attacks. However, among the other relevant legislation, the Cybercrimes Act is the most prominent.

Although the Cybercrimes Act is in place to make the cyberspace safer, the lack of a strong cybersecurity culture (CSC) exposes South Africans to cybercrime threats (Kangapi & Chindenga, 2022:2). As explained by Williams *et al.* (2021), the aim of the Cybercrimes Act is to build an integrated cybersecurity legal framework to effectively deal with cybercrime and manage cybersecurity issues. According to Kritzinger (2019:27), cyber safety awareness is, therefore, critical to ensure that all cyber users have the knowledge and skills to protect themselves and their personal information within cyberspace.

The Cybercrimes Act consists of various chapters that play an important role in combatting cybercrime. These sections, as explained below, are discussed in greater detail in subsequent chapters.

1.3.1 Sentencing

The Cybercrimes Act prescribes specific penalties for offenders, including fines ranging from R5 million to R10 million and/or imprisonment of between 5 and 10 years. More serious offences are punishable by imprisonment of up to 15 years, while computer-related terrorist activity and related offences may result in imprisonment not exceeding 25 years. The Cybercrimes Act creates a punishable offence for the dissemination of data communications that advocate, encourage or instigate hatred, prejudice or violence, with up to two years in prison or a fine.

Under section 276 of the Criminal Procedure Act (CPA) 51 of 1977, the courts have also been given the authority to impose any term they feel appropriate on anyone found guilty of cyber fraud, cyber forgery or uttering.

1.3.2 Jurisdiction

Section 24 of the Cybercrimes Act also grants South African courts' jurisdiction to hear any conduct or omission alleged to be an offence under the Cybercrimes Act and affecting a person in South Africa, even if the defined cybercrime is committed outside of South Africa.

1.3.3 Mutual assistance

Chapter 5 of the Cybercrimes Act enables the South African Police Services (SAPS) to not only investigate, search, access and seize, but also to collaborate with other authorities to investigate cybercrime. Furthermore, the Act requires the National Director of Public Prosecutions to submit a report to the National Prosecuting Authority on the number and outcomes of cybercrime prosecutions.

1.3.4 Reporting obligations and capacity building

Section 54 of the Cybercrimes Act requires electronic communications service providers (ECSPs) and financial institutions, such as banks, to report cybercrime within 72 hours of becoming aware of it. Section 55 of the Cybercrimes Act requires them to establish and maintain sufficient human and operational capacity to detect, prevent and investigate cybercrimes. They are also responsible for collaborating with law enforcement in the investigation of cybercrimes. In some cases, this may entail the transfer of data and hardware.

Additionally, Williams *et al.* (2021) conclude that individuals must educate themselves and exercise extreme caution when communicating, especially on social media. Companies, particularly ECSPs and financial institutions, will need to implement training and compliance programmes to ensure compliance with the Cybercrimes Act (Williams *et al.*, 2021).

1.4 Cyber-related crimes

According to section 1 of the Cybercrimes Act, an "article" is defined as any data, computer program, computer data storage medium, or computer system that is concerned with, connected to, or reasonably believed to be concerned with the commission or suspected commission of an offence. The definition further includes any such item that may afford evidence of the commission or suspected commission of an offence, or that is intended, or reasonably believed to be intended, to be used in the commission of an offence. The statutory definition therefore does not merely describe the technical components of an article, but specifically qualifies it in relation to criminal conduct, whether actual, suspected, or intended.

Section 2 of the Cybercrimes Act criminalises unlawful access. In terms of this provision, any person who unlawfully and intentionally accesses a computer system or computer data storage medium without authority, permission, or justification commits an offence. The section therefore establishes the foundational offence of unauthorised access, which applies irrespective of whether further harm results from the intrusion. By clearly prohibiting intentional access without lawful authority, section 2 provides the statutory basis upon which several other cyber-related offences are constructed.

The Cybercrimes Act introduces 20 new cybercrime offences and imposes cybercrime penalties (Williams *et al.*, 2021). It establishes overarching legal authority for dealing with cybercrime by defining how these offences must be investigated, which includes searching for, acquiring access to or seizing objects related to cybercrime (Williams *et al.*, 2021).

For purposes of this study we will focus on the following 4 of the 20 cybercrimes mentioned in the Cybercrimes Act, as these are the most pertinent to the subject of cybercrime:

- Cyber fraud.
- Cyber forgery and uttering.
- Cyber extortion.
- Corporate property theft.

The remaining offences mentioned in the Cybercrimes Act, should they be relevant to the study, are addressed in a subsequent chapter.

1.4.1 Cyber fraud

Section 8 of the Cybercrimes Act specifies that committing cyber fraud involves the unlawful and intentional making of a misrepresentation by a person. This may occur through the manipulation of, or interference with, data, computer programs, computer data storage media, or computer systems. Such actions must result in, or have the potential to result in, harm or the potential for harm to another individual.

1.4.2 Cyber forgery and uttering

Section 9 of the Cybercrimes Act outlines two specific offences. Firstly, it states that if a person unlawfully creates fake data or a false computer program with the intent to deceive, and this action causes or has the potential to cause prejudice to another person, then they are committing an act of cyber forgery. Secondly, the section clarifies that the unlawful transmission of false data or a

fake computer program, with fraudulent intent and causing, or having the potential to cause, detriment to another person, constitutes the offence of cyber uttering.

1.4.3 Cyber extortion

Cyber extortion is addressed in section 10 of the Cybercrimes Act, which criminalises the unlawful and intentional threat to commit an offence under the Act with the purpose of obtaining an advantage from another person or compelling a person to act or refrain from acting. This provision captures extortionate conduct where threats are used to coerce victims through digital means, including threats to unlawfully access, interfere with, or disclose data or computer systems.

In addition, section 11 of the Cybercrimes Act provides for aggravated offences where the underlying cybercrime involves a restricted computer system, and the perpetrator knew or ought reasonably to have known that the system was restricted. In such circumstances, the offence is elevated to an aggravated form due to the heightened risk and potential harm associated with interference in protected or critical systems. Accordingly, cyber extortion may constitute an aggravated offence only where the conduct falls within the specific circumstances set out in section 11, rather than by virtue of any offence under the Act.

1.4.4 Corporate property theft

Section 12 of the Cybercrimes Act clarifies that the common law offence of theft includes incorporeal property. This inclusion ensures that such property is protected under the definition of theft, highlighting that the Cybercrimes Act recognises the evolving nature of property in the digital age.

1.5 Problem statement

Social engineering attacks constitute a persistent and pervasive threat within digital environments. In South Africa, social engineering remains a significant risk to individuals, organisations, and institutional systems, as these attacks exploit human behaviour rather than technical vulnerabilities, thereby circumventing conventional security controls.

Extensive literature exists on the techniques used in social engineering, including phishing, pretexting, baiting, and impersonation. Organisations are generally aware of these risks, and legal frameworks such as the Cybercrimes Act provide a statutory basis for addressing cyber-enabled offences. However, despite this awareness and regulatory development, social engineering attacks continue to succeed at scale. This persistence suggests not a lack of knowledge, but a

gap in the integration and operationalisation of legal, behavioural, criminological, and technological responses.

A central problem therefore lies in the fragmented nature of current mitigation strategies. Defensive measures are often implemented in isolation, with technical safeguards, awareness training, and legal enforcement functioning as parallel rather than coordinated mechanisms. While specialised expertise exists within cybersecurity, forensic accounting, and law enforcement domains, interdisciplinary collaboration and behaviourally informed implementation remain inconsistent across organisational contexts.

The problem is not that social engineering is poorly understood in theory, but that existing knowledge is not always translated into cohesive and adaptive national and organisational strategies. This misalignment between legislative frameworks, behavioural science insights, offender profiling, and technical controls limits the effectiveness of prevention and response mechanisms.

Accordingly, there is a need for a critical, interdisciplinary examination of how social engineering attacks can be more effectively combatted within the South African context. This leads to the central research question: “How can social engineering attacks be combatted in South Africa?”

1.6 Research objectives

The research objectives are divided into a main objective and a set of secondary objectives that reflect the study’s interdisciplinary scope.

1.6.1 Main objective

The primary objective of this study is to examine the various types of social engineering attacks and evaluate the effectiveness of existing defence mechanisms designed to prevent and mitigate them.

This objective is addressed through a comprehensive evaluation of how social engineering attacks operate, the extent to which current legislative frameworks — such as the Cybercrimes Act and the ECTA — are equipped to mitigate these threats and whether law enforcement practices, psychological deterrents and technical safeguards are sufficiently aligned to counteract these attacks (empirical research objective).

1.6.2 Secondary objectives

As part of the process to achieve the main objective above, the secondary objectives of this study are:

- To critically identify and categorise the nature of social engineering attacks, examining the tactics used to exploit human and procedural vulnerabilities. This is addressed in Chapter 2 (theoretical research objective).
- To critically assess social engineering from legal, psychological, criminological and cybersecurity perspectives, with the aim of evaluating enforcement challenges, behavioural and technical vulnerabilities and proposing targeted recommendations. This interdisciplinary analysis is discussed in detail in Chapter 3 (theoretical research objective).

1.7 Research design and methodology

1.7.1 Paradigmatic assumptions

According to Khatri (2020:1435), the theoretical or philosophical foundation for research is referred to as the research paradigm and, therefore, considered a research philosophy. The researcher's thoughts and beliefs about any issues investigated would then guide their actions (Khatri, 2020:1436). It guides the researcher through the overall investigation process, which includes selecting a research problem, developing research questions, determining the nature and types of reality, knowledge, methodology and the value of the research study (Khatri, 2020:1436).

Therefore, the perspectives and assumptions that each paradigm employs to define reality, knowledge, methodological approaches and values are simply referred to as research paradigm components (Khatri, 2020:1436). The components of a research paradigm are ontology, epistemology, methodology and axiology (Khatri, 2020:1436).

In this section, the ontological, epistemological and methodological assumptions of the proposed research are discussed.

1.7.1.1 Ontological assumptions

Ontology is concerned with philosophical assumptions concerning the nature of reality or existence (Khatri, 2020:1436). According to Khatri (2020:1436), it is simply known as reality theory. Therefore, ontology is the philosophical perspective on the nature of existence or reality,

of being or becoming, as well as the fundamental categories of things that exist and their relationships (Khatri, 2020:1436).

This study aimed to analyse various social engineering attacks in South Africa and how to defend against them. This was achieved by, *inter alia*, reviewing peer-reviewed journal articles, reports, newspaper and magazine articles, laws and regulations.

1.7.1.2 Epistemological assumptions

Epistemology is another component of the research paradigm that deals with how knowledge is obtained from various sources (Khatri, 2020:1437). According to Khatri (2020:1437), it is used in research to describe how researchers come to know something, how they know the truth or reality.

Furthermore, it is concerned with the very foundations of knowledge – its nature, forms and acquisition, as well as how it can be communicated to other people (Khatri, 2020:1437). It focuses on the types of human knowledge and comprehension so that, as a researcher, they may be able to acquire, extend, broaden and deepen understanding in their field of study (Khatri, 2020:1437).

The information gathered from the aforementioned sources was rigorously examined to ascertain the best ways to defend against the various social engineering attacks. This study is, therefore, based on current literature and local statutory laws.

1.7.1.3 Methodology

It is assumed that methodological considerations in a paradigm simply include participants, data collection instruments and data analysis measures through which knowledge about the research problem is gained (Khatri, 2020:1437). The methodology articulates the logic and flow of the systematic processes employed to gain knowledge about a research problem during a research project (Khatri, 2020:1437). It describes the assumptions made, the limitations encountered and how they were mitigated or minimised (Khatri, 2020:1437).

The researcher analysed the interpretations regarding the critical analysis of combatting social engineering attacks in South Africa. The researcher then identified patterns across all the assumptions made and developed a general theory regarding the manner in which forensic accounting practitioners conceptualise the problem addressed in this study.

1.7.2 Literature study

This dissertation constitutes a literature review. The advancement of knowledge must inherently be grounded in previously completed work (Xiao & Watson, 2019:93). To extend the knowledge frontier, researchers must first establish its current boundaries (Xiao & Watson, 2019:93). Researchers understand the breadth and depth of the existing body of work and identify gaps to investigate by reviewing relevant literature (Xiao & Watson, 2019:93). They can test a specific hypothesis and develop new theories by summarising, analysing and synthesising a group of related literature (Xiao & Watson, 2019:93).

Keyword searches were carried out for this literature study. Electronic databases were searched, focusing on literature that pertained to social engineering with the following search keywords: social engineering, social engineering attacks, phishing, cybercrime and cybersecurity. The search was limited to papers published within a certain time frame from the time of writing.

Following that, a content analysis was performed to determine what will be used to support this study. Accordingly, this study conducted a critical review of combatting social engineering attacks. Consequently, this chapter presents theoretical insights and hypotheses advanced in the literature.

1.7.3 Critical literature review

According to Xiao and Watson (2019:93), literature reviews, as scientific investigations, should be valid, reliable and repeatable. Social engineering literature lacks rigorous systematic reviews, partly attributable to insufficient discussion of literature review methodology and inadequate guidance regarding effective review conduct (Xiao & Watson, 2019:93).

The literature review is guided by the research problem statement and provides the basic direction for the current study. The review is structured to first consider studies that address the *modus operandi* of social engineering attacks. Thereafter, studies that address the relevant South African legislation, including the Cybercrimes Act, relevant to the combatting of social engineering attacks, were considered. The synthesis of findings from multiple studies yields a more robust and precise assessment than an individual study in isolation.

The study intends to provide a critical review of combatting social engineering attacks. During this review, primary and secondary data sources were consulted to address the research objectives and therefore respond to the related research questions. This was accomplished using literature from a variety of sources, including but not limited to peer-reviewed journal articles, reports, newspaper and magazine articles, laws and regulations and government publications.

1.8 Ethical considerations

The requirement to consider ethical considerations was noted and was kept in consideration as the study progressed.

This study did not have any human participants or human interaction; therefore, there was limited or no ethical risk involved.

1.9 Chapter overview

Chapter 1: Purpose, scope and outline of the study

This chapter introduced the study by presenting the background, motivation and context underpinning the research on social engineering attacks. It outlined the research problem, objectives and methodology and provided an overview of the structure and scope of the chapters that follow.

Chapter 2: Identifying social engineering attacks: A critical analysis (Article 1)

This chapter critically analyses the *modus operandi* of social engineering attacks, with the objective of identifying, classifying and comparing the primary attack types employed by cybercriminals. This chapter employs a systematic review to explore nine major social engineering attack types. These include phishing, pretexting, baiting, smishing, vishing, *quid pro quo*, tailgating, watering hole and social media manipulation. By analysing their psychological underpinnings and operational methods, the chapter identifies common behavioural and technological patterns that define these attacks. It integrates Cialdini's Six Principles of Influence to explain how human cognitive biases are exploited and relates these attack types to financial fraud trends such as pig butchering, synthetic identity fraud and AI-enabled deception. The insights derived provide a comprehensive understanding of how social engineering operates in practice and form a conceptual foundation for the interdisciplinary and legal analysis presented in the subsequent chapter. Accordingly, this article addresses the first component of the secondary research objectives outlined in Section 1.7.2.

Chapter 3: Identifying social engineering attacks: A critical analysis of legal, psychological, criminological and cybersecurity perspectives (Article 2)

Building upon the behavioural and operational foundations established in Chapter 2, this chapter adopts an interdisciplinary analytical framework encompassing legal, psychological,

criminological and cybersecurity perspectives. It examines how these four domains integrate to inform both the understanding and mitigation of social engineering attacks. Special emphasis is placed on the legal dimension, particularly South Africa's ECTA and the Cybercrimes Act, which provide statutory mechanisms for addressing such offences. The chapter demonstrates how these legal provisions interact with behavioural, criminological and technological insights to establish an integrated response to social engineering. It argues that while legislation forms the cornerstone of accountability and deterrence, it is only effective when supported by an informed human element, strong institutional culture and adaptive technical safeguards. Accordingly, this article addresses the second component of the secondary research objectives stated in Section 1.7.2 and collectively builds towards the final synthesis and recommendations presented in Chapter 4.

Chapter 4: Conclusion and recommendations

The concluding chapter synthesises the findings of both preceding articles, drawing together the legal, psychological, criminological and cybersecurity dimensions of the research. It provides a comprehensive conclusion to the central research question and offers evidence-based recommendations for enhancing the prevention, detection and prosecution of social engineering attacks.

CHAPTER 2 ARTICLE 1

Identifying social engineering attacks: A critical analysis

Journal details: Journal of Financial Crime

ISSN: 1359-0790

Emerald Publishing

Identifying social engineering attacks: A critical analysis

Abstract

Purpose – Social engineering is a prominent aspect of online crime. The global daily use of the internet increases the likelihood of data theft by cybercriminals owing to the greater availability of user data, which enables cybercriminals to gain unauthorised access to sensitive and personal information. This paper provides an in-depth analysis of the various types of social engineering attacks, aiming to offer insights into effectively identifying the underlying motives behind them.

Design/methodology/approach – The paper revisits the literature to understand social engineering, particularly through an analysis of the types of attacks. Common underlying factors are identified, forming a foundational understanding of the specific types of social engineering attacks. The research develops evidence based on theoretical underpinnings to enhance the comprehension of key social engineering attacks. Conclusions are drawn from the literature.

Findings – The study identifies the types of social engineering attacks, supported by extensive literature. This knowledge enables individuals to identify social engineering attacks by increasing their awareness of the different methods cybercriminals employ to exploit personal information.

Originality/value – This paper adds to current research regarding the types of social engineering attacks. It thoroughly examines each attack type, detailing the methods employed and thereby enhancing the understanding of the intentions and strategies used by cybercriminals.

Keywords – Social engineering, phishing, cybercrime, social engineering attacks, social engineering attack types

Paper type – Systematic review

2.1 Introduction

The rapid development of emerging technologies and digital environments has made the threat posed by social engineering increasingly severe (Wang *et al*., 2021). As technology continues to advance, new and more sophisticated forms of social engineering attacks are likely to emerge, posing a significant security risk to individuals and organisations (Parthy & Rajendran, 2019). The widespread adoption of internet-based services has made it increasingly difficult for individuals to safeguard their private data, exposing vulnerabilities that cybercriminals can exploit (Abdulla *et al.*, 2023).

Social engineering is a widely employed method for extracting sensitive information from targeted individuals, leveraging human error to gain unauthorised access to confidential data (Abdulla *et al.*, 2023). Despite its longstanding presence in the cybersecurity landscape, defending against social engineering remains challenging due to inherent human limitations and susceptibility to manipulation (Parthy & Rajendran, 2019). For example, a cybercriminal may distribute a fraudulent email containing a malicious link; once clicked, the victim unknowingly compromises their personal or organisational data (Abdulla *et al.*, 2023).

The severity of social engineering attacks lies in their ability to exploit the psychological and behavioural tendencies of human decision-making (Parthy & Rajendran, 2019). Cybercriminals employ persuasive techniques to manipulate victims into complying with their demands (Parthy & Rajendran, 2019; Jones *et al.*, 2021), making such attacks a significant and pervasive threat.

The increasing prevalence of social engineering attacks is exemplified by the fraud trends observed in 2024, where cybercriminals have exploited psychological manipulation to orchestrate large-scale financial crimes. Notably, pig butchering, deepfakes and account takeovers demonstrate the sophisticated application of social engineering techniques in financial fraud (Staiger, 2024). The continued advancement of AI has further enabled fraudsters to refine their tactics, making their deception more convincing and difficult to detect (Staiger, 2024). These real-world cases underscore the urgency of understanding social engineering methodologies and their implications for cybersecurity, financial integrity and risk mitigation strategies.

This study aims to analyse the types of social engineering attacks and how cybercriminals exploit personal information through deception. Given the increasing diversity and complexity of these attack methods, a comparative analysis is necessary to systematically identify their distinguishing features, overlapping tactics and relative threat levels. In order to address this issue comprehensively, it is essential to establish a foundational understanding of social engineering. Accordingly, this study examines various social engineering attacks and provides an in-depth

analysis of their distinct characteristics and operational methodologies. Each attack is contextualised within contemporary cybersecurity threats, offering insights into how cybercriminals manipulate individuals and organisations through behavioural and technological means. This critical comparison of attack methods highlights both shared and unique vulnerabilities across different vectors, thereby enhancing awareness and informing the development of more nuanced and effective countermeasures in the digital age.

As internet usage continues to expand across individual and organisational domains, there has been a significant increase in data breaches and cybercrime incidents (Abdulla *et al.*, 2023). Emerging technologies such as AI and machine learning are expected to further enhance the sophistication and effectiveness of social engineering attacks (Wang *et al.*, 2021). Although this study focuses on combatting social engineering attacks through prevention, detection and investigation, heightened cybersecurity concerns are also likely to prompt further research and encourage the secure deployment of advanced technologies to mitigate these risks (Parthy & Rajendran, 2019).

Currently, there is limited publicly available research that comprehensively addresses the evolving landscape of social engineering. Indeed, to the author's knowledge, this study is among the first to systematically examine the interplay between social engineering techniques, emerging fraud trends and the role of AI in advancing these attacks. Many existing sources on the subject are relatively outdated, reflecting a gap in contemporary research. This study integrates key findings, academic perspectives and recent developments in social engineering to bridge this gap, thereby contributing to the advancement of cybersecurity and forensic knowledge, particularly in the detection, prevention and investigation of cybercrime, including fraud.

This research presents a thorough analysis of social engineering, including the psychological tactics employed by cybercriminals and the various methods used to exploit victims. The article comprises three main sections: Section 2 introduces social engineering attacks as an escalating cybersecurity concern; Section 3 outlines the research methodology adopted in this study; and Section 4 presents the core analysis. Section 4 is further divided into four subsections: an in-depth exploration of social engineering (4.1), its conceptual foundation (4.2), the underlying motivations of cybercriminals (4.3) and a classification of key social engineering attack types (4.4). A comparative analysis of these attacks is presented in Section 4.5, highlighting their distinct characteristics and methods of exploitation. Finally, Section 5 concludes the article by summarising the key research contributions and offering recommendations for future investigative and defence strategies against social engineering threats.

2.2 Rising threat of social engineering attacks

The increasing frequency of security breaches can primarily be attributed to cybercriminals targeting the most vulnerable aspect of security systems: the human user (Albladi & Weir, 2018b). Human error remains a primary contributing factor to these breaches, as individuals frequently introduce weaknesses that cybercriminals can exploit (Goel & Jain, 2018:527). This persistent vulnerability underscores the importance of addressing social engineering attacks, which manipulate psychological tendencies rather than technical vulnerabilities to achieve malicious objectives. As these attacks continue to evolve, cybercriminals are expected to refine their methods, making them increasingly difficult for individuals and organisations to detect and mitigate (Chen *et al.*, 2020).

The 2024 fraud landscape demonstrates how cybercriminals increasingly leverage AI tools to enhance the sophistication of social engineering attacks, distorting the distinction between human-led and machine-driven deception. Fraudsters now employ AI-driven techniques to generate hyper-realistic phishing scams, automate deception tactics and create synthetic identities to conduct financial fraud. For instance, deepfake scams utilise AI-generated video and voice recordings to impersonate corporate executives, successfully deceiving employees into authorising fraudulent transactions (Staiger, 2024). Similarly, pig butchering scams exploit AI-powered chatbots to fabricate long-term relationships with victims, ultimately coercing them into transferring substantial sums to fraudulent investment platforms (Staiger, 2024). These advancements highlight the growing complexity of social engineering attacks and underscore the urgent need for enhanced cybersecurity strategies to mitigate their impact.

The adaptive and dynamic nature of social engineering presents a formidable challenge in cybersecurity. These attacks exploit human behaviours and cognitive biases to circumvent traditional security measures, rendering technical safeguards insufficient. Effectively mitigating this growing threat necessitates a deeper understanding of both the operational methods employed by cybercriminals and their underlying motivations. Without such a comprehensive understanding, cybersecurity efforts may prove inadequate, leaving individuals and organisations vulnerable to data breaches, financial losses and reputational damage.

Furthermore, the absence of robust legislation specifically addressing social engineering attacks presents a significant challenge. Cybercriminals face minimal deterrents due to limited legal frameworks and a general lack of public awareness, allowing these attacks to evolve into a persistent and increasingly sophisticated threat (Wang *et al.*, 2021). The lack of legal enforcement mechanisms enables social engineering to proliferate unhindered, further emphasising the necessity for targeted research and legislative intervention.

A comprehensive analysis of social engineering attacks is essential for several reasons. Not only does it enhance understanding of the specific methodologies and motivations behind these attacks, but it also facilitates the development of proactive countermeasures. This research aims to provide practical insights to inform organisational security policies, legislative responses and public awareness campaigns by identifying the core techniques used by cybercriminals. Additionally, such analysis provides a foundation for future research to explore emerging threats and innovative solutions to combat the evolving social engineering landscape.

This study contributes to the broader cybersecurity discourse by examining the operational dynamics of social engineering attacks. Through a detailed exploration of these methods, it offers critical insights into how cybercriminals exploit human vulnerabilities, equipping individuals, organisations and policymakers with the knowledge needed to develop robust and evidence-based defence strategies.

2.3 Research methodology

This study employs a systematic review, drawing upon peer-reviewed journal articles, case studies, academic dissertations and government reports. The primary focus is on the various forms of social engineering attacks, with particular emphasis on understanding the interplay between manipulation techniques, emerging fraud trends and the role of AI in enabling more sophisticated deception. The methodology involved a rigorous and structured evaluation of sources, following predefined inclusion and exclusion criteria to identify recurring patterns, tools and behavioural tactics commonly associated with social engineering. This ensured that the study's findings are based on an extensive, transparent and methodologically sound examination of the existing literature.

The systematic review followed established academic protocols, including:

- Research question formulation: Focused on identifying key methods, techniques and evolving patterns in social engineering attacks.
- Inclusion/exclusion criteria: Limited to peer-reviewed articles, case studies, theses and official reports addressing specific social engineering methods or technological enablers.
- Database search: Conducted via WorldCat Discovery, IEEE Xplore and Google Scholar using keywords such as social engineering attacks, phishing, baiting and AI and cybercrime.
- Screening and selection: Sources were evaluated for relevance and methodological rigour. Generic cybersecurity studies without a clear social engineering focus were excluded.

- Thematic analysis: Selected texts were coded to extract recurring tactics, psychological manipulation techniques, victim vulnerabilities and trends such as AI-driven deception and deepfakes.

This approach ensured that the review is comprehensive, replicable and evidence-based, supporting a comprehensive understanding of how social engineering attacks function in modern digital environments. The appropriateness of using a systematic review in this context is supported by studies such as:

- Mouton *et al*. (2016:45) conducted a systematic classification of social engineering attacks to develop a conceptual ontological model.
- Albladi and Weir (2018a:148) used a structured review to analyse risk factors for deception in online communication.

The collected data were systematically categorised and analysed thematically, allowing for the identification of similarities and distinctions across attack types. An in-depth comparative discussion was essential to this process, as it enabled the study to differentiate between techniques (e.g., phishing, baiting, vishing, smishing), highlight shifts in attack sophistication and reveal how AI and automation are transforming attacker strategies. This degree of comparison is necessary to fulfil the central objective of the study — to critically identify and assess the nature and evolution of social engineering attacks — and to equip organisations and individuals with a more nuanced understanding of how these attacks function in real-world contexts.

The following section begins with a conceptual overview of social engineering in Sections 4.1 and 4.2, establishing the theoretical foundation for the comparative analysis presented in Section 4.5. It proceeds to explore the motivations driving cybercriminals in Section 4.3, followed by a detailed evaluation of the key social engineering attack types in Section 4.4. Together, these components illustrate how each method uniquely exploits human or system-based vulnerabilities, providing critical insight into the evolving nature of deception-based cyber threats.

2.4 The dynamics of social engineering attacks — Methods, motivations and emerging threats

2.4.1 Overview of social engineering

This section provides a thorough overview of social engineering, examining the motivations behind such attacks and detailing the various methods employed by cybercriminals. Each attack type — phishing, pretexting, deepfake, business email compromise (BEC), baiting, smishing, vishing, *quid pro quo*, tailgating, watering hole attacks and social media manipulation —

represents a distinct technique used to exploit human vulnerabilities. A systematic analysis of these tactics is essential for understanding their methodologies and the broader risks they pose to individuals and organisations.

Central to the effectiveness of social engineering is the exploitation of psychological and behavioural tendencies. This analysis identifies the key traits that make individuals susceptible to manipulation, revealing how social engineering tactics frequently bypass technical security controls. Cybercriminals manipulate victims into revealing sensitive information or granting unauthorised access by leveraging deception, perceived authority and emotional triggers such as trust, urgency or fear. Recognising the recurring patterns and psychological hooks within these attacks is vital for the development of robust risk assessment frameworks and mitigation strategies.

Recent fraud reports underscore the increasing role of social engineering in contemporary cybercrime. In 2024, schemes such as account takeovers and new account fraud emerged as dominant threats, often facilitated through phishing, pretexting and synthetic identity fraud (Staiger, 2024). Cybercriminals exploit stolen or fabricated credentials to gain access to banking systems, execute fraudulent transactions and create fictitious profiles to obtain credit. Pig butchering scams, in particular, combine multiple social engineering methods, including long-term trust-building via digital platforms, to lure victims into fraudulent cryptocurrency investments (Staiger, 2024).

The sophistication of these attacks has been significantly amplified by advancements in AI. AI-powered tools enable fraudsters to automate deceptive interactions, generate deepfake audio and video content and sustain long-term manipulation campaigns with minimal effort (Staiger, 2024).

These developments make it increasingly difficult to distinguish between human and machine-driven deception, further complicating detection and response efforts. The integration of social engineering with emerging technologies highlights a critical nexus between psychological exploitation and financial crime, underscoring the urgent need for adaptive cybersecurity strategies, advanced detection mechanisms and comprehensive public awareness initiatives.

2.4.2 Conceptual foundation of social engineering

Social engineering relies on establishing trust between the attacker and the target. The first recorded phishing attack was reported in 1995, when cybercriminals manipulated victims into disclosing their confidential information through fraudulent emails (Alabdan, 2020:1). The

evolution of internet technologies has brought with it concerns over cybersecurity risks, particularly the growing vulnerability of users to psychological manipulation (Salloum *et al.*, 2022:65703). The global connectivity of the internet enables real-time communication across borders, yet it also provides an expansive platform for cybercriminals to exploit human vulnerabilities (Koops, 2011:737).

At its core, social engineering relies on psychological manipulation to deceive individuals into performing actions or revealing confidential information (Li, Wang & Horkoff, 2019; Goel & Jain, 2018:527). This form of cybercrime has become increasingly effective, as sensitive personal data has become a prime target for exploitation (Abdulla *et al.*, 2023). Rather than attacking security systems directly, cybercriminals target individuals with access to critical information, using deception to bypass technological defences (Wang *et al.*, 2021; Bullée *et al.*, 2015).

Cybercriminals manipulate human behaviour by exploiting innate psychological tendencies and cognitive biases that influence decision-making. Central to this manipulation are Cialdini's (2007) Six Principles of Influence, which serve as foundational tools in the cybercriminal's arsenal. These include *Reciprocity*, which prompts individuals to return favours; *Commitment and Consistency*, which capitalise on people's desire for behavioural alignment; *Social Proof*, which leverages the inclination to follow others' actions; *Authority*, which plays on deference to figures of power; *Liking*, which exploits familiarity and friendliness; and *Scarcity*, which increases perceived value through limited availability (Cialdini, 2007). Although these principles are not inherently harmful, in the hands of cybercriminals, they become powerful tools for deception (Cialdini, 2007; Savitz, 2012).

The Colorado Department of Education (2020) highlights the centrality of these psychological principles in social engineering, emphasising that attackers frequently employ tactics such as pretexting (masquerading as someone else), baiting (offering something of value), blackmail (threatening disclosure) and *quid pro quo* (offering a service in exchange for information). Understanding the psychological underpinnings of these strategies is critical to developing effective countermeasures.

Modern social engineering attacks have grown increasingly sophisticated. Cybercriminals use publicly accessible data from social media and online platforms to refine their approaches (Abdulla *et al.*, 2023), often deploying phishing websites that closely resemble legitimate platforms to capture login credentials, financial data and other sensitive information (Doke *et al.*, 2020). Impersonation techniques, such as phone calls or emails from fraudsters posing as trusted insiders, further enhance the credibility of their deceptions (Wang *et al.*, 2021).

Recent fraud trends demonstrate the evolving nature of social engineering. Cybercriminals are increasingly leveraging AI and deepfake technologies to execute convincing and large-scale attacks (Staiger, 2024). For example, AI-powered phishing scams and deepfake campaigns utilise synthetic audio and video to impersonate executives, misleading employees into authorising fraudulent transactions. Pig butchering scams further exemplify this trend, using AI-driven chatbots to build long-term trust with victims before coercing them into fraudulent cryptocurrency investments (Staiger, 2024). These developments highlight the urgent need for heightened cybersecurity awareness and sophisticated investigative capabilities to detect and mitigate such threats.

Despite the emergence of advanced security protocols, cybercriminals continue to adapt their tactics. This adaptability has contributed to a steady rise in social engineering-related breaches (Albladi & Weir, 2018b). Fraudsters often entice victims with misleading incentives, a tactic widely observed in investment fraud schemes, cryptocurrency scams and government impersonation cases (Abdulla *et al.*, 2023). The growing complexity and frequency of these attacks emphasise the necessity for dynamic, human-centric defence mechanisms.

Having established the conceptual foundation of social engineering and the psychological mechanisms underpinning these attacks, the following section explores the motivations that drive cybercriminals to engage in such deceptive practices.

2.4.3 Motives of cybercriminals

Social engineering is, at its core, the art of manipulating the human mind, an approach that is often far more accessible to cybercriminals than identifying and exploiting software vulnerabilities (Savitz, 2012). It remains a highly attractive method due to its ability to circumvent technological defences such as firewalls by targeting human vulnerabilities instead (Hijji & Alam, 2021). Rather than attacking system architecture directly, social engineers exploit trust and psychological predispositions to extract sensitive information or prompt actions that compromise organisational security (Li, Wang & Horkoff, 2019).

Unlike technical attacks that rely on coding expertise, social engineering relies on behavioural manipulation. The success of an attack often depends on the persuasiveness of the tactic, which can range from attention-grabbing social media posts to tailored emails referencing company operations or personal interests (Savitz, 2012). These tactics are fuelled by cybercriminals' motivations, which commonly include fraud, identity theft and corporate espionage (Hijji & Alam, 2021).

Goel and Jain (2018:527) outline several key motives behind social engineering attacks:

- Financial gain: Obtaining login credentials to access victims' financial accounts.
- Selling personal information: Harvesting and trading sensitive data for profit.
- Identity theft and fraud: Using stolen or synthetic identities to obtain financial benefits.
- Defamation and corporate sabotage: Spreading misinformation to harm reputations or disrupt operations.
- Exploiting security gaps: Identifying and leveraging vulnerabilities to launch further attacks.
- Status and recognition: Achieving notoriety within underground cybercriminal networks.

These motivations are clearly reflected in recent fraud trends. In 2024, schemes such as pig butchering emerged as complex, multi-layered scams that combined elements of romance fraud and investment deception. According to Staiger (2024), victims are manipulated into forming emotional relationships with fraudsters who, over time, persuade them to invest substantial sums into fraudulent cryptocurrency platforms. Similarly, synthetic identity fraud enables large-scale financial crimes by using fictitious identities constructed from a combination of real and fabricated personal data (Staiger, 2024). These synthetic identities are then used to obtain credit, loans or financial services, often without raising suspicion or detection.

These examples illustrate how cybercriminals continuously refine their techniques to exploit both psychological weaknesses and systemic gaps. As social engineering becomes increasingly sophisticated, it is essential to understand not only the motivations behind such attacks but also the specific methods used to execute them. The following section explores these attacks in greater detail.

2.4.4 Types of social engineering attacks

Social engineering attacks can generally be categorised into two primary forms: human-based, which involve direct interaction with the victim; and computer-based, which exploit digital systems or networks (Abdulla *et al.*, 2023; Ye *et al.*, 2020). While this classification offers a useful conceptual framework, the present study does not adhere strictly to these categories. Instead, it adopts an integrated approach to examine various social engineering methods (see different tables below), allowing for a more holistic understanding of their execution and implications.

This extensive approach facilitates a clearer analysis of the unique features and commonalities among different attack types. The study identifies core psychological and operational mechanisms that enable their success by evaluating these tactics collectively. Such an analysis

is vital for informing the development of effective mitigation frameworks and improving resilience against future attacks.

Recent fraud trends underscore the continuing reliance on social engineering in large-scale cybercrime operations. As financial fraud schemes evolve, they increasingly incorporate sophisticated social engineering techniques to exploit human and systemic vulnerabilities. For instance, account takeovers and new account fraud often employ phishing, pretexting and synthetic identity fraud to obtain unauthorised access to financial systems (Staiger, 2024). Deepfake scams leverage AI-generated video and voice recordings to impersonate senior executives, thereby deceiving employees into authorising large financial transfers (Staiger, 2024).

Another notable example is the pig butchering scam, which combines elements of romance fraud, social media manipulation and investment fraud. These schemes typically involve cultivating long-term trust with victims through digital interaction before coercing them into investing substantial sums into fraudulent cryptocurrency platforms (Staiger, 2024). Such attacks demonstrate the adaptability and escalating sophistication of social engineering techniques, underscoring the need for targeted awareness programmes, robust authentication protocols and advanced detection systems.

In order to provide a comprehensive analysis of the various social engineering attacks, each major attack type is discussed in its own subsection. The following tables present definitions, objectives, tactics, targets, technological enablers, risks and recommended countermeasures for each type. This structured approach facilitates a comprehensive understanding of the nuanced differences between various social engineering attacks.

Please note that in all the tables below, the *Definition and Use of Technology* columns are based on referenced academic literature drawn from the cited sources listed. The columns titled P*rimary Objective, Tactics Used, Targets, Challenges / Risks and Countermeasures* are derived from the authors' synthesis and analysis of the reviewed literature. These sections consolidate observed patterns, typical attack methodologies and industry best practices based on the full context of the study, rather than citing individual works for each entry.

2.4.4.1 Phishing

Phishing remains one of the most pervasive forms of social engineering, targeting users through deceptive digital communications to obtain sensitive information. Table 2.1 below presents an overview of phishing attacks, highlighting their defining characteristics, primary objectives, common tactics, targets, technological components, associated risks and mitigation strategies.

Table 2-1: Overview of Phishing Attacks

Aspect	Description
Attack type	Phishing
Definition	Fraudulent attempts to steal identity and private information by impersonating legitimate entities (Doke *et al.*, 2020; Fakieh & Akremi, 2022; Jakobsson, 2016; Mattera & Chowdhury, 2021; Abdulla *et al.*, 2023).
Primary objective	Obtain private credentials or install malware.
Tactics used	Deceptive emails or messages with links to spoofed websites; impersonation of trusted organisations.
Targets	Users with limited cybersecurity awareness, banking and financial service customers.
Use of technology	Generative AI for realistic emails, deepfake voices and synthetic personas (Staiger, 2024; Colorado Department of Education, 2020).
Challenges/Risks	Highly convincing attacks that bypass technical defences; expanded to multi-channel approaches.
Countermeasures	Public awareness, digital literacy and advanced real-time detection technologies.
Cialdini's Principles of Influence Exploited	Authority, scarcity and social proof (Cialdini, 2007).

Source: Author's own compilation

2.4.4.2 Pretexting

Pretexting is a sophisticated social engineering method that relies on constructing fabricated identities or scenarios to manipulate victims. Table 2.2 below outlines the core aspects of pretexting attacks.

Table 2-2: Overview of Pretexting Attacks

Aspect	Description
Attack type	Pretexting
Definition	Fabrication of false identities or scenarios to manipulate victims into disclosing confidential information (Colorado Department of Education, 2020; Fakieh & Akremi, 2022; Parthy & Rajendran, 2019).
Primary objective	Build trust to elicit sensitive information or coerce systems to compromise.

Aspect	Description
Tactics used	Assume roles such as IT technicians, contractors and executives; leverage publicly available information.
Targets	Employees, customers and the general public, particularly those trusting institutional authorities.
Use of technology	Exploitation of social media, directories and AI to gather reconnaissance data (Syafitri *et al.*, 2022).
Challenges/Risks	Highly credible scenarios; impersonation of real individuals raises detection risks.
Countermeasures	Organisational awareness programmes and verification training.
Cialdini's Principles of Influence Exploited	Authority, commitment and consistency (Cialdini, 2007).

Source: Author's own compilation

2.4.4.3 Baiting

Baiting attacks exploit human curiosity or greed by offering enticing items or opportunities that ultimately compromise security. Table 2.3 below summarises the characteristics of baiting attacks.

Table 2-3: Overview of Baiting

Aspect	Description
Attack type	Baiting
Definition	Exploitation of human curiosity or greed through enticing offers to facilitate cybercrime and compromise security (Colorado Department of Education, 2020; Fakieh & Akremi, 2022; Watson, Mason & Ackroyd, 2014).
Primary objective	Trick individuals into installing malware or disclosing information.
Tactics used	Malicious files disguised as updates/documents; infected USB devices; fraudulent investment opportunities.
Targets	Employees, the general public and users interacting with unknown devices or offers.
Use of technology	Malware embedded in phishing emails, USBs and pirated software (Ozkaya, 2018).
Challenges/Risks	Infection can occur without the user's suspicion; rapid malware spread.

Aspect	Description
Countermeasures	Awareness campaigns on external device risks; device usage policies.
Cialdini's Principles of Influence Exploited	Curiosity (linked to Scarcity) and reciprocity (Cialdini, 2007).

Source: Author's own compilation

2.4.4.4 Smishing

Smishing employs deceptive SMS messages to lure victims into providing sensitive personal or financial information. Table 2.4 below details the key elements of smishing attacks.

Table 2-4: Overview of Smishing Attacks

Aspect	Description
Attack type	Smishing
Definition	Phishing executed through deceptive SMS messages (Parthy & Rajendran, 2019; Fakieh & Akremi, 2022; Bennett, 2023).
Primary objective	Trick individuals into revealing personal or financial information.
Tactics used	Impersonation of banks, tax authorities, or delivery services via SMS; urgent action requests.
Targets	Mobile phone users, particularly financial customers.
Use of technology	Spoofed SMS messages, fake login portals and mobile malware (Mishra & Soni, 2020).
Challenges/Risks	Trust in mobile communication is exploited; urgency escalates compliance.
Countermeasures	Education on mobile scams, use of verified communication channels.
Cialdini's Principles of Influence Exploited	Urgency, authority and scarcity (Cialdini, 2007).

Source: Author's own compilation

2.4.4.5 Vishing

Vishing attacks use telephone calls to impersonate trusted entities and manipulate victims into revealing confidential information. Table 2.5 below presents an overview of vishing attacks.

Table 2-5: Overview of Vishing Attacks

Aspect	Description
Attack Type	Vishing
Definition	Voice-based phishing attacks are conducted through telephone calls (Fakieh & Akremi, 2022; Jones *et al.*, 2021).
Primary objective	Obtain confidential information or prompt risky actions.
Tactics used	Impersonation of trusted figures (for example, bank agents and IT support); use of urgent or threatening scenarios.
Targets	Telephone users, employees and the general public.
Use of technology	Deepfake voice technology; stolen personal data (Staiger, 2024; Clark, 2024).
Challenges/Risks	Realistic voice mimicry; emotional manipulation under time pressure.
Countermeasures	Strong telephone verification protocols and training.
Cialdini's Principles of Influence Exploited	Authority, urgency and liking (Cialdini, 2007).

Source: Author's own compilation

2.4.4.6 Quid pro quo

Quid pro quo attacks offer seemingly legitimate services or rewards in exchange for confidential information. Table 2.6 below outlines the main characteristics of these attacks.

Table 2-6: Overview of Quid pro quo attacks

Aspect	Description
Attack type	Quid pro quo
Definition	Offers of services, benefits, or favours in exchange for sensitive information (Colorado Department of Education, 2020; Fakieh & Akremi, 2022).
Primary objective	Convince victims to disable security measures or disclose credentials, thereby enabling cybercrime.
Tactics used	Impersonation of IT technicians or financial service providers offering help or upgrades.
Targets	Employees seeking assistance or professional benefits.
Use of technology	Deepfake AI-assisted persona creation; professional-sounding pretexts (Staiger, 2024).
Challenges/Risks	Exploitation of reciprocity norms; believable offers.

Aspect	Description
Countermeasures	Staff education on unsolicited help offers; strict internal support protocols.
Cialdini's Principles of Influence Exploited	Reciprocity and Authority (Cialdini, 2007).

Source: Author's own compilation

2.4.4.7 Tailgating

Tailgating is a physical form of social engineering where unauthorised individuals gain access to restricted areas. Table 2.7 below illustrates the core aspects of tailgating.

Table 2-7: Overview of Tailgating Attacks

Aspect	Description
Attack type	Tailgating
Definition	Physical intrusion by following an authorised person into restricted areas (Fakieh & Akremi, 2022; Syafitri *et al.*, 2022).
Primary objective	Gain unauthorised access to secure environments.
Tactics used	Psychological manipulation; use of props; disguises (e.g., delivery personnel).
Targets	Employees in organisations with physical security measures.
Use of technology	Props, professional attire; possible surveillance.
Challenges/Risks	Exploits human politeness; physical systems may not log all entries.
Countermeasures	Strict access control enforcement; training to challenge unauthorised entries.
Cialdini's Principles of Influence Exploited	Liking, authority, commitment and consistency (Cialdini, 2007).

Source: Author's own compilation

2.4.4.8 Watering hole

Watering hole attacks involve compromising legitimate websites frequently visited by targets to distribute malware. Table 2.8 below details this attack vector.

Table 2-8 Overview of watering hole attacks

Aspect	Description
Attack type	Watering hole
Definition	Compromise of legitimate websites to infect visiting users with malware (Syafitri *et al.*, 2022; Ozkaya, 2018).
Primary objective	Obtain sensitive information or enable remote system surveillance.
Tactics used	Embed malware in trusted, high-traffic websites.
Targets	Regular visitors to professional, news and financial sites.
Use of technology	Web server exploits, malware payloads (Ye *et al.*, 2020).
Challenges/Risks	Users trust legitimate sites. Repeated exposure heightens risk.
Countermeasures	Secure website maintenance User education about latent web threats.
Cialdini's Principles of Influence Exploited	Social, proof and authority (Cialdini, 2007).

Source: Author's own compilation

2.4.4.9 Social media manipulation

Social media manipulation involves using publicly available information to craft personalised attacks. Table 2.9 below summarises the characteristics of these attacks.

Table 2-9: Overview of social media manipulation attacks

Aspect	Description
Attack type	Social media manipulation
Definition	Use of personal information shared on social media to target victims (Albladi & Weir, 2018b; Parker & Flowerday, 2020).
Primary objective	Craft personalised attacks or conduct identity theft and fraud.
Tactics used	Data mining, AI-generated fake profiles and manipulation via mutual connections.
Targets	Users of platforms such as Facebook, LinkedIn, Instagram and X (formerly Twitter).
Use of technology	Social media scraping tools, AI-generated personas (Staiger, 2024; McNealy, 2022).
Challenges/Risks	Oversharing and cognitive fatigue increase vulnerability.

Aspect	Description
Countermeasures	Privacy education, cautious sharing practices, vigilance towards fake profiles.
Cialdini's Principles of Influence Exploited	Liking, Social Proof, Commitment and Consistency (Cialdini, 2007).

Source: Author's own compilation

As outlined in the tables above, social engineering attacks employ diverse psychological and technological tactics to exploit human vulnerabilities. These comparative analyses establish a foundation for understanding how these attack methodologies continue to evolve and underscore the importance of adopting a multidimensional approach to prevention and mitigation.

The following section presents a comparative analysis of the identified social engineering attacks, highlighting key similarities, differences, patterns in their tactics, target selection and exploitation strategies.

2.5 Comparative analysis of social engineering attacks

In alignment with the first secondary research objective outlined in Section 1.7.2, this section presents a comparative analysis of the major forms of social engineering attacks identified in the literature. The purpose of this comparison is to highlight both the shared behavioural mechanisms and the distinct operational tactics that characterise each attack type. The preceding tables systematically examined nine principal categories — phishing, pretexting, baiting, smishing, vishing, *quid pro quo*, tailgating, watering hole and social-media manipulation — each illustrating how cybercriminals exploit different psychological triggers such as trust, curiosity, fear or urgency. The study identifies recurring human-factor vulnerabilities and attacker motivations through comparing these attacks, providing a foundation for understanding the common behavioural and technical patterns that inform effective prevention strategies.

Despite their diversity, a recurring theme across these strategies is their reliance on undermining human judgement rather than solely breaching technical systems. This insight underscores the necessity for countermeasures that integrate technological safeguards with structured behavioural reinforcement, targeted awareness initiatives and clearly articulated organisational policies. While many organisations have already incorporated social engineering awareness into internal disciplinary frameworks and issued employees with written guidance on information security practices, the persistence and escalation of attacks indicate that awareness alone is insufficient without contextual reinforcement and practical application.

Effective mitigation therefore requires more than periodic training sessions. Organisations must identify specific operational vulnerabilities within their own environments, such as departments handling high-value transactions, employees with privileged system access or personnel frequently engaging in external communication. Risk-based assessments can then inform tailored interventions, including simulated phishing campaigns for finance teams, executive impersonation scenario testing for senior management and structured debrief sessions following detected social engineering attempts. These measures not only educate individuals directly involved but also create institutional learning that benefits the broader organisation.

Furthermore, social engineering education should not be confined to corporate environments. Given the increasing exposure of younger individuals to digital platforms, foundational digital literacy and online safety education should be embedded within school curricula and community awareness programmes. Early education equips individuals with critical thinking skills that reduce susceptibility to manipulation and contribute to long-term societal resilience.

The comparative analysis presented in this section reveals the intricate and adaptive nature of social engineering attacks. Rather than exploiting solely technical vulnerabilities, these attacks primarily manipulate behavioural biases, emotional triggers and gaps in organisational or individual vigilance. The emergence of advanced technologies — such as deepfake generation, AI-driven persona creation and large-scale data harvesting through social media — has significantly amplified the credibility, reach and success rates of these attacks. Furthermore, the convergence of digital and physical threat vectors, as demonstrated by tailgating and quid pro quo scams, underscores the holistic and evolving nature of the threat landscape.

In order to facilitate a structured comparison, this study systematically categorised and evaluated nine distinct social engineering attack types across multiple analytical dimensions. The comparison was designed to illustrate how each attack type aligns with broader patterns of cyber-enabled fraud, particularly within the financial crime landscape. Specifically, the comparison considered:

- Their alignment with the Top 5 global fraud schemes reported by the Association of Certified Fraud Examiners (ACFE).
- Their involvement in key financial fraud typologies, including synthetic identity fraud, account takeovers and BEC.
- The extent to which each attack type integrates or is enhanced by AI-driven tools, such as deepfakes and digital impersonation technologies.

- Their association with broader deception-based trends, such as romance scams, cryptocurrency investment fraud and government impersonation schemes.

Table 10 (see below) presents the findings of this comparative analysis. It provides a cross-sectional view of how each social engineering method corresponds to major fraud categories and illustrates where AI and social manipulation techniques converge. This comparative framework enables a nuanced understanding of both the commonalities and unique risks posed by each method, supporting more targeted mitigation strategies across legal, technical and organisational dimensions.

2.5.1 Convergence of social engineering techniques and financial fraud trends

Table 2.10 below presents a targeted analysis of the relationship between prominent social engineering attack types and major financial fraud trends, drawing on data from the ACFE's 2024 insights. The table identifies which attack types are most commonly associated with leading fraud schemes, including synthetic identity fraud, account takeovers, new account fraud, BEC, romance scams (pig butchering) and fraudulent cryptocurrency investments. It also reflects the increasing use of AI tools, such as deepfakes and social media manipulation, which enhance the plausibility and impact of these attacks. In addition, the table maps the presence of government impersonation tactics, indicating how attackers increasingly conflate digital deception and perceived authority.

The table provides critical insight into how cybercriminals adapt their tactics to exploit emerging financial vulnerabilities and behavioural weaknesses through visually mapping each social engineering technique to specific fraud trends and identifying where AI is involved.

Table 2-10: Convergence of Social Engineering Techniques and Financial Fraud Trends

Type of SE	Top 5 Fraud Schemes (ACFE Insights)	Synthetic Identity Fraud	Account Takeovers	New Account Fraud	Business Email Compromise	Romance Scams (Pig Butchering)	Fraudulent Cryptocurrency Investments	Deepfakes	Government Impersonation
Phishing	*	✓	✓	✓	✓	✓	✓	✓	
Pretexting		✓	✓		✓	✓	✓	✓	✓
Baiting	*				✓		✓		
Smishing	*			✓		✓	✓		✓
Vishing					✓	✓		✓	✓
Quid pro quo	*								
Tailgating					✓				✓
Watering Hole									
Social Media Manipulation	*	✓	✓	✓		✓	✓	✓	✓
Note: * Indicates the use of AI engineering techniques in the respective social engineering attack.									

Source: Association of Certified Fraud Examiners (ACFE, 2024).

Critically, the analysis above demonstrates that no single defensive strategy is sufficient to address these evolving threats. Effective countermeasures must be multi-layered, incorporating technical safeguards, behavioural interventions, continuous awareness training and strong inter-agency collaboration. This study's structured evaluation of nine distinct social engineering attacks provides a foundation for the conclusions and recommendations in Section 5. The analysis outlines both the persistent challenges and strategic priorities forensic professionals, cybersecurity experts and policymakers face when seeking to combat increasingly sophisticated forms of deception

2.6 Conclusion

Building on the insights gained from this comparative analysis, the following conclusion synthesises the key findings of the study and demonstrates how the research has successfully met its objectives. Specifically, the study has critically examined the various types of social engineering attacks, explored their psychological and operational underpinnings and analysed their correlation with emerging fraud trends and the growing use of AI in cybercrime. In doing so, it provides a comprehensive understanding of how social engineering techniques are evolving and outlines the implications for detection, prevention and forensic investigation.

This study has examined the various types of social engineering attacks, highlighting their methods, psychological foundations and real-world implications. Through a qualitative approach, the research provides a comprehensive understanding of social engineering tactics, detailing the motives behind cybercriminals' use of these deceptive practices. This study has effectively identified and categorised each attack type through analysing different social engineering attacks, including phishing, pretexting, baiting, smishing, vishing, *quid pro quo*, tailgating, watering hole attacks and social media manipulation, explaining how cybercriminals exploit human vulnerabilities to achieve their objectives.

The rise in financial fraud observed in 2024 underscores the growing threat posed by social engineering in the digital age. High-impact schemes such as pig butchering, synthetic identity fraud and AI-enhanced phishing demonstrate how attackers leverage emerging technologies to execute increasingly complex and convincing deception campaigns. The integration of deepfake technology and generative AI into social engineering strategies has intensified the difficulty of detecting and preventing such attacks, challenging even the most robust security systems.

Considering these developments, the role of interdisciplinary expertise becomes increasingly essential. Cybersecurity professionals, forensic accountants, behavioural analysts and policymakers must work collaboratively to address the multidimensional threat posed by social engineering-based financial crime. Greater emphasis on behavioural forensics, AI-driven threat detection and targeted public awareness campaigns is needed to adapt to this evolving threat landscape. Moreover, in the context of minimal legal deterrence and limited public understanding, cybercriminals are enabled to continually refine their techniques. Legislative intervention, supported by cross-sector collaboration and global policy development, is imperative to enhance deterrence, improve accountability and establish a cohesive international response to this growing threat.

In closing, this research contributes to the growing body of cybersecurity literature by offering a detailed exploration of social engineering's psychological foundations, operational methods and emergent trends. It underscores the critical importance of understanding attacker motivations and victim susceptibilities to inform evidence-based defence strategies. Future research should focus on refining the classification of social engineering attacks, particularly by distinguishing between human-based and computer-based tactics, and developing advanced detection and response frameworks that support the prevention, investigation and forensic analysis of such attacks.

Given the increasingly complex nature of social engineering attacks, particularly with the integration of AI and the rise in financially motivated fraud, future research should also prioritise adaptive, interdisciplinary strategies to combat and anticipate emerging threats across digital environments. Critical areas for exploration include deepfake-enabled fraud, AI-assisted impersonation and the generation of synthetic identities, all of which signal the future trajectory of these attacks. Concurrently, the advancement of AI-driven detection systems, behavioural analytics and responsive legal frameworks will be vital in addressing the evolving nature of these attacks. Ultimately, it is only through a coordinated, multidisciplinary approach that the persistent and growing risks posed by social engineering can be effectively mitigated.

CHAPTER 3 ARTICLE 2

Identifying social engineering attacks: A critical analysis of legal, psychological, criminological, and cybersecurity perspectives

Journal details: Journal of Financial Crime

ISSN: 1359-0790

Emerald Publishing

Identifying social engineering attacks: A critical analysis of legal, psychological, criminological, and cybersecurity perspectives

Abstract

Purpose – This study aims to critically analyse the nature of social engineering attacks and examine how behavioural, legal, psychological, criminological and cybersecurity perspectives contribute to understanding and addressing this growing threat. It seeks to identify the underlying mechanisms of manipulation employed by cybercriminals and to evaluate the vulnerabilities they exploit, thereby supporting the development of holistic countermeasures.

Design/methodology/approach – The research adopts a qualitative methodology through a systematic literature review. This includes the analysis of peer-reviewed journal articles, academic dissertations and reports from trusted institutions. A multidisciplinary perspective is applied to investigate social engineering attacks, drawing on theoretical frameworks from law, psychology, criminology and cybersecurity. The study critically evaluates the various types of attacks, victim vulnerabilities and deception strategies and explores how emerging technologies such as artificial intelligence influence the evolution of these attacks.

Findings – There is a critical need to establish preventative measures to effectively prevent social engineering attacks. The study highlights various preventative techniques aimed at reducing these social engineering attacks while enhancing cybersecurity policies and practices.

Originality/value – This paper addresses a critical gap in the literature by providing an interdisciplinary analysis of social engineering attacks. While prior studies have focused on single-discipline approaches, this research offers a holistic examination that integrates legal, psychological, criminological and technical dimensions. The findings provide valuable insights for policymakers, cybersecurity professionals and organisational leaders seeking to support human and systemic defences against deception-based threats in an increasingly digital world.

Keywords – Cybercrime, criminological analysis, cybersecurity, legal frameworks, psychological manipulation, social engineering, social engineering attacks

Paper type – Critical review

3.1 Introduction and background

Social engineering remains one of the most effective and difficult to detect cybersecurity threats due to its reliance on manipulating human cognition and emotion rather than exploiting technical system vulnerabilities (Venkatesha *et al.*, 2021:8). While digital advancements have improved connectivity and efficiency, they have also facilitated criminal opportunities that are psychological and behavioural in nature, contributing to financial losses, societal instability and national security threats (Ramadani *et al.*, 2018:343). In the South African context, this convergence of human manipulation and digital exposure has contributed to an alarming rise in cybercrime, undermining trust in both public and private digital infrastructures and stalling economic growth.

Cybercriminals routinely exploit psychological triggers, such as fear, urgency, curiosity and empathy, to deceive users into performing harmful actions like clicking malicious links, sharing credentials or downloading infected files (Bishnoi *et al.*, 2023:685; Bitaab *et al.*, 2020:1). These actions often bypass technical safeguards entirely, leading to unauthorised access, data breaches, identity theft and legal or reputational consequences (Abe & Soltys, 2019:825). However, the threat extends beyond psychological manipulation alone. From a criminological standpoint, social engineering is driven by calculated offender behaviour, rooted in rational choice theory, opportunity structures and the low perceived risk of detection or prosecution. The success of these attacks often reflects deficiencies in law enforcement, insufficient deterrents and a lack of offender profiling within current institutional frameworks.

Contributing to this vulnerability are cognitive-behavioural factors such as poor cybersecurity literacy, unawareness of attack consequences, behavioural complacency and a lack of collective responsibility regarding digital security (Junger *et al.*, 2017:75). These factors are exacerbated by social dynamics, such as conformity bias and peer imitation, especially prevalent on social media platforms. The widespread use of digital and mobile technologies has intensified these challenges, increasing exposure to manipulative content, misinformation and deception campaigns (Murire *et al.*, 2021:1). Additionally, the rapid evolution of hacking techniques and the increasing availability of sophisticated cybercrime tools have made it more challenging to effectively combat social engineering attacks (Nicholls, Kuppa & Le-Khac, 2021:163966). As new attack vectors emerge, the criminogenic environments created by social networks like LinkedIn, Twitter, Facebook, Snapchat and WhatsApp provide significant opportunities for exploitation. This allows cybercriminals to gather intelligence, impersonate victims and build trust before launching attacks (Rathod *et al.*, 2025:2).

These attacks reflect interdisciplinary failures: psychological vulnerabilities are targeted through criminological insight, while legal enforcement lags behind the speed and creativity of technical

exploitation. For example, the commodification of personal data on digital platforms, coupled with poor regulatory oversight, enables large-scale profiling and manipulation. The inadequacy of technical protections, such as outdated firewalls or ineffective spam filters, is reflected by insufficient legislative enforcement, especially where the law fails to account for the behavioural intricacies of social engineering. Even when laws such as the *Cybercrimes Act 19 of 2020* (hereinafter referred to as "Cybercrimes Act") and the *Electronic Communications and Transactions Act 25 of 2002* (hereinafter referred to as the "ECTA") provide a regulatory basis for prosecution, challenges in evidentiary standards, jurisdictional enforcement and user awareness limit their practical effect (Zweni & Yan, 2022:36).

Cybercrime operates within a structured behavioural framework involving three interrelated elements:

- A victim, selected based on vulnerability and access.
- A motive, typically financial gain or exploitation of social capital.
- A vulnerability or opportunity, exploited through deception and trust violations (Bitaab *et al.*, 2020:2).

This tripartite structure reflects a convergence of criminological decision-making, psychological targeting, technological execution and legal ambiguity. Therefore, effective mitigation requires more than legal provisions; it necessitates coordinated responses across these four domains. While South Africa has taken important legislative steps, these must be met with behavioural resilience strategies, predictive criminological frameworks and adaptive cybersecurity infrastructure.

In conclusion, the persistent rise in social engineering attacks in South Africa demands a comprehensive interdisciplinary response. Laws must evolve to reflect behavioural science. Security programmes must account for psychological manipulation. Law enforcement must be trained in cyber-specific offender typologies. Technical systems must be integrated with user-focused education. Only through this synergistic approach can South Africa begin to reduce the impact of social engineering and build a resilient digital society.

3.1.1 The lifecycle of social engineering attacks

Social engineering attacks have become one of the most insidious and pervasive threats, leveraging the trust users place in digital resources. Cybercriminals manipulate emotional triggers such as greed, fear, empathy and curiosity, which can lead victims to unwittingly authorise access to sensitive personal and financial information (Rathod *et al.*, 2025:2; Junger *et al.*, 2017:77).

Consequently, safeguarding social media platforms against such attacks has become an increasingly urgent challenge, especially as social engineering is often the initial step in gaining unauthorised access to systems.

A typical social engineering attack progresses through several key stages:

- First, the investigation phase involves gathering publicly available data from social media profiles, job platforms and other digital traces to personalise the attack and increase its effectiveness.
- In the planning phase, cybercriminals develop strategies to exploit identified vulnerabilities, choosing the most convincing attack method, such as phishing or impersonation.
- During the contact phase, attackers reach out to their target using phishing emails, fraudulent phone calls or deceptive text messages to build trust and manipulate the victim into taking harmful actions.
- Finally, in the execution phase, attackers collect sensitive data such as login credentials or financial information or deploy malware, all while carefully avoiding detection from security systems (Rathod *et al.*, 2025:2).

Following this understanding of the lifecycle of social engineering attacks — where attackers methodically investigate, contact, manipulate and extract information from victims while avoiding detection — it becomes clear that no single layer of defence is sufficient. The multiphase nature of these attacks highlights the need for legislative interventions, such as South Africa's ECTA and Cybercrimes Act, to work in tandem with organisational policies and user-focused education initiatives. This clarity emerges from recognising that attackers exploit gaps not only in technology but also in legal enforcement and employee awareness. Therefore, a coordinated response is necessary: legislation establishes accountability, policies formalise procedures and education empowers individuals to identify and resist manipulation. Organisations will remain vulnerable to the sophisticated tactics employed by cybercriminals without this layered approach.

This lifecycle of a social engineering attack highlights the complex and multi-layered nature of these threats, emphasising the need for comprehensive organisational defences that combine technical controls with heightened user awareness. As users continue to engage extensively with social media platforms in both personal and professional capacities, the boundary between social interaction and cyber risk becomes increasingly distorted, demanding adaptive and proactive security strategies. Several key factors are discussed below, along with potential interventions to mitigate associated social engineering attacks.

3.1.2 Mitigation approaches for social engineering attacks

Social engineering attacks continue to pose significant threats to organisations by exploiting human psychology, organisational vulnerabilities and technological gaps. Addressing these attacks requires a multifaceted prevention strategy that integrates human-focused education, behavioural insights, technological defences and robust organisational policies. As attackers increasingly manipulate human emotions such as fear, urgency, curiosity and greed, a comprehensive approach is necessary to build resilience against evolving social engineering tactics (Salahdine & Kaabouch, 2019:11; Sethi, 2022:1031-1032).

A foundational element of social engineering prevention is strengthening organisational resilience by fostering a transparent and security-conscious culture. Rather than positioning education as a corrective response to individual shortcomings, research highlights the importance of continuous reinforcement, shared learning and visible organisational commitment to cybersecurity (Junger *et al.*, 2017:77). Social engineers exploit common human tendencies, including trust, routine behaviour and cognitive shortcuts. These vulnerabilities are universal rather than exceptional, and effective mitigation requires collective awareness rather than individual blame.

Accordingly, organisations should normalise discussions around social engineering incidents and near-misses, treating them as learning opportunities rather than failures. Open communication ensures that employees understand how attacks occur in real-world contexts and how behavioural manipulation unfolds in practice. By making social engineering attempts visible within the organisation, individuals are better equipped to recognise similar patterns in future interactions.

Furthermore, organisational culture plays a decisive role in shaping secure behaviour. Where productivity pressures dominate and security concerns are marginalised, employees may ignore warnings or replicate risky practices observed in peers (Junger *et al.*, 2017:77). A culture that actively encourages reporting, transparency and shared responsibility reduces stigma and strengthens collective vigilance.

To operationalise this approach, organisations should implement comprehensive cybersecurity awareness programmes that extend beyond theoretical instruction. These programmes should incorporate realistic phishing simulations, scenario-based exercises and contextual security guidance to develop practical judgement and critical thinking. Importantly, employees should be encouraged to report suspicious activities without fear of sanction, ensuring that reporting mechanisms function as tools for organisational learning rather than disciplinary control (Salahdine & Kaabouch, 2019:11). Regular awareness initiatives, dissemination of anonymised

incident examples and structured onboarding for new staff reinforce cybersecurity as an embedded organisational priority rather than a reactive obligation (Sethi, 2022:1031-1032).

Beyond human-centric interventions, technological defences are vital. The implementation of two-factor authentication (2FA) remains one of the most effective safeguards against phishing attacks, as it requires two forms of verification — typically a password and a physical device — which significantly reduces the likelihood of unauthorised account access (Fakieh & Akremi, 2022). In parallel, robust email security measures, such as encrypted gateways, spam filters and honeypot email accounts, play an essential role in blocking phishing emails and malicious attachments before they can reach end-users (Salahdine & Kaabouch, 2019:11). These systems should be regularly updated and integrated with real-time threat detection capabilities, such as AI-powered anomaly detection, which can identify malicious patterns and alert users to potential threats.

Physical security is widely recognised in the literature as an important layer of defence against social engineering tactics, particularly those involving physical intrusion or observation, such as tailgating, dumpster diving and shoulder surfing. Organisations should implement strict access control protocols, employ biometric verification, monitor facilities with video surveillance and train staff to challenge unauthorised individuals (Fakieh & Akremi, 2022). In high-security environments, advanced systems such as man-trap authentication and single-person turnstiles may be deployed to further prevent unauthorised entry (Watson, Mason & Ackroyd, 2014). Additionally, employees must be trained to securely dispose of sensitive documents and digital media, ensuring that confidential information cannot be retrieved from discarded materials.

Complementary to these strategies, research highlights the importance of promoting good password hygiene, prohibiting password reuse across personal and professional accounts and maintaining up-to-date antivirus and anti-malware protection (Bishnoi *et al.*, 2023:685). Vulnerability assessments focused on social engineering attacks have proven useful in identifying departments or individuals most at risk, allowing organisations to tailor awareness programmes accordingly. Simulated attacks and penetration testing have also been shown to strengthen defences by revealing vulnerabilities in both technical systems and human behaviour (Sethi, 2022:1031-1032).

Moreover, advanced technological solutions are increasingly necessary to counteract sophisticated social engineering attacks. Biometrics, such as fingerprint or facial recognition, provide stronger identity verification (Salahdine & Kaabouch, 2019:11). AI systems, capable of learning from ongoing attack patterns, add an adaptive layer of protection, identifying threats and automatically adjusting security protocols as needed (Rathod *et al.*, 2025:25; Arshey & Angel Viji, 2021:355).

In essence, the mitigation of social engineering attacks cannot rely on siloed responses. Technical defences alone are insufficient if employees lack awareness; awareness efforts are limited without legal backing; and laws are ineffective without a criminological understanding of how attackers adapt. Therefore, a successful prevention strategy must be integrated and interdisciplinary — one that empowers individuals, strengthens systems, aligns organisational behaviours and leverages legal authority to create a hostile environment for cybercriminals. Only through such a comprehensive approach can organisations hope to withstand the evolving threat landscape of social engineering.

3.2 Motivation

Cybersecurity threats, particularly social engineering attacks, have become a growing concern in South Africa, posing significant risks to individuals, businesses and governmental institutions. Social engineering attacks exploit human vulnerabilities rather than technical system weaknesses, making them particularly insidious and difficult to detect (Venkatesha *et al.*, 2021:8). Methods such as phishing, pretexting, baiting and impersonation enable attackers to bypass even advanced defences by manipulating trust, emotion or authority (Bishnoi *et al.*, 2023:685). The consequences extend beyond individual victims, influencing broader institutional systems, resulting in financial loss, reputational damage, legal exposure and public safety risks (Abe & Soltys, 2019:825).

Although legal frameworks such as the Cybercrimes Act and the ECTA aim to criminalise and deter cybercrime, South Africa continues to face increasing rates of cyber-related fraud and identity theft. This exposes gaps in not only legislation and enforcement, but also in the psychological preparedness of users, criminological understanding of attacker behaviour and the technical capabilities of organisations (Zweni & Yan, 2022:36). Specifically, the over-reliance on technological defences has resulted in inadequate attention to behavioural vulnerabilities, particularly in an environment where social media usage and digital communication have expanded the attack surface (Murire *et al.*, 2021:1). Given the rapid evolution of cyber threats, coupled with the increased accessibility of hacking tools and the growing sophistication of cybercriminals, traditional security measures have proven inadequate in preventing social engineering attacks (Nicholls *et al.*, 2021:163966).

A critical component of mitigating social engineering lies in addressing individual cognitive and emotional vulnerabilities, including limited awareness, impulsivity, trust biases and decision fatigue. These psychological dimensions are routinely exploited through persuasive communication and urgency triggers (Junger *et al.*, 2017:75). However, psychological susceptibility alone cannot fully explain the threat. From a criminological perspective, attackers

often act based on rational assessments of opportunity, reward and risk — suggesting that deterrence strategies, offender profiling and social context must also be considered in preventative responses (Bitaab *et al.*, 2020:2). Meanwhile, technical controls such as intrusion detection systems and behavioural analytics remain essential but must operate in synergy with human and legal defences (Murire *et al.*, 2021:3).

This study is motivated by the need to address a persistent gap in the existing literature: the lack of an integrated framework that examines how law, psychology, criminology and cybersecurity interact to shape South Africa's resilience to social engineering threats. While most prior studies explore these disciplines in isolation — focusing either on legal compliance, technological defence, or psychological manipulation — few analyse how their combined limitations create opportunities for cybercriminal exploitation. This research, therefore, adopts an interdisciplinary perspective to advance understanding of how interrelated vulnerabilities, such as legal loopholes, offender motivation, psychological manipulation and technological fragility, jointly enable social engineering attacks.

Accordingly, the study is driven by the need to critically assess South Africa's response to these threats through a multifaceted perspective that reflects their real-world complexity. Integrating insights from multiple disciplines, the research not only identifies where gaps remain, such as insufficient user education, reactive law enforcement, and the absence of psychological deterrents, but also establishes a conceptual foundation for more coordinated policy and practical interventions. This motivation underpins the later discussion, which applies these four perspectives to analyse how South Africa can more effectively combat social engineering in a digital society.

Given the increasing sophistication of social engineering tactics and their ability to exploit both systemic and individual weaknesses, this research evaluates whether South Africa's current legislative tools, enforcement protocols, public awareness initiatives and technical safeguards are adequately aligned. It further assesses whether interventions are behaviourally informed and criminologically sound, drawing on both national case studies and global best practices to establish context-sensitive recommendations.

This study aims to advance the national discourse on cybersecurity through an integrated framework that synthesises legal reform, psychological insight, criminological theory, and cybersecurity strategy. The outcomes will inform targeted interventions, including legislative amendments, awareness campaigns, offender-focused deterrence and advanced technical countermeasures. These measures aim to enhance South Africa's resilience to the evolving and multifaceted threat of social engineering.

3.3 Research methodology

This study employs a qualitative research design, underpinned by a comprehensive interdisciplinary critical review, to evaluate South Africa's approach to combatting social engineering attacks. While the legal framework, particularly the Cybercrimes Act and the ECTA, serves as a core focus, the study goes beyond mere statutory analysis. It systematically integrates legal, psychological, criminological, and cybersecurity perspectives to provide a comprehensive, multidimensional critique of current national responses to these evolving threats.

The research draws upon secondary data sources, including peer-reviewed journal articles, legislative instruments, case law, policy reports, cybersecurity guidelines, psychological studies on human susceptibility and criminological theories of cyber-offender behaviour. This ensures that the critical review not only assesses regulatory coherence and enforcement challenges but also critically investigates human behaviour patterns, offender typologies and the technological vectors that enable manipulation and exploitation in social engineering attacks.

In order to capture the complexity of the threat landscape and the societal response mechanisms, the study is structured around four interconnected analytical perspectives:

- Legal analysis evaluates the scope, clarity and enforceability of South Africa's statutory and policy frameworks, including procedural limitations and evidentiary challenges in prosecuting cyber-facilitated deception.
- Psychological inquiry investigates emotional and cognitive vulnerabilities, such as fear, urgency, trust, and authority bias, that are systematically exploited by social engineers. It also examines individual and organisational blind spots in digital behaviour.
- Criminological exploration assesses offender behaviour, motivation and decision-making processes, drawing on theories such as rational choice, routine activity and situational crime prevention. It also examines enforcement challenges and systemic gaps in offender identification and deterrence.
- Cybersecurity evaluation contextualises the technical mechanisms by which social engineering attacks are deployed, such as phishing, pretexting and malware distribution, and assesses the efficacy of existing organisational defences and threat detection protocols.

The study adopts an interdisciplinary framework to ensure a methodologically coherent and conceptually balanced approach, reflecting the true nature of social engineering as a phenomenon that is simultaneously legal, behavioural, criminal, and technological. The research

identifies not only where the law falls short but also where behavioural interventions, criminological insights and technical safeguards can complement legal reforms.

This interdisciplinary review, supported by peer-reviewed journals, policy documents and comparative case studies, will help identify gaps in South Africa's current framework and suggest context-sensitive reforms to enhance national cybersecurity resilience. It also highlights areas for future interdisciplinary research and capacity building across the public and private sectors to strengthen South Africa's cyber resilience in an increasingly digitised threat environment.

The discussion that follows is deliberately organised around four interconnected analytical perspectives, cybersecurity, criminology, psychology and law, to ensure that the complexity of social engineering attacks is fully captured. Each perspective brings a distinct dimension:

- Cybersecurity perspectives contextualise the technical methods by which attacks are launched and highlight the organisational defences required.
- Criminological insights examine offender motivation, opportunity structures and behavioural patterns that underpin these attacks.
- Psychological inquiry explores cognitive and emotional vulnerabilities that offenders exploit, such as fear, urgency or trust.
- Legal analysis establishes the statutory and policy frameworks that define, prohibit and penalise social engineering practices.

This structure ensures that the study avoids a siloed assessment and instead offers an integrated evaluation of how these domains interact to shape resilience against social engineering.

Although all four perspectives are essential, the legal dimension receives particular attention, reflecting the recognition that legislation and enforcement constitute the principal means for accountability in addressing cyber-enabled offences. Laws not only set boundaries for acceptable behaviour but also determine the capacity of state and institutional actors to prosecute offenders, deter future crimes and protect victims. However, legal instruments are most effective when they are contextualised by technical feasibility, criminological theory and psychological understanding. For this reason, the discussion foregrounds the legal framework, while continuously linking it to technological, criminal and behavioural insights.

3.4 Analytical framework for the discussion

This section outlines the analytical framework that structures the forthcoming discussion, explaining how the study integrates insights from four complementary disciplines, law,

psychology, criminology and cybersecurity, to evaluate South Africa's capacity to combat social engineering attacks. Each analytical perspective offers a distinct yet interconnected perspective: the legal dimension defines statutory boundaries and enforcement mechanisms; the psychological dimension examines cognitive biases and emotional triggers that increase victim susceptibility; the criminological dimension explores offender motivation, deterrence and opportunity structures; and the cybersecurity dimension focuses on technological resilience, organisational defences and digital risk management.

Combining these perspectives, the discussion moves beyond a conventional critical review to achieve a systematic analytical synthesis that critically examines how these domains interrelate to influence national and organisational resilience. While all four perspectives are integral to understanding the phenomenon, greater emphasis is placed on the legal dimension, reflecting its centrality as the primary mechanism for accountability, deterrence and regulatory coherence. This emphasis, however, remains balanced by continuous reference to the behavioural, criminological and technical contexts that determine how law functions in practice.

The framework, therefore, ensures that the discussion avoids disciplinary isolation and instead integrates converging insights from interdisciplinary cybersecurity research, where conceptual synthesis replaces siloed analysis. The study demonstrates that effective prevention of social engineering requires not only legislative precision but also an appreciation of the psychological and criminological dynamics that underpin digital manipulation. This interdisciplinary foundation directly informs the following section, which explores integrated strategies for combatting and preventing social engineering attacks.

3.5 Combatting and preventing social engineering attacks

In order to effectively combat and prevent social engineering attacks, it is essential to adopt a holistic approach that draws on multiple disciplinary insights and regulatory mechanisms. Understanding these attacks requires more than a technical perspective; it demands consideration of human behaviour, social dynamics and organisational vulnerabilities. Interdisciplinary perspectives, therefore, provide a valuable perspective through which to analyse the psychological and sociocultural factors that make individuals and systems susceptible to manipulation.

Following this, an exploration of the legal frameworks addressing social engineering reveals how existing laws attempt to regulate such attacks and where legislative gaps persist. This section begins by examining these interdisciplinary perspectives before turning to the legal mechanisms designed to address and deter social engineering attacks.

3.5.1 Interdisciplinary perspectives on social engineering attacks

As outlined in the research methodology section, this analysis adopts a multidisciplinary approach to ensure a comprehensive understanding of social engineering attacks. Given their complexity, combining legal gaps, behavioural manipulation, criminal intent and technical exploitation, it is essential to explore them through the combined perspectives of law, psychology, criminology and cybersecurity.

Each discipline contributes uniquely to identifying the methods, motives, impacts and preventative strategies underpinning social engineering. This structured approach supports a nuanced evaluation of how these attacks operate and how they can be mitigated through targeted reforms. The following subsections apply these perspectives to critically examine the techniques, enablers and countermeasures discussed throughout the research.

3.5.1.1 Cybersecurity perspectives

From a cybersecurity standpoint, social engineering attacks are a significant threat due to their exploitation of human vulnerabilities rather than technical system flaws. Attackers use methods such as phishing, pretexting, baiting and deepfake technology to deceive users and bypass even the most sophisticated security infrastructures (Ali, 2025:2295). For example, deepfake attacks now allow cybercriminals to replicate voices or visual likenesses, enhancing impersonation scams and making fraudulent communications more convincing than ever. These manipulative tactics enable cybercriminals to gain unauthorised access to sensitive information, systems and financial resources (Hossain, 2023).

Cybersecurity frameworks aim to defend against such attacks through a combination of technical controls, such as multifactor authentication (MFA), email filtering and intrusion detection systems (Ali, 2025:2296; Hossain, 2023; Pham & Vu, 2024). However, the effectiveness of these measures relies significantly on the end-user's ability to recognise and resist social engineering attempts. Consequently, cybersecurity strategies must prioritise continuous user education, simulated phishing exercises and real-time threat detection to combat these evolving attacks successfully (Hossain, 2023).

3.5.1.2 Criminological insights

From the criminological perspective, social engineering attacks can be understood within the broader context of cybercrime behaviour and offender motivation. Criminological theories, such as Routine Activity Theory and Rational Choice Theory, help explain why cybercriminals target specific individuals or organisations (Holt *et al.*, 2018:1723; Lee *et al.*, 2021:510). These theories

suggest that attackers assess opportunities based on the perceived likelihood of success, weighing the risks of detection against potential rewards.

In the case of occupational fraud and global cybercrimes, such as BEC and investment scams, social engineering is often the primary tool for initiating and executing these offences (Siu *et al.*, 2024:444). Deepfake technologies are increasingly being used in BEC scams to impersonate executives and authorise fraudulent transactions, demonstrating the convergence of social engineering with advanced technologies to facilitate high-value crimes (Ali, 2021:326; Lee *et al.*, 2021:523).

Understanding offender profiles, motives and behaviours enables organisations to implement more targeted preventative measures, such as identity verification processes, fraud detection algorithms and stricter internal controls, to reduce opportunities for these crimes to occur (Holt *et al.*, 2018:1735; Lee *et al.*, 2021:524; Siu *et al.*, 2024:454).

3.5.1.3 Psychological manipulation

Psychology plays a central role in social engineering, as these attacks fundamentally rely on manipulating human emotions and cognitive biases (Birthriya *et al.*, 2025:254; Liu *et al.*, 2023:5). Cybercriminals exploit psychological triggers such as fear, urgency, curiosity, authority and greed to pressure victims into making impulsive decisions (Ramamoorti, 2008:527). For example, phishing emails may create a sense of panic by warning of account compromise, prompting the user to provide sensitive information without verifying the legitimacy of the request.

Deepfakes further complicate the psychological dimension by creating hyper-realistic audio and video content that increases the perceived authenticity of fraudulent messages (Birthriya *et al.*, 2025:254; Liu *et al.*, 2023:5). Victims are more likely to comply with requests when they believe they are interacting with a familiar person, such as a company executive, colleague or friend (Campbell, 2019:1131).

Psychological research informs the design of social engineering awareness programmes by highlighting how cognitive biases influence decision-making (Longtchi *et al.*, 2024:210). Interventions such as behaviour-based security training, simulated attack scenarios and cognitive resilience exercises help individuals recognise manipulation techniques and respond appropriately, reducing susceptibility to such attacks (Campbell, 2019:1141; Ramamoorti, 2008:531).

Furthermore, many organisations lack comprehensive, psychologically informed security-awareness programmes that train individuals to recognise manipulation tactics and respond

defensively. This persistent human blind spot creates a disproportionately high return on investment for cybercriminals, allowing social engineering attacks to scale across industries with minimal technological expertise.

Compounding this, South Africa's enforcement ecosystem often lacks the necessary criminological and behavioural tools, such as behavioural threat assessment, recidivism tracking and community-based interventions, that could enhance both prevention and response efforts. Enhancing these dimensions is therefore critical to develop a national defence strategy that integrates law enforcement, behavioural science and organisational awareness to disrupt the social dynamics exploited by attackers.

3.5.2 Legal frameworks addressing social engineering attacks

From a legal perspective, social engineering attacks pose complex challenges, particularly in defining, prosecuting and penalising offenders. While various legislative instruments in South Africa address aspects of cybercrime and deception, this study focuses specifically on the ECTA and the Cybercrimes Act, due to their direct relevance and primary application to social engineering attacks. Other legislative instruments, such as the POPIA 4 of 2013 or the Criminal Procedure Act, fall outside the scope of this analysis. ECTA and the Cybercrimes Act provide the core legal foundation for addressing cyber-enabled offences, including mechanisms for prosecution and the imposition of penalties. These statutes specifically criminalise behaviours commonly associated with social engineering, such as phishing, pretexting and impersonation and impose significant penalties aimed at deterrence.

However, despite these progressive legislative developments, South Africa continues to face significant challenges in effectively combatting cybercrime. Legal frameworks often struggle to keep pace with technological advancements, such as the use of deepfakes in fraud and impersonation. These innovations complicate evidence collection and attribution, making prosecution difficult and increasing the burden on law enforcement agencies. As Cassim (2011:124) notes, a fundamental difficulty in addressing cybercrime lies in the inherent nature of cyberspace, which transcends geographical and political boundaries. This enables cybercriminals to infiltrate systems across the globe with relative ease, rendering domestic legal responses insufficient in isolation.

These challenges are compounded by enforcement gaps, the rapid evolution of cyber threats and the transnational nature of cybercriminal activities (Cassim, 2011:124). Effective legal responses, therefore, require not only strong legislative measures but also robust enforcement mechanisms, specialised training for investigators and prosecutors and international partnerships to address

the globalised nature of cybercrime. Given this complexity, it is imperative for South Africa to prioritise preventative measures over reactive prosecution. Enhancing legislative frameworks with harsher penalties, while simultaneously fostering multisectoral partnerships between government, the private sector and civil society, is essential for building a resilient cybersecurity infrastructure.

Additionally, raising public awareness about legal rights and obligations in cyberspace can empower individuals to report incidents and support broader crime prevention efforts. In order to address these persistent challenges, sustained investment in legal reform, public education, capacity building for law enforcement and international cooperation is required. Such an integrated approach is vital to mitigating cyber threats and enhancing South Africa's long-term cyber resilience.

3.5.3 Electronic Communications and Transactions Act 25 of 2002

The ECTA was introduced to address the inadequacies of South African common law in dealing with cybercrime. It aims to regulate and facilitate electronic communications and transactions in the public interest. The ECTA contains several sections directly relevant to combatting social engineering attacks, particularly those involving unauthorised access, hacking and fraudulent activities.

3.5.3.1 Unauthorised access and hacking

Section 86(4) of the ECTA prohibits the production, sale or use of software designed to bypass or circumvent security systems. This provision is particularly relevant to social engineering attacks involving phishing, credential theft and pretexting, where such tools are often employed to facilitate unauthorised access to systems. Violations of this section carry penalties of up to five years' imprisonment or a fine, serving as a legal deterrent against hacking and system intrusions aimed at exploiting vulnerabilities within information systems.

3.5.3.2 Fraud, forgery and identity theft

Section 87 of the ECTA addresses fraudulent activities, forgery and extortion, which are frequently executed through social engineering tactics such as phishing, impersonation and pretexting. Cybercriminals often manipulate victims into disclosing sensitive credentials, subsequently using this information to commit identity theft, financial crimes and online scams. Offenders convicted under this section face imprisonment of up to five years or a fine, underscoring the serious impact of cyber fraud on individuals and organisations.

3.5.3.3 Email bombing and spamming

Section 86(5) of the ECTA criminalises the mass distribution of unsolicited electronic communications intended to cause disruption or harm. This provision is particularly significant in the context of large-scale phishing campaigns, where cybercriminals send mass emails designed to deceive recipients into divulging sensitive data. Offenders found guilty under this section may face a maximum of five years' imprisonment or a fine, aiming to limit the misuse of bulk messaging techniques in cybercrime.

3.5.3.4 Unsolicited communications

Section 45 of the ECTA regulates the distribution of unsolicited electronic messages for direct marketing purposes, requiring the recipient's prior consent. While primarily targeting spam, this provision plays an indirect role in preventing phishing attacks, which often originate from unsolicited communications masquerading as legitimate correspondence. Violations of section 45 may result in administrative fines, the severity of which depends on the scale and impact of the offence.

3.5.3.5 Investigative powers

Section 82 grants authorised cyber inspectors the power to enter premises and access information pertinent to cybercrime investigations, facilitating the detection and prosecution of social engineering attacks and related offences. However, the exercise of these powers raises concerns about potential infringements on constitutional rights, particularly the right to privacy, as protected under Section 14 of the *Constitution of South Africa* (1996) and the right to property, as outlined in section 25 of the *Constitution of South Africa* (1996). While no direct penalties are prescribed within this section, obstruction of investigations may result in criminal liability, fines or other legal consequences, depending on the nature of the non-compliance.

3.5.3.6 Criticism of the ECTA's penalties

Although the ECTA has contributed significantly to the regulation of cybercrime, its penalties under section 89 have been criticised for lacking the necessary severity to deter sophisticated cybercriminals. For instance, most offences under section 86 carry a maximum penalty of only one year's imprisonment, while more serious offences, such as denial-of-service attacks, are punishable by up to five years of imprisonment or a fine.

This discrepancy in sentencing raises concerns about the adequacy of deterrents against cyber offences. Many critics argue that South Africa's cybercrime laws require stricter enforcement and

harsher penalties to prevent repeat offences and large-scale data breaches. Consolidating the sentencing framework and improving law enforcement capabilities would enhance the effectiveness of legal measures in combatting social engineering attacks and other forms of cybercrime.

3.5.4 Cybercrimes Act 19 of 2020

The Cybercrimes Act was enacted to provide a more robust and comprehensive legal response to cybercrime. It aims to modernise South Africa's legal framework and align it with international standards. Several provisions of this Act are specifically applicable to social engineering attacks, including phishing, pretexting and identity fraud.

3.5.4.1 Unauthorised access and hacking

Section 4 of the Cybercrimes Act criminalises unauthorised access to computer systems or data without proper authorisation, a common consequence of social engineering attacks. Cybercriminals frequently exploit human vulnerabilities through deceptive tactics, such as phishing, pretexting and impersonation, to obtain login credentials and infiltrate protected systems. Offenders found guilty under this section, face penalties of up to 10 years' imprisonment, a fine, or both, serving as a significant deterrent to unauthorised access and hacking.

3.5.4.2 Fraud and identity theft

Section 2 of the Cybercrimes Act addresses offences such as fraud, identity theft and data manipulation, which are central to many social engineering schemes. Cybercriminals deceive victims into disclosing sensitive personal or financial information, enabling fraudulent activities that range from financial deception to the creation of false identities. Convictions under this provision carry penalties of up to ten years' imprisonment, a fine, or both, underscoring the severity of identity-based cyber offences.

3.5.4.3 Possession of data for criminal purposes

Section 7 of the Cybercrimes Act targets individuals who possess unlawfully obtained data with the intent to commit further crimes, such as fraud, extortion or blackmail. This provision is particularly significant in the context of social engineering, where stolen credentials and personal information are often used to facilitate additional offences, including financial fraud and unauthorised transactions. Those convicted face up to ten years' imprisonment, a fine or both, reinforcing protections against the misuse of stolen data.

3.5.4.4 Sentencing framework

Section 10 of the Cybercrimes Act provides a flexible sentencing framework that ensures penalties are proportionate to the gravity of the offence. Sentences are determined based on factors such as the extent of harm caused, the value of compromised data and the overall impact on victims or organisations. Penalties under this framework range from five years to life imprisonment, allowing the courts to impose harsher sentences for severe crimes, such as large-scale fraud, critical infrastructure attacks and coordinated cyber offensives.

3.5.4.5 Reporting obligations of service providers and financial institutions

Section 54 of the Cybercrimes Act imposes a legal obligation on ECSPs and financial institutions to report cybercrime incidents involving their networks or services. If such an entity becomes aware that its infrastructure has been used in the commission of any offence — such as unlawful access, interception, or data interference — it must report the offence to the SAPS without undue delay and, where feasible, no later than 72 hours after becoming aware of it. In addition, the entity is required to preserve any information that may assist SAPS in investigating the offence.

This provision is highly relevant in the context of social engineering attacks, which often rely on exploiting telecommunications and financial systems to deceive victims, disseminate fraudulent messages, or transfer illicit funds. By mandating timely reporting and evidence preservation, section 54 enhances the coordination between the private sector and law enforcement, enhancing the state's ability to investigate and respond to cyber-enabled offences.

Importantly, section 54 promotes proactive incident response and ensures that critical digital evidence is retained during the early stages of an offence, factors that are vital in tracking the perpetrators of social engineering attacks. Its enforcement represents a significant step towards building an integrated national cybersecurity framework where public-private cooperation plays a central role in combatting digital attacks.

3.5.4.6 Analysis of the Cybercrimes Act's penalties

As part of assessing the effectiveness of the legal framework in addressing social engineering attacks, this subsection critically examines the penalty provisions of the Cybercrimes Act. These legal deterrents form an essential part of enforcement mechanisms and contribute to the overall impact of legislation in combatting cyber-enabled deception.

The combined provisions of the ECTA and the Cybercrimes Act establish a comprehensive legal framework to combat social engineering attacks in South Africa. These statutes provide a strong

foundation for prosecuting cybercriminals by addressing critical areas such as fraud, forgery, unauthorised access and deceptive communications. The Cybercrimes Act, in particular, represents a significant advancement over the ECTA by introducing stricter penalties – including sentences of up to life imprisonment for severe offences – and modernised provisions that align with contemporary cyber threats.

However, despite these legal developments, enforcement challenges persist. Gaps remain in addressing physical social engineering tactics, such as tailgating, which exploit weaknesses in organisational security rather than digital vulnerabilities. Effective implementation of these laws requires augmenting investigative capabilities, fostering inter-agency collaboration and enhancing cybersecurity awareness through organisational training and robust security policies. South Africa can reduce its vulnerability to social engineering attacks and build greater resilience against an increasingly sophisticated cyber threat landscape by integrating legal deterrents with proactive security measures.

3.5.5 Application of legislation to social engineering attacks

This section examines the combined effect of the ECTA and the Cybercrimes Act as the cornerstone of South Africa's legal response to social engineering attacks. Together, these legislative instruments provide a comprehensive framework for addressing cybercrime by targeting key elements commonly exploited by social engineers, including unauthorised access, identity fraud, data breaches and the manipulation of victims into disclosing sensitive information.

3.5.5.1 Combatting phishing attacks

Phishing is one of the most prevalent forms of social engineering, in which cybercriminals deceive individuals through fraudulent emails, messages or websites to extract sensitive information such as login credentials and banking details. The ECTA and Cybercrimes Act both play critical roles in combatting phishing.

Section 45 of the ECTA, while originally intended to regulate unsolicited marketing communications, is particularly relevant to phishing prevention, as many phishing attempts originate from unauthorised electronic communications. This provision helps reduce opportunities for phishing attacks by restricting unsolicited emails without prior consent.

Complementing this, the Cybercrimes Act strengthens protections through section 2, which criminalises fraudulent misrepresentation used to unlawfully obtain money, personal information or access to systems. Additionally, section 7 criminalises the possession of unlawfully obtained data, ensuring that stolen credentials and personal data from phishing attacks are also subject to

legal penalties. Offenders convicted under these provisions may face imprisonment of up to 10 years, a fine, or both, establishing strong deterrents against phishing schemes.

3.5.5.2 Combatting tailgating and unauthorised physical access

Tailgating, or piggybacking, is a physical social engineering technique whereby an unauthorised individual gains access to restricted areas by following an authorised person. While primarily a physical security concern, South African law addresses its digital implications when such unauthorised access leads to breaches of computer systems.

Section 86(4) of the ECTA criminalises any act of bypassing security measures to gain unauthorised access to a computer system, which applies if tailgating results in intrusion into secure digital infrastructure. Similarly, the Cybercrimes Act section 4 explicitly prohibits unauthorised access to any computer system or data, regardless of how entry is achieved. These provisions ensure that cybercriminals exploiting physical vulnerabilities to compromise digital systems are held legally accountable, with penalties of up to ten years' imprisonment, a fine, or both.

3.5.5.3 Combatting pretexting and impersonation

Pretexting involves fabricating scenarios or assuming false identities to manipulate victims into disclosing confidential information, often through fraudulent calls, emails or impersonation scams. South African legislation addresses such deceptive practices through overlapping provisions in both the ECTA and Cybercrimes Act.

Section 87 of the ECTA directly criminalises fraudulent misrepresentation and forgery for personal or financial gain, which applies to many pretexting schemes. The Cybercrimes Act further reinforces this through section 2, which covers identity theft and misrepresentation, ensuring that both digital and physical impersonation attacks fall within its scope. Additionally, section 10 of the Cybercrimes Act allows courts to consider the severity of harm caused — financial, reputational, or psychological — when determining sentences, ensuring proportionate punishment for more sophisticated or damaging attacks. Convictions for these offences may result in imprisonment for up to 10 years, a fine or both, reflecting the seriousness of pretexting and impersonation tactics within social engineering.

3.6 Conclusion

The combined legislative force of the ECTA and the Cybercrimes Act provides a robust legal foundation for combatting social engineering attacks in South Africa. While the ECTA introduced

critical provisions such as anti-hacking clauses and the designation of cyber inspectors, the Cybercrimes Act enhanced this framework through stricter penalties and broader offence categories, offering a more comprehensive legal response to evolving cyber threats.

However, the effectiveness of these legislative measures, as assessed through this study's literature-based comparative analysis, relies significantly on implementation and enforcement practices. These include continuous investment in cybersecurity training, strengthened inter-agency coordination and improved public awareness. Without these supporting structures, even the strongest legal provisions may fall short in practice. South Africa can enhance its national resilience to social engineering and better protect individuals and businesses from exploitation by integrating legal deterrents with proactive organisational strategies.

The increasing prevalence of social engineering attacks presents a significant challenge to individuals, businesses and government institutions. These attacks, rooted in psychological manipulation rather than technological exploitation, have led to substantial financial losses, reputational harm and data breaches. Despite the presence of the ECTA and the Cybercrimes Act, enforcement gaps, insufficient awareness and the growing sophistication of cybercriminal tactics continue to hinder progress.

This study assessed South Africa's approach to combatting social engineering attacks through an interdisciplinary analytical framework that integrates legal, psychological, criminological and cybersecurity perspectives. While the primary focus was analytical, the insights drawn from this interdisciplinary approach also inform potential strategies for strengthening South Africa's legislative, organisational and behavioural defences against such attacks.

A key insight from the research — supported by legal, psychological, criminological and cybersecurity literature — is that legislation alone is insufficient to mitigate the risks posed by social engineering. As demonstrated in section 4, which analysed social engineering through these four perspectives (4.1.1 Cybersecurity perspectives, 4.1.2 Criminological insights, 4.1.3 Psychological manipulation and 4.2 Legal frameworks), an interdisciplinary integration is required to address both human and systemic vulnerabilities effectively. The success of legal interventions, including the Cybercrimes Act, depends on robust enforcement, cross-sector collaboration and proactive, human-centred defences. These include security-awareness training, behaviourally informed interventions and technical safeguards.

The role of organisations in fostering a "human firewall" culture is particularly critical, as employees often represent the most vulnerable entry point in social engineering schemes. Structured training, phishing simulations and multifactor authentication can substantially reduce

this risk. Coupled with stronger enforcement and alignment with international cybersecurity standards, these measures can significantly enhance South Africa's overall cyber resilience.

Future research should further evaluate South Africa's legislative approach through comparative studies with global legal frameworks and investigate the potential of emerging technologies — such as AI and machine learning — in detecting and preventing social engineering attacks. Expanding the scope of inquiry to include both human-based and computer-based social engineering tactics will also yield deeper insights into the evolution of cyber deception.

In conclusion, effectively addressing social engineering attacks requires a collaborative, interdisciplinary effort involving government, the private sector and civil society. South Africa can better position itself to confront the growing threat of cyber-enabled deception in an increasingly digital world by enhancing legal enforcement, advancing behavioural and technical safeguards and fostering public awareness. The findings of this study serve as a foundation for policy reform, targeted cybersecurity interventions and future academic inquiry into one of the most pervasive and complex forms of cybercrime.

CHAPTER 4 CONCLUSION AND RECOMMENDATIONS

4.1 Introduction

This concluding chapter brings together the key findings, reflections, and recommendations derived from this study, which explored the increasing threat of social engineering attacks in South Africa and the country's corresponding legal and organisational responses. As established in Chapter One, the research was driven by the need to critically evaluate how social engineering — a form of cyber-enabled crime that manipulates human behaviour rather than exploiting technological vulnerabilities — continues to evolve in complexity and frequency. With South Africa facing escalating digital threats, the urgency to understand, regulate, and defend against such attacks formed the core of the study's problem statement and research objectives.

In response to this, the study adopted an interpretive research paradigm with a relativist ontological foundation, using a qualitative research methodology grounded in a comprehensive literature review. A wide range of secondary sources were consulted, including academic journal articles, cybersecurity reports, South African legislation, and comparative international frameworks.

The research was structured around two interrelated yet independently framed articles:

- Article 1 (Chapter 2) examined the operational mechanics, psychological foundations, and emerging fraud trends associated with social engineering attacks.
- Article 2 (Chapter 3) critically evaluated South Africa's legislative and organisational capacity to mitigate these attacks, with a focus on key statutory instruments such as the ECTA and the Cybercrimes Act. This analysis was conducted through an interdisciplinary lens, integrating legal, psychological, criminological, and cybersecurity perspectives to provide a holistic understanding of the country's strengths, gaps, and opportunities for reform in addressing social engineering attacks.

This study was guided by the central research question introduced in Chapter One: "How can social engineering attacks be combatted in South Africa?" To address this overarching question, the research was structured around two secondary objectives, each developed as an independent article:

- Article 1 (Chapter 2): What are the operational mechanisms, psychological tactics, and emerging trends in social engineering attacks?

- Article 2 (Chapter 3): How effectively do South Africa's legal, psychological, criminological, and organisational frameworks address the threat of social engineering, and what improvements are necessary?

This chapter begins by summarising the conclusions drawn from each article before presenting a conclusive reflection on how the findings collectively answer the main research question. Thereafter, the limitations of the study are acknowledged, followed by clear recommendations for future research. The chapter concludes with closing remarks that reinforce the importance of continued vigilance, policy development, and interdisciplinary collaboration in combatting social engineering attacks in the digital age.

4.2 Conclusion on article-specific research objective

4.2.1 Identifying social engineering attacks: A critical analysis

Article 1, presented in Chapter Two, focused on providing a critical and in-depth analysis of the rising threat of social engineering attacks. The article explored the operational dynamics, psychological foundations, and evolving sophistication of these attacks, with a specific focus on their increasing use in financial fraud, identity theft, and corporate sabotage. A defining contribution of this article was its integration of Cialdini's Six Principles of Influence, which offered a theoretical framework for understanding the behavioural techniques leveraged by cybercriminals.

The study systematically categorised key social engineering methods, including phishing, pretexting, deepfake BEC, baiting, smishing, vishing, quid pro quo, tailgating, watering hole attacks, and social media manipulation. In doing so, it demonstrated how cybercriminals exploit psychological triggers — such as fear, trust, urgency, and curiosity — to manipulate victims into revealing confidential information or performing risky actions.

A significant insight was the role of emerging technologies, especially AI and deepfake tools, in enhancing the credibility of these attacks. By mimicking human behaviour with alarming accuracy, these technologies have transformed social engineering into a highly sophisticated form of cybercrime, capable of bypassing traditional technical safeguards.

The article concluded that combatting social engineering requires a multidisciplinary approach that extends beyond technical interventions. It highlighted the need for enhanced behavioural awareness training, proactive organisational policies, and improved detection systems that can recognise and counteract psychological manipulation techniques. Crucially, it affirmed that the

human element remains the most vulnerable target in the cybersecurity chain and must therefore be the central focus of any effective mitigation strategy.

4.2.2 Identifying social engineering attacks: A critical analysis of legal, psychological, criminological, and cybersecurity perspectives

Chapter Three, comprising the second article of this study, offered a critical assessment of South Africa's legislative, institutional, and behavioural response to the escalating threat of social engineering attacks. The article adopted an interdisciplinary perspective, drawing on cybersecurity, criminology, psychology, and law to evaluate the efficacy of existing frameworks and to identify both their limitations and opportunities for improvement in the country's cybercrime prevention efforts.

While the analysis centred on two primary statutory instruments — the ECTA and the Cybercrimes Act — it extended beyond legal analysis to consider behavioural and organisational dimensions of cybercrime prevention. The study acknowledged the Cybercrimes Act as a significant legislative advancement, introducing broader offence definitions and stricter sentencing; however, it also revealed persistent challenges in enforcement, public awareness, and technological adaptation. In particular, it underscored the need for improved investigative capacity, specialised training, and greater responsiveness to emerging attack forms such as deepfakes, AI-driven impersonation, and transnational cybercrime.

In addition to evaluating legislative frameworks, the article examined organisational and behavioural mitigation strategies. These included security-awareness training, phishing simulations, multifactor authentication, access control protocols, and the promotion of a security-conscious workplace culture. Emphasis was placed on the importance of cultivating a "human firewall" by equipping individuals with the behavioural awareness and critical thinking skills necessary to recognise and resist manipulation.

Ultimately, Article 2 concluded that an integrated and adaptive approach — combining legal reform, behavioural science, organisational resilience, and the advancement of technical safeguards — is essential for effectively mitigating social engineering threats in South Africa's evolving digital ecosystem. The findings strongly support the need for ongoing policy reform, multisectoral collaboration, and national awareness campaigns to build a more robust and future-ready cybersecurity posture.

4.3 Conclusion on the problem statement and main objective

This study set out to address a pressing and contemporary issue: the increasing prevalence of social engineering attacks in South Africa and the limitations of current frameworks in preventing and responding to these attacks. As stated in Chapter One, the central problem was the ability of cybercriminals to bypass technical defences by exploiting human vulnerabilities — such as trust, urgency, and fear — through sophisticated psychological manipulation and deception techniques.

The primary objective of the study was to critically examine the methods employed in social engineering attacks and assess South Africa's capacity — legally, organisationally, and behaviourally — to mitigate their impact. To achieve this, the research adopted an interpretive paradigm with a relativist ontological position and employed a qualitative, literature-based methodology. Two key questions guided the study:

1. What are the psychological and operational dynamics underpinning social engineering attacks?
2. How effective is South Africa's legal and strategic response in addressing this form of cyber-enabled crime?

The objective was successfully met through the dual-article approach. Chapter Two (Article 1) provided a detailed conceptual analysis of social engineering, outlining its various forms, psychological foundations, and the role of emerging technologies — particularly AI and deepfakes — in amplifying its reach and credibility. Chapter Three (Article 2) offered a critical evaluation of South Africa's legislative and institutional responses, focusing on the ECTA and the Cybercrimes Act, and highlighting both progress and persistent challenges in enforcement, public education, and legal adaptation.

The study found that while legislative developments such as the Cybercrimes Act mark significant progress, their success is contingent on effective enforcement, cross-sectoral cooperation, and a national culture of cybersecurity awareness. Crucially, the research reaffirmed that social engineering is as much a behavioural issue as it is a technical or legal one. The most exploitable aspect of any security system remains the human element — requiring a broader, interdisciplinary response that blends technological innovation, robust legal tools, and behavioural resilience strategies.

In conclusion, this dissertation fulfilled its main objective by offering a holistic assessment of social engineering attacks in the South African context and proposing actionable insights for improving national resilience. It emphasised the urgent need to move beyond traditional security models

and adopt integrated strategies that account for the human, technological, and legal dimensions of cyber risk.

4.3.1 Answer to the research question

As articulated in Section 1.6, the central research question of this study asked: “How can social engineering attacks be combatted in South Africa?” This question was comprehensively addressed through the integrated findings of Chapters Two and Three, which collectively demonstrate that combatting social engineering requires a multidimensional and interdisciplinary strategy. The study concludes that while South Africa’s legislative instruments, particularly the Cybercrimes Act and ECTA, form a critical foundation for criminalising and deterring social engineering offences, legislation alone is insufficient.

Effective mitigation depends equally on behavioural resilience, organisational security culture, and technological adaptation. Therefore, an optimal national response must combine:

- Robust legal enforcement and continuous policy reform.
- Psychological and criminological insight into offender tactics and victim susceptibility.
- Cybersecurity measures such as AI-driven threat detection, phishing simulations, and access control protocols.
- Sustained cross-sector collaboration and public awareness campaigns as the primary platforms through which national prevention strategies are coordinated, communicated, and embedded across society.

In essence, South Africa can combat social engineering effectively only through an integrated approach in which law, human behaviour, and technology are operationalised through continuous collaboration between government, industry, civil society, and the public. Public awareness initiatives and cross-sector cooperation are therefore not supplementary measures, but essential mechanisms for promoting national resilience, fostering behavioural change, and ensuring the effective implementation of all recommended mitigation strategies.

4.4 Limitations of this study

Although this study provides a comprehensive exploration of social engineering attacks in South Africa and critically assesses the country's legislative and organisational response mechanisms, it is important to recognise certain limitations that may have influenced the scope, depth, and generalisability of its findings.

Exclusive reliance on secondary data

- The research was conducted solely through a literature-based review, relying on academic journals, legislative texts, reports, and expert commentary. While this enabled a theoretically rich discussion, the absence of primary data — such as interviews with cybersecurity professionals or surveys of affected organisations — meant that first-hand insights were not incorporated. As a result, the study may not fully capture practical experiences or operational challenges faced on the ground.

Absence of quantitative or statistical analysis

- As a qualitative study, this research focused on conceptual analysis and interpretive findings. No empirical or statistical methods were employed, which limited the ability to measure the frequency, prevalence, or impact of social engineering attacks quantitatively. A mixed-method approach could have allowed for a more robust triangulation of findings and the identification of statistically significant trends.

Dynamic nature of social engineering attacks

- Social engineering is a constantly evolving threat, with tactics continually adapting to emerging technologies such as AI, machine learning, and synthetic identities. While the study incorporates current fraud trends (notably from 2024), the fast-paced nature of technological innovation may render some observations outdated over time.

Geographic and jurisdictional narrowness

- The study focused exclusively on South Africa, examining its legal instruments such as the ECTA and the Cybercrimes Act. Although these were analysed in detail, limited reference was made to regional cybersecurity dynamics or international legislative comparisons. As such, the findings are context-specific and may not be generalisable to other legal or cultural environments.

Scope of legislative coverage

- The legal analysis centred primarily on the ECTA and the Cybercrimes Act, without extensively evaluating related frameworks such as the POPIA, the National Cybersecurity Policy Framework, or industry-specific compliance requirements. These exclusions may have constrained the overall assessment of South Africa’s legal preparedness.

In acknowledging these limitations, this study highlights opportunities for future research to adopt empirical methodologies, expand comparative analyses across jurisdictions, and incorporate real-time data from practitioners and affected organisations. Such research would serve to validate and build upon the foundations established in this dissertation, ultimately contributing to a more nuanced and actionable body of knowledge in the field of cybersecurity and social engineering.

4.5 Recommendations for future research

While this study has contributed to a deeper understanding of social engineering attacks, it also highlights several areas in which further research is warranted. The following recommendations aim to guide future academic inquiry and practical intervention in the evolving field of cybersecurity:

Empirical research and primary data collection

- Future studies should aim to complement literature-based analyses with primary research methods such as interviews with cybersecurity experts, law enforcement officials, and affected organisations. Surveys and case studies could also offer rich, real-world perspectives on the nature and impact of social engineering attacks, particularly within South Africa's key sectors.

Comparative legislative analysis

- A deeper comparison between South Africa's cybercrime legislation and the regulatory frameworks of countries with advanced cybersecurity protocols — such as the United Kingdom, United States, and European Union — would be valuable. Such studies may uncover global best practices that could inform future policy revisions and legal reform within South Africa.

Assessment of law enforcement and judicial capacity

- Further research should investigate the practical enforcement of the Cybercrimes Act and ECTA. This includes evaluating prosecution rates, sentencing outcomes, and law enforcement capabilities to determine whether legal tools are being used effectively and where gaps in implementation may exist.

Exploration of AI in cyber defence

- As AI becomes increasingly central to both attacks and defence, future research could explore how machine learning, biometric security, and automated threat detection can be employed to identify and mitigate social engineering attacks. Additionally, AI-powered solutions to detect deepfakes and synthetic identities warrant focused investigation.

Behavioural and psychological profiling studies

- Given the inherently human-centric nature of social engineering, further exploration into user behaviour, risk perception, and psychological susceptibility would be beneficial. Research in behavioural forensics, decision-making psychology, and social cognition can guide the design of more effective training, awareness, and detection systems.

Evaluation of public awareness campaigns

- Studies assessing the reach, effectiveness, and behavioural impact of national cybersecurity awareness initiatives would offer insights into whether these campaigns are successfully building user resilience against manipulation and deception.

Sector-specific risk research

- Targeted research examining how various industries — such as finance, healthcare, telecommunications, and education — experience and respond to social engineering attacks can support the development of tailored risk mitigation strategies and industry-specific protocols.
- As discussed in Chapter Three, the lack of psychologically informed security-awareness programmes and behaviourally grounded enforcement mechanisms remains a major barrier to effectively combatting social engineering attacks in South Africa. Addressing this challenge requires an interdisciplinary strategy that integrates legal reform, behavioural threat assessment, and organisational awareness initiatives. Future research should therefore explore how law enforcement agencies, educational institutions, and private-sector organisations can collaborate to embed behavioural science principles into cybersecurity policy, training, and national prevention frameworks.

4.6 Final remarks

This study has provided a timely and comprehensive examination of the growing threat posed by social engineering attacks within the South African context. By exploring the operational mechanics, psychological drivers, and legislative responses to these attacks, the research has contributed both to academic understanding and to the practical discourse on cybersecurity resilience. It has highlighted that while technological defences are crucial, the human element remains the most vulnerable and frequently targeted aspect of any security system.

Through the two articles presented in Chapters Two and Three, this dissertation has not only unpacked the methods and psychological manipulation strategies used by cybercriminals but also assessed the adequacy of South Africa's legal and organisational countermeasures. The findings reaffirm the view that social engineering is a multifaceted attack requiring a multifaceted response — one that blends robust legal enforcement, behavioural interventions, and proactive organisational strategies.

Meaningful progress in combatting social engineering will depend on South Africa's ability to remain dynamic and adaptive. Legislation such as the Cybercrimes Act represents a significant step forward; however, without widespread enforcement, public education, and private-sector collaboration, its full potential will remain unrealised. Moreover, the complexity of modern

cybercrime — especially with the advent of AI-driven impersonation and synthetic identities — demands continuous vigilance and innovation across all levels of society.

As the digital landscape evolves, so too must our defences. The study underscores the need for collaborative engagement across academia, government, industry, and civil society to build a strong, informed, and digitally resilient population. Education and awareness must be central pillars in this effort, equipping individuals with the tools to recognise, resist, and report manipulative cyber tactics.

Ultimately, the fight against social engineering is not just a battle against cybercriminals — it is a broader challenge to strengthen digital trust and human resilience in an increasingly connected world. The work initiated in this dissertation provides a foundation for ongoing dialogue, research, and action, ensuring that South Africa is better prepared to meet the complex cyberattacks of today and tomorrow.

REFERENCES

Abdulla, R.M., Faraj, H.A., Abdullah, C.O., Amin, A.H. & Rashid, T.A. 2023. Analysis of social engineering awareness among students and lecturers. *IEEE Access*, 11:101098–101111. https://doi.org/10.1109/ACCESS.2023.3311708

Abe, N. & Soltys, M. 2019. Deploying health campaign strategies to defend against social engineering threats. *Procedia Computer Science*, 159:824–831. https://doi.org/10.1016/j.procs.2019.09.241

Alabdan, R. 2020. Phishing attacks survey: types, vectors, and technical approaches. *Future Internet*, 12(168):1–39. https://doi.org/10.3390/fi12100168

Albladi, S.M. & Weir, G.R.S. 2018a. A semi-automated security advisory system to resist cyber-attack in social networks. In: *Computational collective intelligence – 10th international conference, ICCCI 2018, proceedings*. Lecture notes in computer science, 11055. Cham: Springer. pp. 146–156. https://doi.org/10.1007/978-3-319-98443-8

Albladi, S.M. & Weir, G.R.S. 2018b. User characteristics that influence judgment of social engineering attacks in social networks. *Human-centric Computing and Information Sciences*, 8(1):1–24. https://doi.org/10.1186/s13673-018-0128-7

Ali, S. 2021. Criminal minds: profiling architects of financial crimes. *Journal of Financial Crime*, 28(2):324–344. https://doi.org/10.1108/JFC-11-2020-0221

Ali, S. 2025. Cyber security and forensic accounting in combating criminals using artificial intelligence – A forward analysis. *International Journal of Innovative Research in Technology*, 11(9):2294–2297.

Almadhoor, L., Alserhani, F. & Humayun, M. 2021. Social media and cybercrimes. *Turkish Journal of Computer and Mathematics Education*, 12(10):2972–2981. https://api.semanticscholar.org/CorpusID:236578271

Arshey, M. & Angel Viji, K.S. 2021. Thwarting cyber crime and phishing attacks with machine learning: a study. In: *2021 7th international conference on advanced computing and communication systems (ICACCS)*. pp. 353–357. https://doi.org/10.1109/ICACCS51430.2021.9441925

Bennett, B. 2023. Phishing, vishing, smishing and beyond. *NZBusiness*, 37(2):36–37.

Birthriya, S.K., Ahlawat, P. & Jain, A.K. 2025. A comprehensive survey of social engineering attacks: taxonomy of attacks, prevention, and mitigation strategies. *Journal of Applied Security Research*, 20(2):244–292. https://doi.org/10.1080/19361610.2024.2372986

Bishnoi, A., Garv, Bishnoi, S. & Gupta, N. 2023. Comprehensive assessment of reverse social engineering to understand social engineering attacks. In: *2023 5th international conference on smart systems and inventive technology (ICSSIT)*. pp. 681–685. https://doi.org/10.1109/ICSSIT55814.2023.10061054

Bitaab, M., Cho, H., Oest, A., Zhang, P., Sun, Z., Pourmohamad, R., Kim, D., Bao, T., Wang, R., Shoshitaishvili, Y., Doupe, A. & Ahn, G.J. 2020. Scam pandemic: how attackers exploit public fear through phishing. In: *2020 APWG symposium on electronic crime research (eCrime)*. pp. 1–10. https://doi.org/10.1109/eCrime51433.2020.9493260

Bulleé, J.H., Montoya, L., Pieters, W., Junger, M. & Hartel, P.H. 2015. The persuasion and security awareness experiment: reducing the success of social engineering attacks. *Journal of Experimental Criminology*, 11(1):97–115. https://doi.org/10.1007/s11292-014-9222-7

Campbell, C.C. 2019. Solutions for counteracting human deception in social engineering attacks. *Information Technology & People*, 32(5):1130–1152. https://doi.org/10.1108/ITP-12-2017-0422

Cassim, F. 2011. Addressing the growing spectre of cyber crime in Africa: evaluating measures adopted by South Africa and other regional role players. *CILSA*, 44(1):123–138. https://api.semanticscholar.org/CorpusID:146685273

Chen, R., Gaia, J. & Rao, H.R. 2020. An examination of the effect of recent phishing encounters on phishing susceptibility. *Decision Support Systems*, 133:113287. https://doi.org/10.1016/j.dss.2020.113287

Cialdini, R.B. 2007. *Influence: the psychology of persuasion*. Revised ed. New York, NY: HarperCollins Publishers Inc.

Clark, T. 2024. Vishing in the age of AI. *ITNOW*, 66(2):39. https://doi.org/10.1093/itnow/bwae052

Colorado Department of Education. 2020. *Social engineering education*. https://www.cde.state.co.us/dataprivacyandsecurity/socialengineeringeducation Date of access: 24 Mar. 2025.

Constitution of the Republic of South Africa 1996.

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):31–38. https://doi.org/10.19101/IJACR.2016.623006

Criminal Procedure Act 51 of 1977.

Cristescu, I., Ciupercă, E.M. & Cirnu, C.E. 2022. Exploiting personality traits in social engineering attacks. *Romanian Journal of Information Technology and Automatic Control*, 32(1):113–122. https://doi.org/10.33436/v32i1y202209

Cybercrimes Act 19 of 2020.

Dashora, K. 2011. Cyber crime in the society: problems and preventions. *Journal of Alternative Perspectives in the Social Sciences*, 3(1):240–259. https://api.semanticscholar.org/CorpusID:113094591

Doke, T., Khismatrao, P., Jambhale, V. & Marathe, N. 2020. Phishing-Inspector: detection & prevention of phishing websites. *ITM Web of Conferences*, 32:03004. https://doi.org/10.1051/itmconf/20203203004

Electronic Communications & Transactions Act 25 of 2002.

Fakieh, A. & Akremi, A. 2022. An effective blockchain-based defense model for organizations against vishing attacks. *Applied Sciences*, 12(24):13020. https://doi.org/10.3390/app122413020

Gehl, R.W. & Lawson, S.T. 2022. *Social engineering: How crowdmasters, phreaks, hackers, and trolls created a new form of manipulative communication*. Cambridge: MIT Press. Date of access: 22 Jul. 2023. https://doi.org/10.1177/10575677251410559

Goel, D. & Jain, A.K. 2018. Mobile phishing attacks and defence mechanisms: state of art and open research challenges. *Computers & Security*, 73:519–544. https://doi.org/10.1016/j.cose.2017.12.006

Harkin, D. & Whelan, C. 2022. Perceptions of police training needs in cyber-crime. *International Journal of Police Science & Management*, 24(1):66–76. https://doi.org/10.1177/14613557211036565

He, D., Lv, X., Xu, X., Yu, S., Li, D., Chan, S. & Guizani, M. 2022. An effective double-layer detection system against social engineering attacks. *IEEE Network*, 36(6):92–98. https://doi.org/10.1109/MNET.105.2100425

Hijji, M. & Alam, G. 2021. A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: challenges and prospective solutions. *IEEE Access*, 9:7180–7208. https://doi.org/10.1109/ACCESS.2020.3048839

Holt, T.J., Burruss, G.W. & Bossler, A.M. 2018. Assessing the macro-level correlates of malware infections using a routine activities framework. *International Journal of Offender Therapy and Comparative Criminology*, 62(6):1720–1741. https://doi.org/10.1177/0306624X16679162

Hossain, M.Z. 2023. *Emerging trends in forensic accounting: data analytics, cyber forensic accounting, cryptocurrencies, and blockchain technology for fraud investigation and prevention*. State University of Bangladesh.

Huseynov, F. & Kose, B.O. 2022. Using machine learning algorithms to predict individuals' tendency to be victim of social engineering attacks. *Information Development*:1–21. https://doi.org/10.1177/02666669221116336

Ivanov, M.A., Kliuchnikova, B.V., Chugunkov, I.V. & Plaksina, A.M. 2021. Phishing attacks and protection against them. In: *2021 IEEE conference of Russian young researchers in electrical and electronic engineering (ElConRus)*. IEEE:425–428. https://doi.org/10.1109/ElConRus51938.2021.9396693

Jakobsson, M. 2016. *Understanding social engineering based scams*. New York, NY: Springer. https://doi.org/10.1007/978-1-4939-6457-4

Jenkins, A., Kokciyan, N. & Vaniea, K. 2022. PhishED: automated contextual feedback for reported phishing. In: *18th symposium on usable privacy and security*. pp. 1–5. Date of access: 31 May 2023. https://www.research.ed.ac.uk/en/publications/phished-automated-contextual-feedback-for-reported-phishing/

Jones, K.S., Armstrong, M.E., Tornblad, M.K. & Namin, A.S. 2021. How social engineers use persuasion principles during vishing attacks. *Information & Computer Security*, 29(2):314–331. https://doi.org/10.1108/ICS-07-2020-0113

Junger, M., Montoya, L. & Overink, F.J. 2017. Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior*, 66:75–87. https://doi.org/10.1016/j.chb.2016.09.012

Kangapi, T.M. & Chindenga, E. 2022. Towards a cybersecurity culture framework for mobile banking in South Africa. *IST-Africa 2022 conference proceedings*. IST-Africa Institute and Authors. pp. 1–8. https://doi.org/10.23919/IST-Africa56635.2022.9845633

Khatri, K.K. 2020. Research paradigm: a philosophy of educational research. *International Journal of English Literature and Social Sciences*, 5(5):1435–1440. https://doi.org/10.22161/ijels.55.27

Koops, B.J. 2011. The internet and its opportunities for cybercrime. *Tilburg Law School Legal Studies Research Paper Series*, 9(1):735–754. https://research.tilburguniversity.edu/en/publications/cacedf83-6d90-404d-b4f8-fa92081234cc

Kritzinger, E. 2019. Cyber safety for all school learners – creating a cyber safety culture for South African schools. *Servamus Community-based Safety and Security Magazine*, 112(10):27–29. https://doi.org/10.18489/sacj.v29i2.471

Lee, B., Fenoff, R. & Spink, J. 2021. Routine activities theory and food fraud victimization. *Security Journal*, 35(2):506–530. https://doi.org/10.1057/s41284-021-00287-1

Li, T., Wang, K. & Horkoff, J. 2019. Towards effective assessment for social engineering attacks. In: *2019 IEEE 27th international requirements engineering conference (RE)*. pp. 392–397. https://doi.org/10.1109/RE.2019.00051

Liu, Y., Naveed, R.T., Kanwal, S., Tahir Khan, M., Dalain, A.F., Lan, W. & Jermsittiparsert, K. 2023. Psychology in action: social media communication, CSR, and consumer behavior management in banking. *PLOS ONE*, 18(8):e0289281. https://doi.org/10.1371/journal.pone.0289281

Longtchi, T.T., Rodriguez, R.M., Al-Shawaf, L., Atyabi, A. & Xu, S. 2024. Internet-based social engineering psychology, attacks, and defenses: a survey. *Proceedings of the IEEE*, 112(3):210–246. https://doi.org/10.1109/JPROC.2024.3379855

Mansor, R.A.N. 2015. Forensic accounting and fraud risk factors: the influence of fraud diamond theory. *The American Journal of Innovative Research and Applied Sciences*, 1(5):186–192. https://doi.org/10.1002/9781119601906.ch12

Mattera, M. & Chowdhury, M. 2021. Social engineering: the looming threat. In: *2021 IEEE international conference on electro information technology (EIT)*. pp. 056–061. https://doi.org/10.1109/EIT51626.2021.9491884

McNealy, J.E. 2022. Platforms as phish farms: deceptive social engineering at scale. *New Media & Society*, 24(7):1677–1694. https://doi.org/10.1177/14614448221099228.

Mimecast. 2023. *The state of email security 2023*. https://www.mimecast.com/state-of-email-security/ Date of access: 24 Jul. 2023.

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*, 108:803–815. https://doi.org/10.1016/j.future.2020.03.021

Mouton, F., Leenen, L. & Venter, H.S. 2016. Social engineering attack examples, templates and scenarios. *Computers & Security*, 59:186–209. https://doi.org/10.1016/j.cose.2016.03.004

Murire, O.T., Flowerday, S., Strydom, K. & Fourie, C.J. 2021. Narrative review: social media use by employees and the risk to institutional and personal information security compliance in South Africa. *TD: The Journal for Transdisciplinary Research in Southern Africa*, 17(1):a909. https://doi.org/10.4102/td.v17i1.909

Nagunwa, T. 2014. Behind identity theft and fraud in cyberspace: the current landscape of phishing vectors. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, 3(1):72–83.

Nicholls, J., Kuppa, A. & Le-Khac, N.A. 2021. Financial cybercrime: a comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. *IEEE Access*, 9:185621–185640. https://doi.org/10.1109/ACCESS.2021.3134076

Obuhuma, J. & Zivuku, S. 2020. Social engineering based cyber-attacks in Kenya. *IST-Africa 2020 conference proceedings*. IST-Africa Institute and Authors. pp. 1–9.

Ozkaya, E. 2018. *Learn social engineering: learn the art of human hacking with an internationally renowned expert*. Birmingham: Packt Publishing. https://ebookcentral.proquest.com/lib/northwu-ebooks/detail.action?docID=5379705 Date of access: 28 Jul. 2024.

Parker, H.J. & Flowerday, S.V. 2020. Contributing factors to increased susceptibility to social media phishing attacks. *South African Journal of Information Management*, 22(1):a1176. https://doi.org/10.4102/sajim.v22i1.1176

Parthy, P.P. & Rajendran, G. 2019. Identification and prevention of social engineering attacks on an enterprise. In: *International Carnahan conference on security technology (ICCST) CHENNAI, India 2019 Oct. 1 – 2019 Oct. 3*. pp. 1–5. https://doi.org/10.1109/CCST.2019.8888441

Pham, Q.H. & Vu, K.P. 2024. Insight into how cyber forensic accounting enhances the integrated reporting quality in small and medium enterprises. *Cogent Business & Management*, 11(1):2364053. https://doi.org/10.1080/23311975.2024.2364053

Protection of Personal Information Act 4 of 2013.

Ramadani, S., Siahaan, A.P.U., Sutrisno, R.S., Amelia, W.R., Dalimunthe, H. & Munthe, R. 2018. Impact of cybercrime on technological and financial developments. *International Journal for Innovative Research in Multidisciplinary Field*, 4(10):341–344.

Ramamoorti, S. 2008. The psychology and sociology of fraud: integrating the behavioral sciences component into fraud and forensic accounting curricula. *Issues in Accounting Education*, 23(4):521–533. https://doi:10.2308/iace.2008.23.4.521

Rathod, T., Jadav, N.K., Tanwar, S., Alabdulatif, A., Garg, D. & Singh, A. 2025. A comprehensive survey on social engineering attacks, countermeasures, case study, and research challenges. *Information Processing and Management*, 62(1):103928. https://doi.org/10.1016/j.ipm.2024.103928

Rezaee, Z., Wang, J. & Lam, B. 2018. Toward the integration of big data into forensic accounting education. *Journal of Forensic and Investigative Accounting*, 10(1):87–99.

Salahdine, F. & Kaabouch, N. 2019. Social engineering attacks: a survey. *Future Internet*, 11(4):89. https://doi.org/10.3390/fi11040089

Salloum, S., Gaber, T., Vadera, S. & Shaalan, K. 2022. A systematic literature review on phishing email detection using natural language processing techniques. *IEEE Access*, 10:65703–65727. https://doi.org/10.1109/ACCESS.2022.3183083

Salmon-Powell, Z., Scarlata, J. & Vengrouskie, E.F. 2021. Top five artificial intelligence trends affecting leadership & management. *Journal of Strategic Innovation and Sustainability*, 16(4):1–3. https://doi.org/10.33423/jsis.v16i4.4616

Savitz, E. 2012. *Social engineering: hacking the human mind*. https://www.forbes.com/sites/ciocentral/2012/03/29/social-engineering-hacking-the-human-mind/ Date of access: 24 Mar. 2025.

Sethi, P. 2022. Social engineering in cyber security. *Jus Corpus Law Journal*, 3(1):1025–1032.

Siu, J.C.L., Zhong, H. & Nivette, A. 2024. Exploring the impact of routine activity and financial strain on fraud victimization during the COVID-19 pandemic in Hong Kong. *Asian Journal of Criminology*, 19(3):441–458. https://doi.org/10.1007/s11417-024-09438-w

Snail, S. 2009. Cyber crime in South Africa – hacking, cracking, and other unlawful online activities. *Journal of Information, Law & Technology*, 2009(1):1–13. https://warwick.ac.uk/fac/soc/law/elj/jilt/2009_1/snail/

Soomro, T.R. & Hussain, M. 2019. Social media-related cybercrimes and techniques for their prevention. *Applied Computer Systems*, 24(1):9–17. https://doi.org/10.2478/acss-2019-0002

Staiger, A. 2024. *Fraudify wrapped 2024: the year in fraud trends*. https://www.acfe.com/acfe-insights-blog/blog-detail?s=fraudify-wrapped-2024 Date of access: 22 Nov. 2025.

Syafitri, W., Shukar, Z., Mokhtar, U., Sulaiman, R. & Ibrahim, M.A. 2022. Social engineering attacks prevention: a systematic literature review. *IEEE Access*, 10:39325–39343. https://doi.org/10.1109/ACCESS.2022.3162594

Venkatesha, S., Reddy, K.R. & Chandavarkar, B.R. 2021. Social engineering attacks during the COVID-19 pandemic. *SN Computer Science*, 2(2):90. https://doi.org/10.1007/s42979-020-00443-1

Wang, Z., Zhu, H. & Sun, L. 2021. Social engineering in cybersecurity: effect mechanisms, human vulnerabilities and attack methods. *IEEE Access*, 9:11895–11910. https://doi.org/10.1109/ACCESS.2021.3051633

Watson, G., Mason, G. & Ackroyd, R. 2014. *Social engineering penetration testing: executing social engineering pen tests, assessments and defense*. Waltham, Massachusetts: Syngress. Date of access: 28 Jul. 2024.

Williams, G., Fourie, T. & Siyaya, S. 2021. *The newly enacted Cybercrimes Act and what it means for South Africans*. https://www.golegal.co.za/newly-enacted-cybercrimes-act/ Date of access: 25 Apr. 2023.

Xiao, Y. & Watson, M. 2019. Guidance on conducting a systematic literature review. *Journal of Planning Education and Research*, 39(1):93–112. https://doi.org/10.1177/0739456X17723971

Ye, Z., Guo, Y., Ju, A., Wei, F., Zhang, R. & Ma, J. 2020. A risk analysis framework for social engineering attack based on user profiling. *Journal of Organizational and End User Computing (JOEUC)*, 32(3):37–49. https://doi.org/10.4018/JOEUC.2020070104

Zweni, A. & Yan, B. 2022. The role of municipal officials in financial crimes and the effects thereof: a conceptual framework to combat financial crimes in South African municipalities. *African Renaissance*, 19(4):35–57. https://journals.co.za/doi/abs/10.31920/2516-5305/2022/19n4a2 Date of access: 2025

ANNEXURE A: ETHICS APPROVAL LETTER OF STUDY

South Africa 2520

Tel: 018 299-1111/2222
Fax: 018 299-4910
Web: http://www.nwu.ac.za

Senate Committee for Research Ethics
Tel: 018 299-484
Feziwe.Mseleni@nwu.ac.za

19 April 2024

ETHICS APPROVAL LETTER OF STUDY

Based on approval by the **Economic and Management Sciences Research Ethics Committee (EMS-REC)** on, 19 April 2024 the Economic and Management Sciences Research Ethics Committee hereby **approves** your study as indicated below. This implies that the North-West University Senate Committee for Research Ethics (NWU-REC) grants its permission that, provided the special conditions specified below are met and pending any other authorisation that may be necessary, the study may be initiated, using the ethics number below.

Study title: Combatting social engineering attacks in South Africa: A critical analysis

Study Leader/Supervisor (Principal Investigator)/Researcher): Mr Frans Triegaardt

Student: N. Van der Linde(25909932)

N	W	U	-	0	0	6	4	8	-	2	4	-	A	4
Institution				Study Number						Year			Status	

Status: S = Submission; R = Re-Submission; P = Provisional Authorisation; A = Authorisation

Application Type:
Commencement date: 19/04/2024 **Risk:** **Minimal**
Expiry date: 19/04/2025
Approval of the study is initially provided for a year, after which continuation of the study is dependent on receipt and review of the annual (or as otherwise stipulated) monitoring report and the concomitant issuing of a letter of continuation.

Special in process conditions of the research for approval (if applicable):

- None.

General conditions:

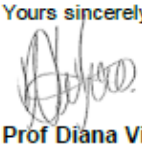
While this ethics approval is subject to all declarations, undertakings and agreements incorporated and signed in the application form, the following general terms and conditions will apply:

- *The study leader/supervisor (principle investigator)/researcher must report in the prescribed format to the EMS-REC:*
  - *annually (or as otherwise requested) on the monitoring of the study, whereby a letter of continuation will be provided, and upon completion of the study; and*
  - *without any delay in case of any adverse event or incident (or any matter that interrupts sound ethical principles) during the course of the study.*
- *The approval applies strictly to the proposal as stipulated in the application form. Should any amendments to the proposal be deemed necessary during the course of the study, the study leader/researcher must apply for approval of these amendments at the EMS-REC, prior to implementation. Should there be any deviations from the study proposal without the necessary approval of such amendments, the ethics approval is immediately and automatically forfeited.*
- *Annually a number of studies may be randomly selected for an external audit.*
- *The date of approval indicates the first date that the study may be started.*
  n the interest of ethical responsibility, the NWU-SCRE and EMS-REC reserves the right to:

- *request access to any information or data at any time during the course or after completion of the study;*
- *to ask further questions, seek additional information, require further modification or monitor the conduct of your research or the informed consent process;*
- *withdraw or postpone approval if:*
  - *any unethical principles or practices of the study are revealed or suspected;*
  - *it becomes apparent that any relevant information was withheld from the EMS-REC or that information has been false or misrepresented;*
  - *submission of the annual (or otherwise stipulated) monitoring report, the required amendments, or reporting of adverse events or incidents was not done in a timely manner and accurately; and / or*
  - *new institutional rules, national legislation or international conventions deem it necessary.*

The EMS-REC would like to remain at your service as scientist and researcher, and wishes you well with your study. Please do not hesitate to contact the EMS-REC or the NWU-SCRE for any further enquiries or requests for assistance.

Yours sincerely,



Prof Diana Viljoen-Bezuidenhout
Chairperson: NWU Economic and Management Sciences Research Ethics Committee

ANNEXURE B: DECLARATION OF LANGUAGE EDITING

Jomoné Müller
Language Practitioner
SATI No. 1002831
BA Hons (Language practice)

www.jmuller.co.za
Tel: +27 84 406 0029
jomone@jmuller.co.za

22 November 2025

To whom it may concern

RE: Declaration of Language Editing

This is to confirm that I, the undersigned, have language edited the research entitled:

"Combatting social engineering attacks in South Africa: A critical analysis."

No changes were permanently affected and were left to the discretion of the author. The responsibility of implementing the recommended language changes rests with the author of the dissertation.

Yours truly

Jomoné Müller