Scientific Research Publishing

Open Journal of Social Sciences, 2026, 14(6), 136-150
https://www.scirp.org/journal/jss
ISSN Online: 2327-5960
ISSN Print: 2327-5952

Social Engineering and Victim Vulnerability: Phishing, Smishing, and Vishing in South Africa's Cyber Landscape

Nondumiso Ayanda Ndlovu[1], Zandile Faith Mpofu[2], Slindile Ngcece[2], Bongolethu Diko[2], Nomathamsanqa Mthethwa[2]

[1]Department of Criminology and Security Science, University of South Africa, Pretoria, South Africa
[2]Department of Corrections Management, University of South Africa, Pretoria, South Africa
Email: ndlovan@unisa.ac.za

How to cite this paper: Ndlovu, N. A., Mpofu, Z. F., Ngcece, S., Diko, B., & Mthethwa, N. (2026). Social Engineering and Victim Vulnerability: Phishing, Smishing, and Vishing in South Africa's Cyber Landscape. *Open Journal of Social Sciences, 14,* 136-150.
https://doi.org/10.4236/jss.2026.146007

Received: February 25, 2026
Accepted: June 9, 2026
Published: June 12, 2026

Abstract

This study examines the incidents, methods, and vulnerabilities of phishing, smishing, and vishing attack victims in South Africa through a qualitative desktop review of existing literature. The paper primarily relied on available literature to analyse how this type of cybercrime exploits technological, psychological, and social factors to target individuals and organizations. It has been found that cybercriminals employ more advanced methods, including social engineering, malware-based communications, and real-time deceit. At the same time, victims are weak in various ways, including low levels of digital literacy, ignorance, and a reliance on the familiar. The article underscores the value of digital awareness campaigns, technological protection, and behavioural preventive actions to minimize vulnerability and increase cybersecurity in South Africa. This study further contributes by differentiating between phishing, smishing, and vishing within the South African context and applying Routine Activity Theory to explain victim vulnerability in a developing digital economy.

Keywords

Phishing, Smishing, Vishing, Cybercrime, Digital Literacy, South Africa, Victim Vulnerabilities

1. Introduction

Crime continues to evolve rapidly, with offenders constantly adopting new and sophisticated methods to strengthen their criminal activities. As criminals become more technologically advanced, ordinary citizens are increasingly at risk of vic-

timisation. Among the fastest-growing threats is cybercrime, which has expanded significantly as society becomes more digitally dependent. International research highlights cybercrime as a growing global concern, and South Africa has witnessed a notable rise in phishing, smishing, and vishing cases (Pigola & Rezende da Costa, 2023). Mpuru and Kgoale (2025) observe that cybercrime across Africa has become more complex as organised networks diversify their techniques. They further note that public discourse often portrays the continent as a central hub of cybercriminal activity. Interpol statistics reinforce this perception: South Africa recorded approximately 230 million cyber-threat detections, followed by Kenya with 72 million and Morocco with 71 million, while Nigeria ranked fifth globally for the range of cybercrimes committed within its borders (Mpuru & Kgoale 2025).

These attacks exploit the widespread use of digital communication channels, such as email, mobile messaging, and telephone calls, to deceive individuals into revealing confidential information, including banking credentials, identification numbers, and access codes. Phishing commonly involves fraudulent emails or websites designed to imitate trusted institutions (Moore, 2010). Smishing employs similar tactics but is executed through SMS or instant messaging, while vishing relies on voice manipulation, often using calls that impersonate banks or government agencies (Kebande & Awad, 2024). The threat of such attacks continues to rise in South Africa as more people engage in digital activities such as mobile banking, e-government services, and online shopping. These environments expose individuals with limited cybersecurity knowledge, such as the elderly, students, and digitally inexperienced users, to heightened risk (Stefaniuk, 2020).

Understanding the strategies, behavioural patterns, and vulnerabilities associated with these attacks is essential for developing effective prevention measures. This paper reviews the literature to identify key trends, techniques, and implications of phishing, smishing, and vishing in the South African context.

1.1. Problem Statement

Despite advancements in cybersecurity, South Africa continues to experience significant financial and reputational harm from phishing, smishing, and vishing attacks (Weekes et al., 2025). Evidence gathered between November 2024 and May 2025 shows that these forms of social engineering account for 52% of all cyber threats in the country, almost double the global average of 28% (ESET, 2025). The groups most exposed to these attacks include older adults, students, and individuals with limited digital literacy. Although these crimes occur in digital environments, their impact is real and often undermines victims' privacy, finances, reputations, and broader sense of personal security (ESET, 2025).

South Africa primarily addresses these offenses through the Cybercrimes Act 19 of 2020, which criminalises illicit online activities and establishes clear procedures for reporting and investigating cyber-related offences. However, the persistent nature of cybercrime in the country suggests deeper, underlying challenges. Scholars emphasise that social and cultural dynamics within African contexts con-

tribute to the endurance of cybercrime. For instance, Akanle and Shadare (2019) note that some Nigerian "Yahoo boys" claim to rely on dark ritual practices often referred to as *voodoo* to influence or manipulate their victims, believing these rituals strengthen the success of their scams. Similar forms of online fraud have also been documented in countries such as Kenya and South Africa.

Low digital literacy, misplaced trust in online cues, and weak cybersecurity infrastructure further increase vulnerability across the region. These issues highlight a clear research gap: there is still limited understanding of the specific attack patterns, operational methods, and victimisation experiences shaping the South African cybercrime landscape.

1.2. Aim of the Study

This study aims to examine the prevailing trends, attack techniques, and victim vulnerabilities associated with phishing, smishing, and vishing in the South African context.

1.3. Research Questions

This study is guided by the following research questions:

1) What are the dominant methods used in phishing, smishing, and vishing attacks in South Africa?

2) What behavioural and socio-economic factors contribute to victim vulnerability in these attacks?

3) How do gaps in capable guardianship facilitate social engineering victimisation within the South African cyber landscape?

2. Literature Review

Phishing scams no longer exist in their crude form via email but have evolved into highly funded, targeted spear-phishing campaigns (Ram, 2025). Smishing and vishing occur within the context of mobile and voice technologies, where attackers exploit a sense of urgency, fear, or position to obtain sensitive information (Kebande & Awad, 2024). It has been found that the key tool in such attacks is social engineering, and criminals have been exploiting social trust rather than technical vulnerabilities (Stefaniuk, 2020).

Several factors contribute to the victim's vulnerability. Poor digital literacy hinders users' ability to detect fraudulent communications (Ram, 2025). They are also prone to influence due to cognitive biases, including an overconfidence effect when individuals identify a scam or believe in a well-known brand (Ram, 2025).

Users who are less tech-savvy, older people, and those in rural regions with less access to cybersecurity education are at a higher risk (Ram, 2025). The South African situation presents some challenges. Smishing attacks have found fertile ground in high mobile banking adoption, with little cybersecurity awareness campaigns (Ram, 2025). Phishing and vishing attacks have also been used in corporate bodies and government services, causing both data breaches and financial loss

(Stefaniuk, 2020).

2.1. Understanding Vulnerabilities and User Susceptibility to Phishing, Smishing, and Vishing in South Africa

In South Africa, vulnerabilities to phishing, smishing, and vishing stem from a range of factors influencing human susceptibility to these attacks. According to Mabitsela et al. (2025), key reasons for this vulnerability include a lack of knowledge about computer systems, limited awareness of security indicators, inadequate attention to the absence of such indicators, and the increasing sophistication of spoofed sites, which poses a significant threat. Pigola & Rezende da Costa (2023) emphasize the pivotal role that knowledge and experience play in reducing susceptibility to phishing attempts. Systemic issues, such as inadequate internal control procedures, make it easier for phishers to compromise systems (Mabitsela et al., 2025).

Phishing thrives in environments lacking established protocols, and when individuals are unaware of company policies, they become attractive targets for phishers (Pigola & Rezende da Costa, 2023). Furthermore, many users do not know which channels to use to report fraud or account maintenance issues, leaving them vulnerable. User susceptibility is shaped by cognitive factors, emotional responses, and volitional behaviour, leading to actions that are often irrational when faced with a decision (Huitt, 2012). Even with advanced technical safeguards, infiltration may occur if users fall for phishing attempts (Hong, 2012). Organizations depend on employees as the first line of defence against phishing emails, yet social engineering tactics exploit human emotions, undermining this security measure.

Different personality types exhibit unique responses to phishing emails; conformists may align with others' behaviour, while selfish individuals prioritize personal interests in their decision-making. Consistent individuals tend to stick to known behaviours, and rule-of-thumb thinkers rely on initial instincts or established rules (Green & Dorey, 2016). The rapid advancement of technology, particularly the Internet and smartphones, has significantly altered the threat landscape, facilitating faster, more anonymous communication that is attractive to cybercriminals (Alazab et al., 2013).

The discussion surrounding the impacts of phishing extends beyond financial loss to include breaches of sensitive data, reputational damage, and business disruption. The legal framework, such as the Protection of Personal Information Act (POPIA), underscores the need for organizations to handle personal information responsibly to avoid violations (Buys, 2017). Ultimately, addressing the multifaceted nature of these vulnerabilities requires ongoing awareness-raising, user education, and the implementation of robust security measures to mitigate the risks associated with phishing, smishing, and vishing.

2.2. Differentiating Phishing, Smishing, and Vishing in South Africa

While phishing, smishing, and vishing all fall under social engineering attacks,

they differ in communication channels, execution, and victim targeting strategies.

Phishing typically occurs through fraudulent emails or websites that mimic legitimate institutions such as banks or government services. Victims are often prompted to disclose login credentials or financial information. In South Africa, phishing frequently targets individuals engaged in online banking and e-commerce activities (Gan, Lee, & Liew, 2024).

Smishing involves SMS-based attacks, where victims receive text messages containing malicious links or urgent prompts, such as fake delivery notifications or banking alerts. Due to high mobile phone penetration in South Africa, smishing disproportionately affects mobile-first users and individuals with lower levels of digital literacy (Mabitsela et al., 2025).

Vishing occurs through voice calls, where offenders impersonate trusted entities such as bank officials or law enforcement agents. These attacks rely on real-time interaction and are particularly effective against elderly individuals and those less familiar with digital security practices (Pigola & Rezende da Costa, 2023).

Although these attack types differ in execution, they share common psychological manipulation tactics, including urgency, fear, authority, and familiarity, which significantly increase victim susceptibility.

3. Theoretical Framework

The research paper draws upon the Routine Activity Theory (RAT) to understand the patterns of victimization. RAT was initially presented by Cohen and Felson in 1979 to analyse and elucidate the concept of victimization. This theory posits that crime occurs when motivated offenders meet suitable targets in the absence of capable guardians. The theory acknowledges the impact of daily life activities on crime opportunities. It posits that crime rates and patterns result from the daily activities of individuals (such as employment, shopping, banking), which converge with offenders and potential targets in both space and time. RAT was initially formulated to better understand the dynamics of contact crimes, which require interaction between offenders and victims; however, it has also proven helpful for elucidating incidents of cyber victimization (Suzuki, Shikata, & Shimada, 2025). According to the RAT, societal and structural changes, such as those driven by technology, may increase the convergence of motivated criminals and suitable targets, thereby increasing victimization. Considering the lack of competent online guardians and the wide range of daily activities performed by users, the Internet enhances the "visibility" and "accessibility" of criminal targets (Maimon et al., 2021).

The application of Routine Activity Theory in this study enables a structured understanding of how cybercrime victimisation occurs when motivated offenders exploit suitable targets in the absence of capable guardianship within digital environments.

3.1. Motivated Offenders

The presence of likely offenders is often facilitated by the increasing number of

people using the Internet, which in turn increases the number of individuals with the technological knowledge to commit cyber offences. In relation to the study, Offenders use technological vulnerabilities, such as Voice over Internet Protocol (VoIP) and SMS gateways, to spoof caller IDs and sender information, making calls and messages look legitimate and evading specific security measures (Gan, Lee, & Liew, 2024). Phishing, smishing, and vishing attackers exploit trust and use social engineering tactics, such as creating a sense of urgency or fear, for example, alluding that "your account is compromised, act now", which manipulates victims into acting quickly and supersedes their rational decision-making. Williams (2016) asserts that all internet users likely have the advantage of anonymity and no geographical limitations. This, therefore, allows offenders to avoid detection or criminal charges because law enforcement agencies are hindered by jurisdictional, legislative, and evidentiary issues. Phishing can be acquired online and requires a minimum level of experience to utilise; therefore, it is usually the most omitted cybercrime offense in South Africa. According to Williams (2016), the motivational elements common to all types of cyber offenders are financial strain, power over others, and the gratification obtained from manipulating people and situations.

3.2. A Suitable Target

An appropriate target is an individual or asset that appeals to the perpetrator and is susceptible to assault. In the context of the study, the target is frequently an individual who is digitally vulnerable and heavily uses online services (Gan, Lee, & Liew, 2024). Increased online engagement, including extended durations spent on computers, banking, online shopping, and communication, amplifies vulnerability to potential offenders. Suitable targets for phishing include accounts maintained at financial institutions and online businesses, such as banks, which frequently encounter identity theft among their customers due to phishing attacks. The number of suitable targets increases as more people use the Internet and internet banking. A lack of knowledge and awareness of cybercrimes, as well as outdated security systems, are other factors that heighten susceptibility to cyberattacks (Khadka, Ullah, & Marroquin, 2025; Wannenburg, Nieman, & Wannenburg, 2023).

3.3. Absence of a Capable Guardian

Lack of Capable guardianship indicates the absence of security or monitoring that could prevent criminal activity. Security mechanisms, such as firewalls, antivirus software, and email filters, as well as individuals (like police, security guards, friends, or family), can serve as guardians against criminal activity. To protect digital assets, reduce vulnerabilities, and ensure a robust defence against cyber threats, capable guardianship requires competent and proactive management of online security measures. According to RAT, inadequate security management raises the risk of online victimization for Internet users. The likelihood of falling

victim to cybercrime, especially phishing, is decreased by effective online security management (such as online privacy) (Gan, Lee, & Liew, 2024). As phishing, smishing, and vishing often rely on attacks that exploit aspects of human nature rather than technical vulnerabilities, a capable guardian can be created by providing the public with information and awareness, rather than relying solely on security software. Williams (2016) argues that increasing public awareness of potential victimization enhances a person's ability to act as a responsible guardian. However, it is crucial to remember that many people use the Internet in various ways to accomplish their work-related activities every day. Responding to and answering emails is one such task. Employees are frequently overwhelmed by both legitimate and fraudulent emails during the workday, despite having received training to identify phishing emails. As a result, target suitability may be increased for individuals who regularly use the Internet for work or education. Maimon et al. (2021) state that the combination of social engineering and technical elements used by criminals in phishing may render guardianship in the more conventional sense (i.e., antivirus software) ineffective. Network administrators must therefore recognize and mitigate risk factors resulting from both technical and human vulnerabilities to prevent cyber offenses (Maimon et al., 2021).

Additionally, people can employ target hardening by using firewalls and passwords. 'Deflecting offenders' is another crime-prevention strategy that aims to reduce criminal opportunities. Using email filters is one way to deflect phishing attacks. Email filters are effective in preventing spam and stopping phishing attempts. However, specific phishing attacks may go unnoticed due to email filters' limited ability to identify authentic messages (Williams, 2016).

4. Methodology

This study employed a qualitative desktop review methodology to synthesise existing literature and information on phishing, smishing, and vishing attacks within the South African context. A desktop review entails the systematic collection, evaluation, and analysis of secondary data sources, including peer-reviewed journal articles, industry reports, government publications, and relevant online materials (Digital Service Design Office, 2023).

This method was selected for its efficiency in accessing and integrating a broad range of existing knowledge without primary data collection. Sources were included based on their relevance, credibility, and recency, with a focus on publications from the past five years to date to ensure that the review captured contemporary developments in social engineering attacks in South Africa. The selection process was conducted manually by the researchers, who critically assessed each identified source for suitability and relevance to the study objectives. Data extracted through this process were subjected to thematic content analysis, enabling the identification of recurrent patterns, themes, and categories across the reviewed literature, thereby providing a comprehensive overview of incidents, methods, and vulnerability of phishing, smishing, and vishing attacks.

The search for relevant literature was conducted using a combination of keywords, including "phishing", "smishing", "vishing", "social engineering", "cyber fraud", "cyber victimization", "online scams", and "South Africa". These keywords were applied across multiple platforms, including academic databases, institutional repositories, and recognized online sources, ensuring comprehensive coverage of pertinent literature. To enhance the breadth and precision of the search results, Boolean operators and keyword variations were used.

Key academic databases such as Google Scholar, as well as institutional library databases, were utilized in conjunction with reports from cybersecurity organizations, financial institutions, and government departments. The selection of sources was systematically narrowed through an initial review of titles and abstracts, followed by a full-text assessment to verify the relevance aligned with the study's focus on victim vulnerability, attack techniques, and preventive measures against these cyber threats. Only sources that were available in English and considered methodologically and contextually relevant to the South African context were incorporated into the final analysis. This rigorous approach ensured that the included literature effectively captured the complexities of cyber victimization within the specified geographical setting, ultimately enriching the study's findings.

Inclusion and Exclusion Criteria

The study included peer-reviewed journal articles, industry reports, and policy documents published between 2015 and 2025. Only English-language sources focusing on social engineering and cybercrime were included. Sources lacking relevance to phishing, smishing, or vishing, or not applicable to South Africa or similar contexts, were excluded.

Data Sources and Search Strategy

Literature was collected from databases such as Google Scholar, institutional repositories, and cybersecurity reports. Keywords included "phishing South Africa", "smishing attacks", "vishing fraud", and "cyber victimisation". Boolean operators were used to refine search results.

Screening Process

A three-stage screening process was followed. Initially, 40 sources were identified, and 30 were retained after screening for relevance.

Data Analysis

Thematic content analysis was employed. Data were coded into recurring patterns such as urgency tactics, authority exploitation, and technological enablers. Routine Activity Theory guided the categorisation into motivated offenders, suitable targets, and absence of capable guardianship.

To enhance reliability, a subset of sources was re-analysed to ensure consistency in coding and theme development.

5. Integrated Findings and Discussion

This qualitative analysis highlights how phishing, smishing, and vishing victimi-

zation significantly impact individuals' lives in South Africa. The findings reveal that these experiences are often driven by social and behavioural dynamics associated with routine digital interactions, rather than by mere technical failures. By applying Routine Activity Theory (RAT), the discussion fosters an understanding of how motivated offenders, suitable targets, and gaps in guardianship converge in everyday digital practices, encouraging the audience to recognize victims as real people.

The analysis indicates that regular interactions across digital communication platforms, such as mobile banking apps, email services, instant messaging apps, and phone calls, heighten consumers' susceptibility to motivated offenders. These interactions often occur under conditions of urgency, distraction, or emotional stress, which can diminish individuals' ability to critically evaluate messages and lead to hasty responses to fraudulent communications. A key theme of RAT is that individuals become suitable targets not only through negligence but also through a structural reliance on digital systems within a highly interconnected environment (Cohen & Felson, 1979). This dependence makes them more vulnerable to offenders' manipulative tactics.

Moreover, the findings show that motivated offenders effectively exploit cognitive biases and emotional responses, leveraging elements such as fear, urgency, authority, and familiarity to their advantage (Bada, Sasse, & Nurse, 2020). While there is a general awareness of cybercrime threats, research indicates a significant gap between this awareness and the protective behaviours individuals adopt. Emotional appeals often compromise rational decision-making, leading to victim compliance even among those who can recognize typical scam indicators. This emphasizes that the behavioural aspects of victimization cannot be adequately addressed solely through technical safeguards.

A significant outcome of this analysis is the fragmented and inconsistent state of capable guardianship within South Africa's digital landscape. Although technical safeguards, such as spam filters, antivirus software, and authentication mechanisms, exist, they are frequently poorly implemented and not adequately supported by essential organizational controls, behavioural training, or institutional response strategies (Weekes et al., 2025). The absence of robust public reporting pathways and victim support systems exacerbates initial victimization and increases the likelihood of repeat targeting. This highlights a critical need for enhanced capable guardianship that extends beyond technology to include behavioural awareness and institutional support.

The integration of these findings strongly confirms the relevance of the Routine Activity Theory in understanding contemporary social engineering cybercrimes. Motivated offenders navigate an environment characterized by anonymity and a low perceived risk of detection, while suitable targets are created through habitual online behaviour. The failures of capable guardianship across technical, organizational, and institutional levels are evident (Reyns, Henson, & Fisher, 2011). This research paper expands the applicability of RAT, illustrating its relevance beyond

traditional contact crimes and offering a victim-centred perspective on cybercrime.

The results robustly support the application of RAT to explain victimization from phishing, smishing, and vishing within South Africa's cyber landscape. The interplay among motivated offenders, suitable targets, and insufficient guardianship is well-documented, reaffirming the theory's applicability beyond conventional crime contexts. Offenders exploit anonymity and minimal perceived risk, along with the complexities of jurisdictional boundaries in cyberspace. Advances in communication technology, such as Voice over Internet Protocol (VoIP), SMS gateways, and AI-assisted messaging, have increased offenders' ability to impersonate trusted institutions, reducing operational challenges and enhancing the credibility and success rates of social engineering attacks (Bada, Sasse, & Nurse, 2020).

The emergence of suitable targets is not merely a product of individual negligence; it stems from a structural reliance on digital infrastructure. In South Africa, the widespread adoption of mobile banking, easy access to digital services, and the ubiquity of instant communication tools enhance the visibility and accessibility of potential victims (Pigola & Rezende da Costa, 2023). Routine online behaviour, especially when compounded by varying levels of digital literacy, positions ordinary users as attractive targets for social engineering schemes.

The noticeable lack of capable guardianship presents a crucial vulnerability. While technological controls are essential, guardianship must also encompass behavioural awareness, organizational accountability, and institutional support. Strengthening these areas can build trust among users, encourage organizations to take a proactive role in safeguarding digital communities, and reinforce collective efforts against cybercrime.

To effectively address the barriers that prevent individuals from reporting cybercrime incidents, it is vital to understand the underlying factors that drive this reluctance. Awareness campaigns should be organized to raise public knowledge about the importance of reporting cybercrime and the support available (Reyns, Henson, & Fisher, 2011). This entails emphasizing the anonymity and confidentiality of reporting processes as well as elucidating the consequences of failing to report incidents for both individuals and the broader community.

Collaborating with community leaders and influencers can help break down stigma and create an environment where victims feel empowered to come forward. Cultural factors significantly shape perceptions of cybersecurity and protective behaviours (Mabitsela et al., 2025). Educational programs must be tailored to resonate with diverse communities, incorporating locally relevant examples, addressing specific concerns, and using appropriate language to enhance accessibility and comprehension.

On the technological front, developing automated systems that leverage artificial intelligence (AI) and machine learning to detect social engineering attacks in real time can significantly improve response times. These solutions could analyse

communication patterns for anomalies indicative of phishing or vishing attempts and provide instant alerts to potential victims (Li et al., 2025). The implementation of AI-powered chatbots can also help individuals identify suspicious messages and outline steps to report incidents. By prioritizing proactive measures, such technologies can empower users and bolster overall cybersecurity defences in South Africa.

These findings align with Routine Activity Theory, demonstrating that cyber victimisation occurs when motivated offenders exploit suitable targets in the absence of effective digital guardianship, particularly within routine online interactions.

6. Study Contribution

This study makes three significant contributions to the literature on cybercrime and victimization. First, it presents a victim-centred perspective on phishing, smishing, and vishing in the South African context, shifting the focus from financial implications alone to victims' behavioural and emotional vulnerabilities. Second, it extends the application of Routine Activity Theory to contemporary social engineering threats by demonstrating how routine digital practices actively create suitable targets in environments characterized by fragmented guardianship. This study further contributes by providing a differentiated analysis of phishing, smishing, and vishing within South Africa and linking specific vulnerabilities to targeted intervention strategies.

Finally, this study integrates both academic and industry evidence to offer context-sensitive insights relevant to policy development, awareness initiatives, and institutional responses in the Global South.

7. Recommendations

Given these insights, several recommended actions can strengthen protection for individuals against phishing, smishing, and vishing in South Africa. Firstly, targeted digital literacy and awareness programs must be prioritized. Awareness efforts should go beyond generic alerts and target vulnerable groups, including older adults, students, rural communities, and employees of small- to medium-sized enterprises. These outreach programs should emphasize recognizing social engineering strategies, emotional manipulation tactics, and cues of urgency rather than focusing solely on technical warning signs.

Secondly, organizations should incorporate behaviour-based cybersecurity training into their operational frameworks. These training initiatives should address cognitive biases and decision-making under pressure, preparing users to pause, verify, and report any suspicious communications. Implementing phishing simulations and scenario-based learning can bolster practical skill development and promote long-term behavioural changes (Pigola & Rezende da Costa, 2023).

Thirdly, strengthening capable guardianship requires heightened institutional coordination. Financial institutions, telecommunications companies, and governmental bodies should work together to create clear, accessible, and well-publicized

reporting pathways for suspected fraud. Prompt response mechanisms and victim support systems could significantly reduce harm, facilitate recovery efforts, and enhance users' trust in digital platforms (Kebande & Awad, 2024).

Fourthly, there is a pressing need for improved policy implementation and enforcement to prevent cybercrime. This necessitates a coherent alignment among the Cybercrimes Act, Protection of Personal Information Act (POPIA) compliance mechanisms, and victim-support frameworks to ensure effective prevention, accountability, and redress. Regulatory bodies must assume a more visible role in fostering public education and ensuring institutional accountability.

Based on the findings, targeted interventions are required across multiple sectors. Financial institutions should implement real-time fraud detection systems and strengthen customer alert mechanisms to mitigate phishing attacks. Telecommunications providers must enhance SMS filtering technologies to detect and block smishing campaigns. Government agencies should develop national cybersecurity awareness programmes targeting vulnerable populations, including elderly individuals and digitally inexperienced users.

Employers should implement behaviour-based cybersecurity training programmes that address cognitive biases and decision-making under pressure. Individuals should adopt precautionary behaviours such as verifying communications and avoiding impulsive responses to urgent requests.

Strengthening coordination between banks, telecommunications providers, and law enforcement agencies is essential to improving reporting mechanisms and response times. These targeted interventions directly address vulnerabilities identified within the Routine Activity Theory framework by enhancing capable guardianship.

Finally, future research should prioritize empirical qualitative studies that delve into victim narratives and lived experiences. Research that captures these perspectives will deepen understanding of the emotional impacts, reporting behaviours, and coping strategies of individuals affected by cyber victimization. This approach would complement existing quantitative analyses and contribute to a more comprehensive understanding of the issue (Weekes et al., 2025).

8. Study Limitations

Despite its contributions, this study is not without limitations. As a qualitative desktop analysis, its findings derive from secondary sources and thus do not capture first-hand narratives or the lived experiences of cybercrime victims. While this approach permits broad synthesis, it hinders insights into individual coping mechanisms, behaviours following victimization, and the overall impacts experienced. Additionally, reliance on industry reports, while vital in a rapidly evolving field, may introduce reporting biases or undercount instances of informal victimization. These limitations underscore the necessity for future empirical qualitative and mixed-methods research centred on victim experiences across diverse South African contexts.

9. Conclusion

In conclusion, this study has investigated phishing, smishing, and vishing victimization in South Africa through a qualitative desktop analysis of existing literature. Guided by Routine Activity Theory, the research paper has demonstrated that cyber victimization is shaped by the convergence of routine digital activities, motivated offenders, and inadequate guardianship. The findings emphasize that social engineering attacks largely succeed by exploiting human behaviour, emotional responses, and structural reliance on digital systems rather than merely overcoming technical defences. Although awareness of cybercrime is widespread, significant gaps between knowledge and safe behavioural practices persist, highlighting the limitations of technology-centred preventive strategies.

By adopting a victim-centred analytical lens, this study contributes to the understanding of South African cybercrime scholarship by emphasizing the psychological, behavioural, and social dimensions of cyber victimization. The insights derived highlight the imperative for integrated prevention approaches that fuse digital literacy, behavioural awareness, organizational responsibility, and effective policy implementation. As South Africa's digital ecosystem continues to expand, enhancing capable guardianship and empowering users are crucial steps in reducing vulnerability and mitigating the escalating threat posed by phishing, smishing, and vishing attacks.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

Akanle, O., & Shadare, B. R. (2019). Yahoo-Plus in Ibadan: Meaning, Characterization and Strategies. *International Journal of Cyber Criminology, 13,* 343-357.

Alazab, M., Layton, R., Broadhurst, R., & Bouhours, B. (2013). Malicious Spam Emails Developments and Authorship Attribution. In *2013 Fourth Cybercrime and Trustworthy Computing Workshop* (pp. 58-68). IEEE. https://doi.org/10.1109/ctc.2013.16

Bada, A., Sasse, A. M., & Nurse, J. R. C. (2020). Cybersecurity Awareness Campaigns: Why Do They Fail? Information Fusion. https://efaidnbmnnnibpcajpcglclefind-mkaj/https://www.cs.ox.ac.uk/files/7194/csss2015_bada_et_al.pdf

Buys, R. (2017). *Cyberlaw @ SA IV: The Law of the Internet in South Africa*. Van Schaik Publishers.

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review, 44,* 588-608. https://doi.org/10.2307/2094589

Digital Service Design Office (2023). *Desktop Research Methodology Guidelines*. Government of New South Wales. https://www.digital.nsw.gov.au

ESET (2025). *Phishing Accounts for More than Half of South Africa's Cyber Threats, Double the Global Average-ESET Bi-Annual Threat Report 2025*. https://www.eset.com/za/about/newsroom/press-releases-za/press-releases/hook-line-

and-sinker-sas-phishing-crisis-deepens

Gan, C. L., Lee, Y. Y., & Liew, T. W. (2024). Fishing for Phishy Messages: Predicting Phishing Susceptibility through the Lens of Cyber-Routine Activities Theory and Heuristic-Systematic Model. *Humanities and Social Sciences Communications, 11,* Article No. 1552. https://doi.org/10.1057/s41599-024-04083-1

Green, J. S., & Dorey, P. (2016). *The Weakest Link: Why Your Employees Might Be Your Biggest Cyber Risk*. Bloomsbury Publishing.

Hong, J. (2012). The State of Phishing Attacks. *Communications of the ACM, 55,* 74-81. https://doi.org/10.1145/2063176.2063197

Huitt, W. (2012). *A Holistic View of Education and Schooling: Guiding Students to Develop Capacities, Acquire Virtues, and Provide Service*. Revision of Educational Psychology Interactive, Valdosta State University. https://www.edpsycinteractive.org/papers/holistic-view-of-schooling-rev.pdf

Kebande, V. R., & Awad, A. I. (2024). Industrial Internet of Things Ecosystems Security and Digital Forensics: Achievements, Open Challenges, and Future Directions. *ACM Computing Surveys, 56,* 1-37. https://doi.org/10.1145/3635030

Khadka, K., Ullah, A. B., & Martinez Marroquin, E. (2025). Unmasking Persuasion in Phishing: A Content Analysis of Principles of Persuasion in Emails and Subject Lines. *Information & Computer Security, 34,* 104-121. https://doi.org/10.1108/ics-12-2024-0321

Li, K., Li, C., Yuan, X., Li, S., Zou, S., Sohail Ahmed, S. et al. (2025). Zero-Trust Foundation Models: A New Paradigm for Secure and Collaborative Artificial Intelligence for Internet of Things. *IEEE Internet of Things Journal, 12,* 46269-46293. https://doi.org/10.1109/jiot.2025.3603957

Mabitsela, I., Lekgau, T., & Matome, M. J. (2025). *Defending against Fraud: Cyber Fraud Detection and Prevention Techniques*. SSRN. https://doi.org/10.2139/ssrn.5652552

Maimon, D., Howell, C. J., Perkins, R. C., Muniz, C. N., & Berenblum, T. (2021). A Routine Activities Approach to Evidence-Based Risk Assessment: Findings from Two Simulated Phishing Attacks. *Social Science Computer Review, 41,* 286-304. https://doi.org/10.1177/08944393211046339

Moore, T. (2010). The Economics of Cybersecurity: Principles and Policy Options. *International Journal of Critical Infrastructure Protection, 3,* 103-117. https://doi.org/10.1016/j.ijcip.2010.10.002

Mpuru, L., & Kgoale, C. (2025). Recognizing the Evolving Cybercrime Threats in South Africa. *African Security, 19,* 36-60. https://doi.org/10.1080/19392206.2025.2515302

Pigola, A., & Rezende da Costa, P. (2023). Dynamic Capabilities in Cybersecurity Intelligence: A Meta-Synthesis to Enhance Protection against Cyber Threats. *Communications of the Association for Information Systems, 53,* 1099-1135. https://doi.org/10.17705/1cais.05347

Ram, A. (2025). Navigating the Phishing Threat Landscape: A Comprehensive Survey of Techniques, Trends, and Countermeasures. *International Journal of Computer Science and Security, 19,* 167-199. https://mail.cscjournals.org/manuscript/Journals/IJCSS/Volume19/Issue5/IJCSS-1755.pdf

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being Pursued Online: The Role of Routine Activities in the Occurrence of Cyberstalking. *Criminal Justice and Behavior, 38,* 1149-1169. https://doi.org/10.1177/0093854811421448

Stefaniuk, T. (2020). The Analysis of Behavior of Internet Users from the Perspective of

Safety. *Safety & Defense, 6,* 63-76. https://doi.org/10.37105/sd.62

Suzuki, A., Shikata, K., & Shimada, T. (2025). Patterns and Predictors of Cyber Fraud Victimization: Testing Routine Activity Theory and General Theory of Crime in Japan. *Journal of Economic Criminology, 9,* Article ID: 100186. https://doi.org/10.1016/j.jeconc.2025.100186

Wannenburg, M. C., Nieman, A., Steyn, B., & Wannenburg, D. G. (2023). South Africans' Susceptibility to Phishing Attacks. *Southern African Journal of Accountability and Auditing Research, 25,* 53-72. https://doi.org/10.54483/sajaar.2023.25.1.4

Weekes, C. J., Storey, J. E., & Pina, A. (2025). Cyberstalking Perpetrators and Their Methods: A Systematic Literature Review. *Trauma, Violence, & Abuse,* 1-17. https://doi.org/10.1177/15248380251333411

Williams, M. L. (2016). Guardians upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level. *British Journal of Criminology, 56,* 21-48. https://doi.org/10.1093/bjc/azv011