Kabarak Journal of Research & Innovation Volume 16 Number 2 (2026)
ISSN 2305-784X (print) ISSN 2410-8383 (online)
https://journals.kabarak.ac.ke/index.php/kjri/

Factors Contributing to Vulnerability Towards Social Engineering Attacks Among Kenyan Social Media Users

Authors:
Julius Sirma[1], Patrick K. Wumuyu[1] and Dalton Ndirangu[1]

Affiliations:
[1]USIU-Africa

Corresponding Author:
Julius Sirma –E-mail: julius.sirma@gmail.com

Article History: *Submitted: 6th December 2025; Accepted: 23rd April 2026; Published (online): 9th July 2026*

Abstract

This study examined factors contributing to vulnerability towards social engineering attacks among Kenyan social media users. The research problem centers on identifying the underlying human, technological, and institutional factors that increase susceptibility to online manipulation. Using a systematic literature review approach, the study synthesizes existing research and organizes findings into six key themes: awareness and education, trust in online interactions, technological proficiency, socio-economic influences, behavioral traits, and regulatory frameworks. The findings reveal that limited cybersecurity awareness and low digital literacy significantly expose users to attacks, with many unable to recognize common threats. Cultural norms that promote trust and community further increase vulnerability, as attackers exploit these social dynamics. Additionally, socio-economic pressures encourage risky online behavior, while individual traits such as curiosity, overconfidence, and emotional responsiveness make users easier targets. The review also highlights gaps in public awareness campaigns and weaknesses in existing regulatory and institutional support systems. The study concludes that reducing vulnerability requires a comprehensive approach that combines user education, simplified and inclusive awareness strategies, stronger legal and institutional frameworks, and targeted interventions addressing behavioral and socio-economic risks.

Keywords
Social engineering, cybersecurity, social media, digital literacy, awareness campaigns, institutional support, cultural trust, behavioral traits

Introduction

The rapid expansion of internet technologies has fundamentally transformed communication patterns globally, with social media platforms becoming central to everyday interactions. In Kenya, increased internet penetration and mobile connectivity have accelerated the adoption of social media, making platforms such as WhatsApp, Facebook, and YouTube integral to communication, business transactions, and information sharing. According to DataReportal (2023), Kenya has experienced substantial growth in social media usage, driven largely by mobile internet access and affordable smartphones. Similarly, reports by the Communications Authority of Kenya (2022) indicate that mobile-based platforms dominate digital interactions, reflecting a highly connected population.

While this digital transformation has enhanced socio-economic participation, it has simultaneously exposed users to increasing cybersecurity risks. Among these, social engineering attacks have emerged as a significant threat. Social engineering refers to the manipulation of individuals into divulging confidential information or performing actions that compromise their security (Mitnick & Simon, 2011). Unlike conventional cyberattacks that exploit technical vulnerabilities, social engineering targets human behavior, making it particularly difficult to detect and prevent.

The evolution of cybercrime has shifted from basic activities such as spam messaging to more sophisticated forms including phishing, identity theft, and impersonation attacks (Hadnagy, 2018). Social media platforms have amplified these risks due to their interactive nature, high levels of trust among users, and the widespread sharing of personal information. Cybercriminals exploit these characteristics to craft convincing attacks that rely on deception, urgency, and social influence, often targeting individuals perceived to have lower resistance or awareness (Jagatic et al., 2007).

In the Kenyan context, the widespread use of mobile technologies and mobile money services such as M-Pesa has created unique vulnerabilities. Social engineering attacks frequently involve fraudulent messages or calls impersonating financial institutions or mobile service providers, prompting users to transfer money or reveal sensitive information. Studies have shown that attackers exploit trust in familiar communication channels such as SMS and WhatsApp, increasing the likelihood of successful deception (Kigen et al., 2021). This highlights the intersection between technological adoption and user behavior in shaping cybersecurity risks.

Social media-related risks can broadly be categorized into technological and behavioral dimensions. Technological risks include malware, unauthorized access, and system vulnerabilities, while behavioral risks arise from user actions such as oversharing information, interacting with unknown individuals, and responding to unsolicited requests (Albladi & Weir, 2020). Social engineering attacks primarily exploit these behavioral vulnerabilities, demonstrating that technical safeguards alone are insufficient to mitigate cyber threats.

Despite growing awareness of cybersecurity risks, social engineering attacks continue to succeed at a significant rate. This persistence suggests the existence of an “awareness-behavior gap,” where users possess basic knowledge of cyber threats but fail to translate this awareness into secure online practices. Factors such as overconfidence, urgency, financial pressure, and trust in

social networks often influence decision-making, increasing susceptibility to manipulation (Vishwanath et al., 2018).

In Kenya, socio-cultural dynamics further contribute to vulnerability. Strong community-oriented values, such as collective responsibility and trust, can inadvertently be exploited by cybercriminals who impersonate friends, family members, or community figures. Additionally, the rapid digitalization of services has occurred alongside varying levels of digital literacy. While many users are proficient in navigating social media platforms, they may lack critical cybersecurity skills, such as identifying phishing attempts or verifying the authenticity of online communications.

Furthermore, the "leapfrogging" nature of Kenya's digital development—where many users transitioned directly to mobile internet without prior exposure to traditional computing environments—has resulted in a gap between platform usage and cybersecurity awareness. This disparity increases vulnerability, as users may be unfamiliar with underlying security concepts such as secure authentication, data privacy, and risk identification.

Consequently, the growing prevalence of social engineering attacks in Kenya cannot be fully understood without examining the interplay between technological, behavioral, and socio-economic factors. Addressing these vulnerabilities requires a shift from purely technical solutions to a more holistic approach that considers user behavior, cultural context, and institutional frameworks.

Social media platforms have become central to communication, information exchange, and socio-economic interactions. However, their widespread use has also introduced significant cybersecurity risks, particularly those associated with human-centered attacks such as social engineering. User vulnerability in this context refers to the susceptibility of individuals to manipulation techniques that lead them to disclose sensitive information or perform actions that compromise their security (Albladi & Weir, 2020).

Unlike traditional cyber threats that exploit technical system weaknesses, social engineering attacks primarily target human behavior, decision-making processes, and social interactions. Social media environments amplify these risks due to high levels of trust, informal communication, and extensive sharing of personal information. Users frequently disclose identifiable data such as birthdays, contact details, and location information, which attackers can exploit to design highly personalized and convincing attacks (Hadnagy, 2018; Jagatic et al., 2007).

A key determinant of vulnerability is the level of cybersecurity awareness among users. Although many individuals possess basic knowledge of online risks, they often lack the skills required to identify sophisticated threats such as phishing, impersonation, and malicious links. This gap between knowledge and actual behavior commonly referred to as the "awareness-behavior gap"—has been identified as a major contributor to successful social engineering attacks (Vishwanath et al., 2018).

Behavioral factors further influence susceptibility to social engineering. Users are more likely to trust communications received from familiar platforms or known contacts, reducing their likelihood of verifying the authenticity of messages. Social engineers exploit psychological

triggers such as urgency, fear, authority, and curiosity to manipulate user responses and bypass rational decision-making processes (Cialdini, 2009; Workman, 2008). For example, fraudulent messages that simulate emergencies or financial incentives can prompt immediate action without adequate verification.

Socio-cultural factors also play a significant role in shaping user vulnerability. In many societies, including Kenya, strong community ties and trust-based interactions encourage individuals to respond positively to requests from perceived acquaintances or authority figures. Attackers exploit these cultural norms by impersonating trusted individuals, organizations, or institutions, thereby increasing the likelihood of compliance (Albladi & Weir, 2020).

Technological factors further contribute to vulnerability. While many users demonstrate high levels of proficiency in using social media platforms, they often lack a deeper understanding of cybersecurity mechanisms such as secure authentication, data protection, and threat detection. This imbalance between platform usage and security awareness increases susceptibility to deception (Krombholz *et al*., 2015).

Additionally, the increasing reliance on mobile devices for accessing social media introduces unique security challenges. Mobile interfaces may limit users' ability to detect phishing indicators, verify URLs, or critically assess suspicious communications. In contexts such as Kenya, where mobile-based financial services like M-Pesa are widely used, cybercriminals frequently exploit SMS and messaging platforms to execute fraudulent schemes, including impersonation and mobile money scams (Kigen *et al*., 2021).

Addressing user vulnerability requires a comprehensive approach that extends beyond technical safeguards. While technological solutions such as encryption and multi-factor authentication are essential, they must be complemented by user-centered interventions, including cybersecurity education, awareness programs, and behavioral change strategies. Enhancing users' ability to critically evaluate online interactions and recognize manipulation techniques is crucial in reducing susceptibility to social engineering attacks (Albladi & Weir, 2020; Vishwanath et al., 2018).

The rapid growth of social media usage in Kenya has created new opportunities for communication, business, and information exchange. However, this increased digital engagement has also exposed users to a rising number of cybersecurity threats, particularly social engineering attacks. These attacks exploit human vulnerabilities such as trust, limited awareness, and behavioral tendencies rather than technical system weaknesses, making them highly effective and difficult to prevent (Albladi & Weir, 2020).

Despite increased awareness of cyber threats, social engineering attacks continue to succeed at a significant rate, indicating that awareness alone is insufficient to protect users. Existing studies suggest that individuals often possess basic knowledge of cybersecurity risks but fail to translate this knowledge into secure online behavior, resulting in what is commonly referred to as the "awareness–behavior gap" (Vishwanath *et al*., 2018). This gap is particularly critical in social media environments, where informal communication and trust-based interactions increase susceptibility to manipulation.

In the Kenyan context, the problem is further compounded by socio-economic and technological factors. The widespread use of mobile-based platforms and financial services such as M-Pesa has made social engineering attacks more financially motivated and immediate in impact, as cybercriminals can directly exploit users through fraudulent messages and impersonation schemes. Additionally, varying levels of digital literacy mean that while many users are proficient in using social media applications, they may lack the necessary skills to identify and respond to sophisticated cyber threats.

Empirical evidence also indicates that Kenyan social media users frequently encounter negative online experiences, including impersonation and deceptive interactions, which are closely linked to social engineering techniques (Wamuyu, 2020). However, existing research in Kenya has largely focused on general cybercrime trends or online harassment, with limited attention given to the specific factors that drive user vulnerability to social engineering attacks.

Furthermore, current countermeasures implemented by social media platforms and regulatory bodies remain fragmented and largely reactive. While technological safeguards have been introduced, they often fail to address the human and behavioral dimensions of cybersecurity. Users are frequently ill-equipped to recognize and respond to manipulation tactics, and reporting mechanisms remain underutilized due to complexity or lack of awareness.

Therefore, there is a critical need for a comprehensive analysis of the factors contributing to vulnerability towards social engineering attacks among Kenyan social media users. Understanding these factors is essential for developing targeted, context-specific interventions that go beyond technical solutions to address behavioral, socio-cultural, and technological drivers of vulnerability.

Methods

Study Design

This study employed a systematic literature review (SLR) design to synthesize existing knowledge on factors influencing vulnerability to social engineering attacks among Kenyan social media users. The design is appropriate because it enables a structured, transparent, and replicable process of identifying and analyzing relevant studies. The study was not confined to a physical setting but focused on published research within the domains of cybersecurity, information systems, and social media. The "participants" in this context were the selected peer-reviewed studies, which provided empirical and theoretical insights into user vulnerability.

Participants and Sampling

The target population comprised all scholarly publications addressing social engineering, cybersecurity, and user vulnerability in digital or social media contexts. The sampling frame included studies retrieved from selected academic databases. A purposive sampling technique

was applied, guided by predefined inclusion and exclusion criteria to ensure relevance and quality. Only studies that directly addressed social engineering and user susceptibility within the defined scope were included, resulting in a final sample of 25 studies.

Data Collection Instruments

A data extraction form was used as the primary tool for collecting relevant information from the selected studies. The form captured study characteristics such as objectives, methodology, context, and key findings. Validity was ensured through alignment of the extraction tool with the study objectives, while reliability was enhanced by applying a consistent extraction procedure across all studies. The tool was adapted from standard SLR guidelines to suit the focus on cybersecurity and social engineering.

Procedure

Data collection followed the PRISMA-guided process. First, studies were identified through database searches using predefined keywords. Second, duplicates were removed, followed by title and abstract screening to eliminate irrelevant studies. Third, full-text articles were assessed for eligibility based on inclusion criteria. Finally, the selected studies were systematically reviewed, and relevant data were extracted and organized for analysis.

Data Analysis

The study utilized thematic analysis to synthesize findings from the selected literature. Extracted data were coded and grouped into recurring categories reflecting factors influencing vulnerability. Patterns and relationships were identified across studies and organized into key themes. Since the study was qualitative in nature, no statistical tests were conducted, and therefore statistical indicators such as *p*, *M*, and *SD* were not applicable.

Ethical Considerations

This study relied exclusively on secondary data from published sources and therefore did not involve human subjects. As such, formal ethical approval was not required. However, ethical research standards were upheld by ensuring proper citation of all sources, avoiding plagiarism, and accurately representing the findings of the reviewed studies.

Limitations

The study is limited to secondary data and may be constrained by publication bias and the availability of Kenya-specific empirical studies.

Results

Overview of Findings

The systematic literature review identified six interrelated themes influencing vulnerability to social engineering attacks among Kenyan social media users: cybersecurity awareness and education gaps, socio-cultural trust dynamics, technological proficiency, socio-economic pressures, behavioral tendencies, and institutional and regulatory limitations. Across the 25 reviewed studies, the evidence consistently shows that vulnerability is multidimensional and results from the interaction of behavioral, technological, and contextual factors rather than a single cause.

Cybersecurity Awareness and Education Gaps

Findings indicate widespread deficiencies in cybersecurity awareness among social media users. Most studies show that users possess only basic knowledge of cyber threats and struggle to identify advanced social engineering techniques such as phishing and impersonation. A recurring gap exists between awareness and behavior, where users who understand risks still engage in unsafe practices. In the Kenyan context, awareness campaigns are reported to be uneven in reach, often overly technical, and less effective among rural and low-income populations.

Socio-Cultural Trust and Social Influence

The review reveals that trust-based social interactions significantly increase vulnerability. Users are more likely to respond to requests perceived as originating from familiar individuals or institutions. In Kenya, cultural norms emphasizing trust and community belonging amplify this effect. Attackers exploit these norms through impersonation and authority-based deception. However, trust alone is not a vulnerability; it becomes risky when combined with weak verification behavior and low cybersecurity awareness.

Technological Proficiency and Digital Literacy

The findings show a clear gap between social media usage skills and cybersecurity competence. While users are proficient in navigating platforms, they often lack the ability to detect threats such as phishing links and fake profiles. Rapid digital adoption has created a “usage–security gap,” particularly among mobile-first users who lack formal cybersecurity training. Lower digital literacy consistently correlates with higher susceptibility to attacks.

Socio-Economic Pressures

Socio-economic conditions significantly influence vulnerability. Individuals under financial strain are more likely to engage with fraudulent online opportunities, especially those promising quick financial gains. In Kenya, attackers frequently exploit mobile money systems and economic hardship through fake job offers and fraudulent financial alerts. Socio-economic pressure also intensifies psychological triggers such as urgency and reward expectation.

Behavioral and Psychological Factors

Behavioral traits such as curiosity, overconfidence, impulsivity, and urgency bias increase susceptibility to manipulation. Users who overestimate their ability to detect scams are more likely to fall victim to attacks. Emotional manipulation techniques—such as fear, authority, urgency, and greed—are widely used to bypass rational decision-making, increasing the success rate of phishing and impersonation attacks.

Institutional and Regulatory Constraints

Although cybersecurity policies and institutions exist, their effectiveness is constrained by weak enforcement and limited public awareness. Many users are unaware of reporting mechanisms or available support systems. Institutions such as the Kenya Computer Incident Response Team Coordination Centre play a key role in cybersecurity response, but their preventive reach remains limited compared to the scale of digital adoption.

Synthesis of Findings

Overall, vulnerability is driven by the interaction of multiple reinforcing factors. Limited cybersecurity awareness, high trust in social interactions, low digital literacy, and socio-economic pressure combine to create a persistent risk environment. These factors mutually reinforce each other, meaning that addressing vulnerability requires integrated behavioral, educational, and institutional interventions rather than isolated technical solutions.

Discussion

The findings of this systematic literature review demonstrate that vulnerability to social engineering attacks among Kenyan social media users is a multidimensional phenomenon shaped by the interaction of behavioral, technological, socio-cultural, socio-economic, and institutional factors. This finding is consistent with previous studies which argue that successful social engineering attacks exploit human psychology more than technological weaknesses (Hadnagy, 2018; Parsons et al., 2017). Across the reviewed studies, cybersecurity awareness and education

gaps emerged as the most dominant determinant of vulnerability. Similar findings have been reported by Wash and Cooper (2018) and Albladi and Weir (2020), who found that individuals with limited cybersecurity knowledge are significantly more susceptible to phishing and impersonation attacks. However, this review extends previous literature by demonstrating that awareness alone does not necessarily translate into secure online behavior. Several reviewed studies reported that users who were aware of common cyber threats continued to engage in risky practices such as responding to suspicious messages, clicking unknown links, or sharing personal information without verification. This supports the argument by West et al. (2021) that cybersecurity behavior is influenced not only by knowledge but also by cognitive biases, habits, and contextual pressures. Within the Kenyan context, awareness campaigns were also found to be unevenly distributed, with rural and low-income populations receiving limited exposure to practical cybersecurity education, suggesting that future interventions should focus on changing behavior rather than merely increasing awareness.

The review further established that socio-cultural trust and technological proficiency significantly influence users' susceptibility to social engineering attacks. Consistent with the findings of Jagatic et al. (2007) and Workman (2008), attackers exploit trust, authority, and familiarity to manipulate victims into disclosing confidential information. The reviewed studies indicate that Kenyan users are particularly vulnerable because strong community relationships and cultural norms emphasizing trust increase the likelihood of accepting requests appearing to originate from family members, employers, government agencies, or financial institutions. Nevertheless, this review demonstrates that trust alone does not necessarily lead to victimization; rather, vulnerability increases when trust is accompanied by weak verification practices and inadequate cybersecurity awareness. Similarly, the findings confirm previous research by Van Deursen and Van Dijk (2014), which distinguishes digital usage skills from cybersecurity competence. Although many Kenyan users are highly proficient in using smartphones and social media platforms, they often lack the security skills necessary to identify phishing links, fake accounts, and impersonation attempts. This "usage-security gap" appears particularly pronounced in Kenya, where rapid digital adoption through mobile technologies has outpaced investments in cybersecurity education, thereby creating an environment in which cybercriminals can easily exploit inexperienced users.

The review also found that socio-economic pressures and behavioral characteristics significantly increase vulnerability to social engineering attacks. These findings support previous studies by Williams et al. (2018), which showed that financial hardship increases susceptibility to fraudulent investment opportunities, fake employment offers, and financial scams. In Kenya, this vulnerability is amplified by widespread dependence on mobile money services, which cybercriminals exploit through fake transaction alerts, emergency financial requests, and fraudulent payment notifications. Unlike studies conducted in developed economies, the

reviewed literature highlights how economic challenges and digital financial inclusion interact to create unique opportunities for social engineering attacks within the Kenyan context. Furthermore, the findings reinforce earlier research by Vishwanath et al. (2016) and Canfield et al. (2017), which identified curiosity, impulsivity, urgency bias, fear, greed, and overconfidence as key psychological factors influencing phishing susceptibility. The review found that users who believed they could easily recognize scams often became less vigilant and were therefore more likely to become victims, demonstrating that confidence in one's cybersecurity abilities does not necessarily translate into safer online behavior.

Finally, the review established that institutional and regulatory limitations continue to undermine efforts to reduce social engineering attacks despite Kenya's progress in developing cybersecurity policies and institutions. While frameworks such as the Kenya Computer Incident Response Team Coordination Centre have strengthened national incident response capacity, several reviewed studies indicate that preventive initiatives remain inadequate relative to the rapid expansion of digital technologies. Similar implementation gaps have been reported in other developing countries, where cybersecurity strategies often prioritize incident response over public awareness and prevention. The findings therefore support Institutional Theory by suggesting that formal regulations alone are insufficient unless supported by effective enforcement, public education, and collaboration among government agencies, financial institutions, telecommunications companies, educational institutions, and social media platforms. Overall, this review contributes to existing knowledge by demonstrating that vulnerability to social engineering attacks is not driven by isolated factors but by the interaction of multiple reinforcing influences. Consequently, effective mitigation strategies should adopt an integrated approach that simultaneously strengthens cybersecurity awareness, digital literacy, behavioral resilience, socio-economic protection, and institutional capacity rather than relying solely on technical security measures.

Conclusion and Recommendations for Further Work

This systematic literature review concludes that vulnerability to social engineering attacks among Kenyan social media users is driven by a combination of cybersecurity awareness gaps, socio-cultural trust, low digital literacy, socio-economic pressures, behavioral tendencies, and institutional limitations. These factors interact to create a complex vulnerability ecosystem that cannot be addressed through single interventions. The study contributes to understanding cybersecurity risk in developing digital economies and highlights the need for integrated educational, behavioral, and policy-based interventions.

Future studies should adopt primary data approaches such as surveys or experiments to measure real-time user behavior and test intervention effectiveness.

Authorship Statement
The author conceptualized the study, conducted the literature search, performed screening and selection of studies, extracted and synthesized data, and wrote the manuscript.

Funding
This study received no external funding.

Declaration of Competing Interests
The author declares no competing interests.

Acknowledgements
The author acknowledges the contribution of academic databases and researchers whose work formed the foundation of this systematic review. Appreciation is also extended to academic supervisors and peers who provided guidance during the development of this study.

Author Contributions:
We the authors, declare that each author contributed significantly to the conception, research, writing and preparation of the final work.

Ethical Approval and Research License
The review adhered to established ethical principles for secondary research by accurately representing the findings of the included studies, properly acknowledging all sources through appropriate citation and referencing, and maintaining academic integrity throughout the research process.

Licensing Statement
© 2026 The Author(s). This article is published by Kabarak Journal of Research & Innovation (KJRI) under the Creative Commons Attribution 4.0 International (CC BY 4.0) License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author(s) and source are credited.

References

Albladi, N. J. & Weir, I. L. (2020). A Survey on Human and Personality Vulnerability Assessment in Cyber-security: Challenges, Approaches, and Open Issues. *Journal of Cryptography and Security, 2*(1), 23-56

Communications Authority of Kenya. (2022). *Cybersecurity report*. Nairobi, Kenya.

Cronbach, L. J. (2004). My Current Thoughts on Coefficient Alpha and Successor Procedures. *Educational and Psychological Measurement, 64*(3), 391 418.

Hadnagy, L. T (2018). *Strategies used to mitigate social engineering attacks*. Retrieved from: https://core.ac.uk/download/346462362.pdf.

Hadnagy, S. M., (2011). User characteristics that influence judgment of social engineering attacks in social networks. *Human-centric Computing and Information Sciences, 10*(1), 1–24.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Connecting the Actual with the Virtual: The Internet and Social Movement Theory in the Muslim World—The Cases of Iran and Egypt. *Social phishing*. *Communications of the ACM, 50*(10), 94–100.

Kenya Computer Incident Response Team Coordination Centre. (2022). *Annual cybersecurity report*. Nairobi, Kenya.

Kigen, A. M., Nantes, E. A., Larrosa, J. M., & Gómez, L. J. (2021). Marketing and social networks: a criterion for detecting opinion leaders. *European Journal of Management and Business Economics, 26*(3), 2444-8451.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). *Advanced social engineering attacks*. *Journal of Information Security and Applications, 2*(2), 113–122.

Lerner, M. Y. (2019). Connecting the Actual with the Virtual: The Internet and Social Movement Theory in the Muslim World—The Cases of Iran and Egypt. *Journal of Muslim Minority Affairs*, (2), 557-567.

Lismini, R., Narti, S., & Octaviani, V. (2023). Netnographic study of online gender-based violence (KBGO) on Twitter. *Education, Social science and Planning technique journal, 12*(2), 176-189.

Mitnick, P. M., & Simon, I. (2011). Social media use and its impact on adolescent mental health: An umbrella review of the evidence. *Journal of Current Opinion in Psychology, 44*(5), 58-68.

Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research, 45*(8), 1146–1166.

Vishwanath, W., Shukur, Z., Mokhtar, U. A., Sulaiman, R., & Ibrahim, M. A. (2018). Social engineering attacks prevention: a systematic literature review. *Digital Object Identifier journal, 10*(2), 20-35.

Vrhovec, S., & Markelj, I. B. (2022). Explaining information seeking intentions: Insights from a Slovenian social engineering awareness campaign. *Computers & Security, 125*(2), 123-234

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats. *Information Systems Security, 17*(4), 215–223.

Zulkurnain, A. U., Hamidy, A. K. B. K., Husain, A.B., & Chizari, H. (2020). Social engineering attack mitigation. *International Journal of Mathematics and Computational Science 1*(4), 188-198.