iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.70136

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

A Multi-Level Theoretical Framework for Understanding Social Engineering Attacks in Corporate IT Environments

Rajkumar Paswan[1], Prerna Dusi[2]
Faculty of Computer Science & IT, Kalinga University, Raipur, India

Abstract: ***Social engineering (SE) attacks have emerged as a critical threat to corporate information technology (IT) security, exploiting human vulnerabilities rather than technological flaws. Unlike conventional cyberattacks, SE leverages psychological manipulation to bypass security protocols, with tactics such as phishing, pretexting, and baiting responsible for a significant proportion of corporate breaches. This paper presents a comprehensive theoretical exploration of SE by synthesising multi-disciplinary literature across psychology, cybersecurity, and organisational behaviour. A three-layered conceptual framework is developed to analyse how micro-level (individual cognitive traits), meso-level (organisational structures), and macro-level (technological and societal factors) contribute to SE susceptibility across the attack lifecycle. The findings reveal significant gaps in existing models, especially regarding context-specific defences and the influence of emergent technologies like generative AI. This work contributes to the academic discourse by integrating behavioural, organisational, and technological factors, while also offering practical insights to guide policy formulation and risk mitigation in corporate environments.***
Keywords: Cybersecurity, Corporate Security, Phishing, Social Engineering, IT

I. INTRODUCTION

Modern cybersecurity challenges require social engineering (SE) analysis since it has evolved into a significant security threat for corporate IT systems. SE differs from typical cyberattacks because it leverages human psychological vulnerabilities to compromise security protocols, thus becoming a worldwide threat to organisations. Multiple recent research papers confirm social engineering's severe threat level because a substantial number of cyber incidents involve its methods, while phishing, along with pretexting and baiting, rank among the most commonly used tactics [1].

Kinds of SE attacks have received comprehensive theoretical investigation through multiple academic disciplines, including psychology and sociology, and the information systems field. SE exploitation capabilities can be explained with the assistance of models such as the Elaboration Likelihood Model and the Heuristic-Systematic Model, while the Social Engineering Attack Lifecycle framework provides ordered instructions about SE attack stages from initial information collection to execution and exploit steps.

However, the advent of advanced technologies, particularly artificial intelligence (AI), has amplified the sophistication and reach of SE attacks [2]. Generative AI models can craft highly convincing phishing emails, mimic voices for vishing attacks, and even create deepfake videos, thereby enhancing the plausibility of fraudulent communications [3].This technological evolution necessitates a reevaluation of existing theoretical models to account for the enhanced capabilities and novel vectors introduced by AI-driven SE tactics [4].

Despite the wealth of literature on SE, gaps remain in understanding the interplay between organisational culture, employee behaviour, and susceptibility to SE attacks. While individual cognitive biases have been studied, there is a paucity of research examining how organisational structures, communication patterns [5], and cultural norms influence the effectiveness of SE strategies. Moreover, the dynamic nature of SE, characterised by its adaptability and context-specific tactics, challenges static theoretical models, calling for more flexible and integrative frameworks.

This study aims to bridge these gaps by conducting a comprehensive literature review of theoretical models about SE attacks on corporate IT security. By synthesising existing frameworks and identifying their limitations, we seek to propose a nuanced understanding of SE that incorporates organisational and technological dimensions. In doing so, we aspire to contribute to the development of more robust defence mechanisms and inform policy-making to mitigate the risks posed by SE in the corporate realm.

II. LITERATURE REVIEW

A. *Conceptualising Social Engineering Attacks*

Social engineering refers to the deceptive methods which attackers use to trick users into revealing sensitive information while giving unauthorised access to their systems. These attacks bypass technology protection systems because they exploit weaknesses in human behavioural response, which proves more vulnerable than cyber infrastructure [6]. According to [6][7], the SE tactics are categorised into phishing, pretexting, baiting, tailgating, vishing, and smishing [7][8].

SE continues to develop through principles of psychological manipulation that allow attackers to use authority as well as urgency alongside reciprocity and familiarity to achieve their objectives [9]. According to Yasin et al., social proof and cognitive dissonance serve as fundamental psychological frameworks enabling SE attacks' success because they base their attacks on behavioural science principles [10]. The strategies rely on targeting human operators because they represent the main security vulnerability, yet exist within environments that lack proper training and educational initiatives [11].

B. *Frameworks and Lifecycle Models of Social Engineering*

Several frameworks conceptualise the SE lifecycle. The classic model involves four stages: reconnaissance, engagement, exploitation, and execution [12]. More contemporary frameworks emphasise socio-technical interactions and context sensitivity. For example, Adil et al [13] and Krol et al [9] conducted a systematic literature review revealing that SE models are typically fragmented and call for unification into comprehensive frameworks that reflect both attacker techniques and contextual defensive responses [14].

Further, Syafitri et al. identify the lack of rigorous prevention models as a key limitation in SE research. They call for the integration of human-centric frameworks such as "human-as-sensor" models with traditional threat modelling approaches to build more resilient systems [15]. This aligns with Adil et al., who advocate for the inclusion of psychological constructs in SE models to account for user susceptibility under different organisational cultures and communication dynamics [13].

C. *Common Attack Vectors and Contextual Variants*

Among SE attack types, phishing remains the most documented, with real-world case studies from organisations such as Twitter and Ubiquiti Networks demonstrating severe operational and financial consequences [16][17]. The Verizon DBIR 2023 confirms that over 74% of cyber breaches involved some form of human manipulation, emphasising the need for proactive SE defence mechanisms [18].

Special attention is also given to context-specific vulnerabilities. Patel underscores how healthcare organisations face unique risks due to the high volume of sensitive patient data and reliance on loosely regulated third-party systems [16]. This supports the broader argument that SE models must be adaptive across industries and account for domain-specific constraints and behaviours.

D. *The Organisational and Cultural Dimensions of SE*

Recent literature advances the notion that SE susceptibility is not merely an individual cognitive problem but also a function of organisational culture, trust levels, and compliance environments. Alneami's framework introduces national culture and organisational hierarchy as mediators of SE risk, especially regarding authority-based phishing [6]. Similarly, Adil et al. argue that remote work setups, weak policy enforcement, and distributed responsibility models increase exposure to sophisticated SE tactics [13].

Furthermore, Aldawood and Skinner contend that the success of SE attacks reflects failures not only in individual awareness but in institutional training, communication protocols, and security policy integration. Their critical appraisal identifies gaps in organisational readiness to address dynamic SE threats despite advances in technical defences [18].

E. *Prevention, Defence Mechanisms, and Gaps*

A wide range of technical and behavioural strategies has been proposed for SE prevention. These include email filtering, endpoint protection, and behavioural monitoring technologies, alongside employee training, simulated phishing campaigns, and security culture reinforcement [19][20]. However, empirical validation of these methods remains sparse.

Syafitri et al. and Abu Hweidi and Eleyan both highlight the need for cross-disciplinary models that evaluate not only the occurrence but also the *avoidance* of SE incidents—something largely missing in current literature [14][15]. They emphasise the integration of ethical penetration testing, policy simulation, and cultural adaptation mechanisms into holistic SE defence strategies.

F. Research Gaps and Emerging Challenges

Despite the growing corpus of SE research, gaps remain pronounced. First, theoretical models often overlook the attacker's strategic adaptations, especially with the advent of AI-generated phishing and deepfake-enhanced pretexting [12]. Second, while corporate SE studies are abundant, comparative cross-sectoral analyses (e.g., healthcare vs. finance) are limited [19][21].

Third, there is a notable deficiency in long-term impact assessments of SE training interventions and resilience-building initiatives. As Yasin et al. point out, many studies stop at incident analysis without probing organisational recovery or systemic resistance over time [17].

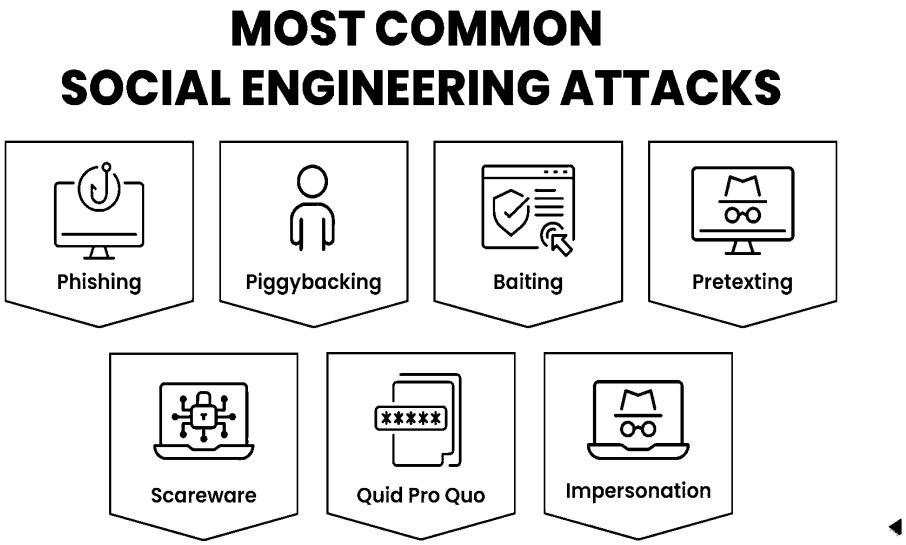


Figure 1: Common Social Engineering Attacks.

III. METHODOLOGY

This study adopts a theoretical and conceptual research design, aimed at developing an integrative framework for understanding social engineering (SE) attacks on corporate IT security. Instead of collecting empirical data, the research relies on critical analysis and synthesis of existing academic literature, conceptual models, and systematic reviews spanning cybersecurity, psychology, and organisational studies.

Several peer-reviewed articles and authoritative reports published between 2018 and 2025 were selected from reputable databases such as IEEE Xplore, ScienceDirect, SpringerLink, and ResearchGate. Inclusion criteria prioritised studies that addressed SE attack lifecycles, psychological manipulation tactics, organisational risk factors, and defence strategies. Excluded materials lacked theoretical contributions or were overly technical without a behavioural dimension.

The analysis proceeded in three phases. First, existing SE models were categorised and compared to identify recurring patterns and theoretical gaps. Second, an integrated multi-level framework was developed, encompassing micro-level (individual cognition and traits), meso-level (organisational culture and policies), and macro-level (societal and technological trends) factors. These were aligned with four stages of the SE attack lifecycle: reconnaissance, approach, exploitation, and exfiltration. Lastly, the proposed model was validated through cross-referencing with established theoretical constructs, ensuring internal consistency and interdisciplinary alignment.

This methodology enables a structured and critical understanding of how human, organisational, and environmental factors converge to influence SE susceptibility, offering a foundation for both theoretical advancement and practical application.

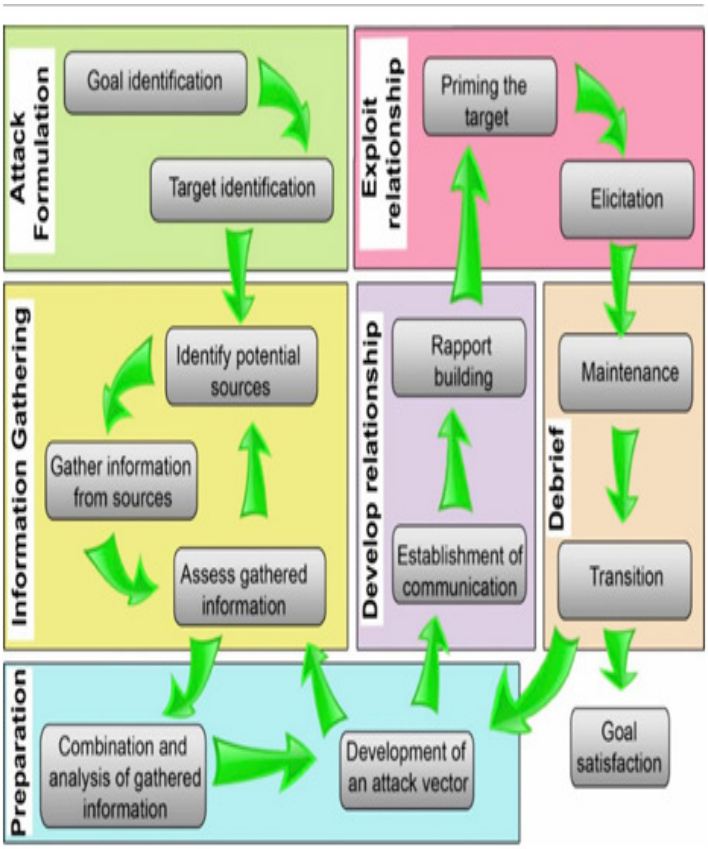


Figure 2: Social Engineering Attacks flowchart. Source: [2]

IV. FINDINGS

The conceptual analysis yielded a multi-layered framework that elucidates the mechanisms by which social engineering exploits vulnerabilities within corporate IT systems. Key findings are organised according to the three analytical levels, micro, meso, and macro, and their influence across the SE attack lifecycle.

At the micro level, individual factors such as cognitive biases (e.g., authority bias, urgency effect), personality traits (e.g., agreeableness, risk tolerance), and lack of training were found to significantly contribute to the success of phishing, baiting, and pretexting attacks. These align with dual-process persuasion models, suggesting that SE exploits heuristic decision-making when cognitive attention is low.

The meso level emphasises the role of organisational structures. Companies with hierarchical cultures, ambiguous communication protocols, and weak security policies were shown to be more susceptible to authority-based or insider impersonation attacks. Trust climates and policy enforcement mechanisms emerged as critical mediators of SE resilience.

At the macro level, environmental factors such as national cultural dimensions, regulatory maturity, and technological developments (e.g., remote work, generative AI) influence the prevalence and sophistication of SE attacks. For example, the rise of deepfake-enabled pretexting represents a novel risk not addressed by traditional models.

Across all levels, the analysis revealed a fragmentation in existing SE frameworks, most focus narrowly on individual susceptibility or attack techniques, neglecting the interplay between personal, organizational, and societal variables. The proposed framework addresses this gap by mapping the layered vulnerabilities and corresponding defences across the full SE lifecycle.

This model not only synthesises existing theory but also introduces new relational pathways between variables, offering a comprehensive structure for evaluating and anticipating SE threats in organisational contexts. Figure 3 represents the social engineering framework.

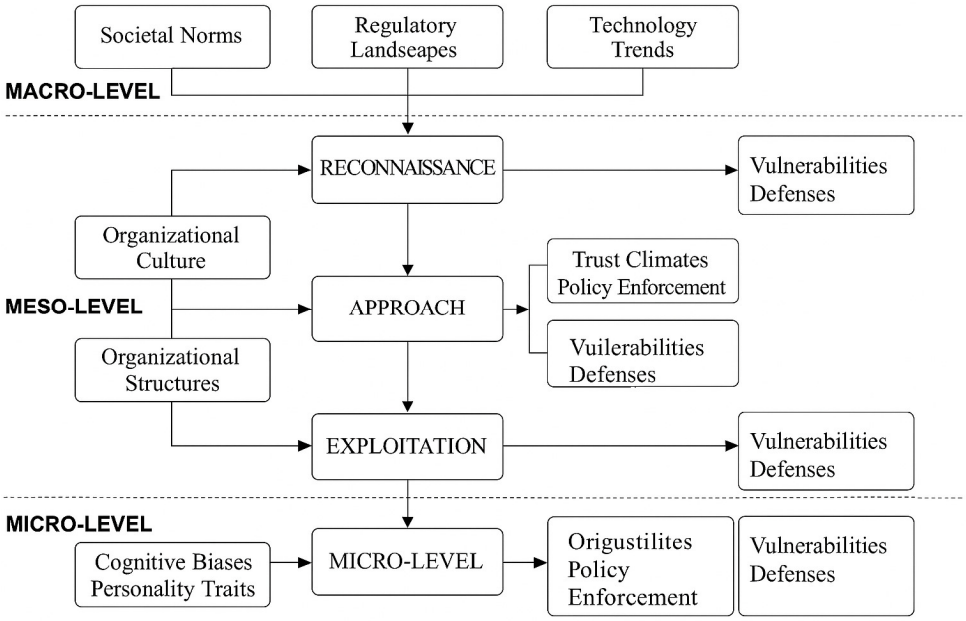


Figure 3: Social Engineering Attacks framework.

V. CONCLUSION

This study provides a theoretically grounded, multi-level framework for understanding and mitigating the impact of social engineering attacks on corporate IT security. It departs from reductionist models that treat SE as a purely psychological or technical issue, instead offering a systemic perspective that links individual vulnerabilities, organizational dynamics, and macro-environmental factors across the lifecycle of an attack.

The conceptual synthesis demonstrates that effective SE defence requires more than security awareness or technical barriers. It demands a cultural and structural alignment across the enterprise—spanning employee education, trust governance, regulatory adaptation, and anticipatory technological design. In doing so, this work contributes both to academic discourse and to the actionable insights needed by cybersecurity practitioners.

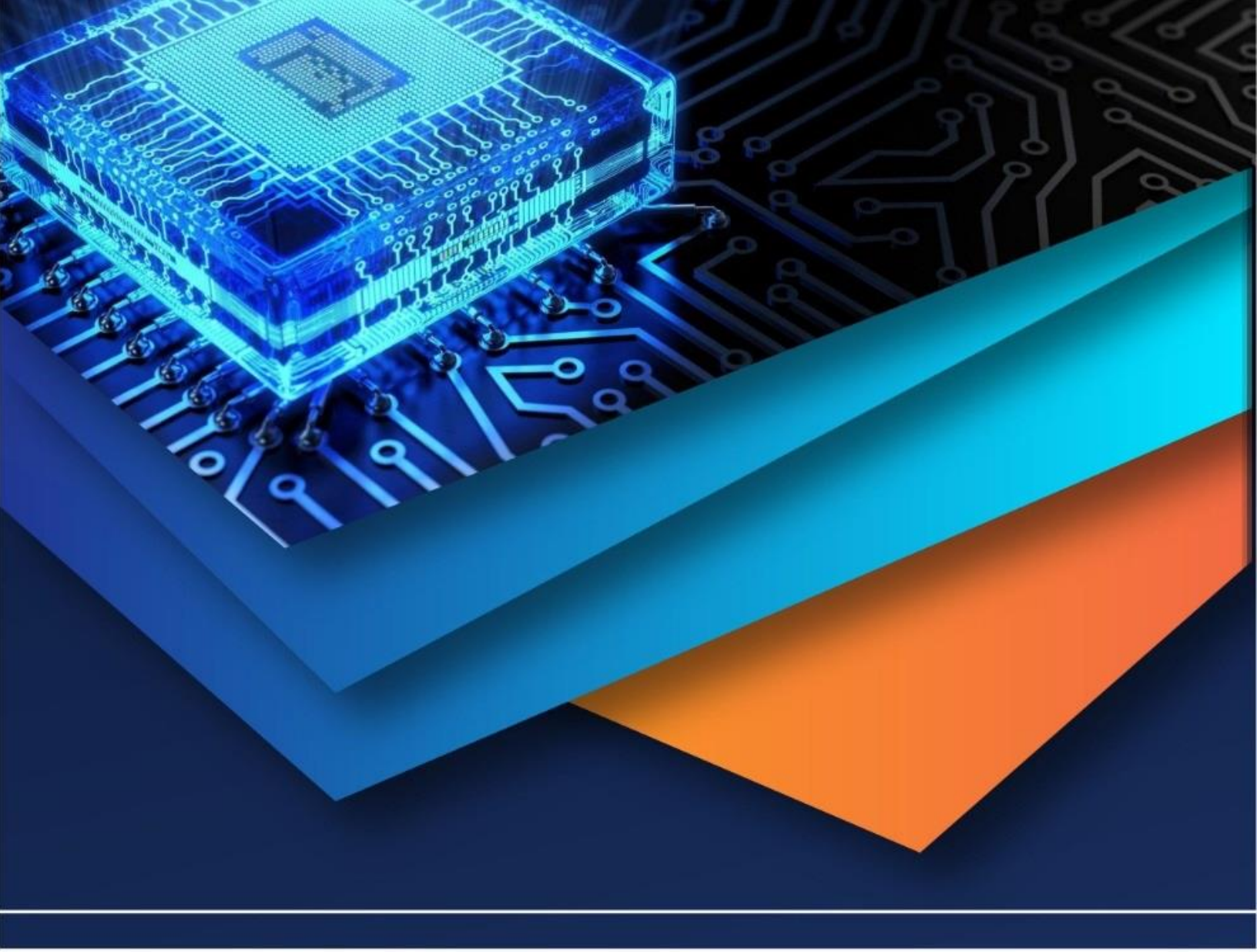
Future research should build on this foundation by empirically validating the model through comparative case studies, simulations, or longitudinal assessments across industries. Additionally, expanding the framework to account for adversarial adaptation and attacker profiling could enhance predictive power and resilience planning.

In sum, this research advances the theoretical sophistication of social engineering studies while promoting an integrated, context-sensitive approach to cybersecurity strategy. As SE techniques continue to evolve, so too must our frameworks for understanding and resisting them.

REFERENCES

[1] '60+ Social Engineering Statistics [Updated 2025]', Secureframe. Accessed: Apr. 30, 2025. [Online]. Available: https://secureframe.com/blog/social-engineering-statistics
[2] M. Schmitt and I. Flechais, 'Digital deception: generative artificial intelligence in social engineering and phishing', 2024.
[3] A. Alshammari, M. Hussain, and K. Salah, "An Enhanced Analysis of Social Engineering in Cyber Security: Research Challenges, Countermeasures—A Survey," IEEE Access, vol. 13, pp. 22534–22560, 2025. doi: 10.1109/ACCESS.2025.3305678
[4] N. Abu Hweidi and D. Eleyan, "Social Engineering Attacks and Defence Mechanisms: Literature Review," International Journal of Computer Applications, vol. 177, no. 40, pp. 1–8, 2020.
[5] A. Salahdine and B. Kaabouch, "Social Engineering Attacks: A Survey," Future Internet, vol. 11, no. 4, p. 89, 2019. doi: 10.3390/fi11040089
[6] A. Alneami, "The Triggers of Social Engineering Attacks in the Context of National Culture: A Conceptual Framework," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 12, no. 2, pp. 648–656, 2021. doi: 10.14569/IJACSA.2021.0120275
[7] B. Wang, T. Duong, and R. Safavi-Naini, "A Systematic Literature Review on the Human-aspects of Social Engineering Attacks," in Proc. 2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 220–231, 2023. doi: 10.1109/EuroSPW59978.2023.00032
[8]
[9] A. Abass, "Social Engineering: The Neglected Human Factor for Information Security," Journal of Information Security Research, vol. 9, no. 2, pp. 63–70, 2018.

[10] L. Atkins and W. Huang, "A Study of Social Engineering in Online Frauds," Open Journal of Social Sciences, vol. 1, no. 3, pp. 79–84, 2013. doi: 10.4236/jss.2013.13014
[11] "Social Engineering Statistics: Phishing, Baiting & Human Hacking," Secureframe, 2024. [Online]. Available: https://secureframe.com/blog/social-engineering-statistics
[12] M. P. Król and D. S. Cruzes, "Social Engineering Attack Concepts, Frameworks and Awareness: A Systematic Literature Review," Journal of Systems and Software, vol. 201, p. 111427, 2024. doi: 10.1016/j.jss.2023.111427
[13] Y. Li, S. Kumar, and J. Lin, "AI in Cybersecurity: Opportunities and Risks in Phishing and Deepfake Threats," Artificial Intelligence Review, 2024. [Online]. Available: https://link.springer.com/article/10.1007/s10462-024-10973-2
[14] M. U. Adil, S. Ali, A. Haider, M. A. Javed, and H. Khan, "An Enhanced Analysis of Social Engineering in Cyber Security: Research Challenges, Countermeasures—A Survey," Asian Bulletin of Big Data Management, vol. 4, no. 4, pp. 321–331, Dec. 2024. doi: 10.62019/abbdm.v4i4.274.
[15] R. F. Abu Hweidi and D. Eleyan, "Social Engineering Attack Concepts, Frameworks, and Awareness: A Systematic Literature Review," Int. J.Comput. Dig. Sys., vol. X, pp. 1–18, 2020. [Online]. Available: http://journals.uob.edu.bh
[16] W. Syafitri, Z. Shukur, U. A. Mokhtar, R. Sulaiman, and M. A. Ibrahim, "Social Engineering Attacks Prevention: A Systematic Literature Review," IEEE Access, vol. 10, pp. 39325–39340, Apr. 2022. doi: 10.1109/ACCESS.2022.3162594.
[17] V. Karhadkar, R. Kale, C. Talakokkula, and S. A. Khan, "Social Engineering: Bridging the Gap Between Psychology and Cybersecurity," in Int. Res. J. Eng. Technol. (IRJET), vol. 12, no. 1, pp. 308–312, Jan. 2025. [Online]. Available: https://www.researchgate.net/publication/388457521
[18] A. Yasin et al., "Understanding and Deciphering of Social Engineering Attack Scenarios," Security and Privacy, vol. 4, no. 2, pp. e161, Mar. 2021. doi: 10.1002/spy2.161
[19] H. Aldawood and G. Skinner, "Contemporary Cyber Security Social Engineering Solutions, Measures, Policies, Tools and Applications: A Critical Appraisal," International Journal of Security (IJS), vol. 10, no. 1, pp. 1–12, 2019.
[20] N. Patel, "Social Engineering as an Evolutionary Threat to Information Security in Healthcare Organizations," Jurnal Administrasi Kesehatan Indonesia, vol. 8, no. 1, pp. 56–64, Jun. 2020. doi: 10.20473/jaki.v8i1.2020.56-64
[21] S. Gupta, M. Moharir, A. Shrivastava, A. Kumar, M. Pritwani, and M., "A Comprehensive Analysis of Social Engineering Attacks: From Phishing to Prevention—Tools, Techniques and Strategies," in Proc. Int. Conf. on Intelligent Computing and Informatics (ICoICI), Bengaluru, India, Aug. 2024. doi: 10.1109/ICoICI62503.2024.10696444
[22] Mustapha, A., & Sinha, A. (2024). Cyberfraud in the Nigerian banking sector: The techniques and preventive measures. International Journal of Innovative Science and Research Technology, 9(8), 171–179. https://doi.org/10.38124/ijisrt/IJISRT24AUG395



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY