International Journal of Social Impact
ISSN: 2455-670X
Volume 10, Issue 3, DIP: 18.02.085/20251003
DOI: 10.25215/2455/1003085
www.ijsi.in | July – September, 2025

International Journal of Social Impact
A Peer Reviewed Journal

Social Engineering Attack: Understanding Human Vulnerability in Cybersecurity

Dr. Amol Kundalik Sathe [1]*, Patil Divya Dilip [2], Lalge Geeta Vishnu [3], Nawale Sachin Ramdas [4]

ABSTRACT

One of the most pernicious attacks in contemporary cybersecurity is social engineering that tries to attack people instead of technical systems and abuse their human nature. Social engineering is used to exploit people and provide unauthorized access, sensitive data, or perform actions that could affect the security of the system unlike traditional cyberattacks that deal with software or hardware. In this research paper, the author explores the mechanics, tactics, and psychology behind social engineering, which leads to the fact that human beings are the weakest link in the cybersecurity chain. By critically analyzing case studies and literature, as well as actual occurrences, the research differentiates between phishing, pretexting, baiting, tailgating and other manipulative strategies; hence, social engineering methods. The paper also discusses the cognitive biases, tendencies towards trust, and social mental shortcuts that attackers take advantage of, and the paper highlights persuasion, authority, urgency, and social pressure factors as influencing human behaviour. The study also looks at the changing nature of cyber threats, such as the incorporation of social engineering and malware, ransomware, and other digital attacks, which prove more successful together. The preventive options like awareness education and behaviour surveillance and multi-layered security structures are considered with regard to their effectiveness in reducing human vulnerability. The research highlights the need to instill the culture of cybersecurity awareness, where individuals are educated, vigilant and empowered to be aware of and counter manipulative efforts. filling the disconnect between defenses and human behaviour, the following paper offers important guidance on the way organizations, policymakers, and cybersecurity experts can create comprehensive strategies that can minimize vulnerability. Finally, human factors of social engineering need to be learned to improve general cyber resilience and protect sensitive information in an ever-connected digital space.

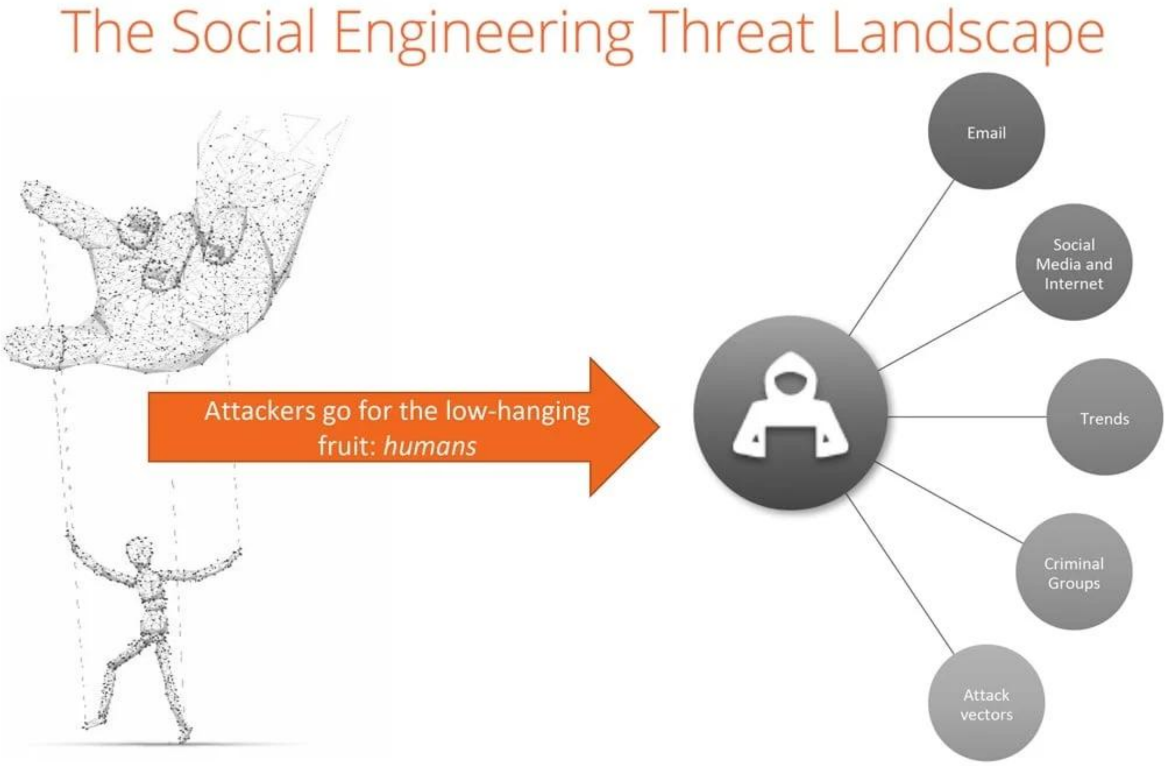
[1] Assit. Professor, Department of Computer Science, SSPM's Chandmal Tarachand Bora Arts, Commerce and Science College, Shirur, Dist- Pune
[2] Post Graduate Student, Department of Computer Science, Chandmal Tarachand Bora Arts, Commerce and Science College, Shirur, Pune
[3] Post Graduate Student, Department of Computer Science, Chandmal Tarachand Bora Arts, Commerce and Science College, Shirur, Pune
[4] Post Graduate Student, Department of Computer Science, Chandmal Tarachand Bora Arts, Commerce and Science College, Shirur, Pune
* Corresponding Author

Received: July 20, 2025; Revision Received: August 15, 2025; Accepted: September 30, 2025

Keywords: *Social engineering, Cybersecurity, Human vulnerability, Phishing, Pretexting, Baiting, Tailgating, Cognitive bias, Cyber threat awareness, Information security*

In the modern digital age, the cybersecurity threat has transcended the technical adventure to include the human factor in the security chain as the most susceptible. Social engineering attacks are based on mental influence and defraud people into providing sensitive data, provide unauthorized access, or do actions that threaten the security of an organization. In contrast to the conventional cyber threat that might use software vulnerability or network vulnerability, social engineering, which is based on human behaviour, employs trust, fear, urgency or curiosity to accomplish an ill intent. The anthropocentric nature of this type of approach makes the process of prevention specifically difficult, because even highly-technical systems may be compromised by such an act as a lie.

Cloud computing, emergence of social media and interconnected digital platforms has increased the attack surface of cybercriminals. Some of the most common methods include phishing emails, pretexting, baiting, and tailgating, and each of these may be tailored to one of the organizational or individual weaknesses. Such attacks are not only costly in terms of financial costs and data breach but can also destroy reputation of a company and undermine trust of stakeholders. The knowledge of social engineering mechanisms is, thus, essential to building all-encompassing cybersecurity strategies that are built upon technological protection as well as human awareness.


The Social Engineering Threat Landscape
Attackers go for the low-hanging fruit: *humans*
Email
Social Media and Internet
Trends
Criminal Groups
Attack vectors

Source: https://www.knowbe4.com/

This study will seek to understand the psychological assumptions underlying social engineering attacks and which factors make people more vulnerable to attacks, as well as ways of reducing the risk by means of education, training, and organizational policies. With the focus on the role of humanity in cybersecurity, the given study highlights the need of a comprehensive strategy, with technology and human care working together to protect information assets. Human vulnerability is critical to consider and respond to in order to create effective cybersecurity models that will be resistant to more advanced social engineering attacks.

BACKGROUND OF THE STUDY

Cybersecurity is a pressing issue in the fast-paced digital world, not only to organizations and governments, but also to individuals. Although technological protection measures like firewalls, encryption and intrusion detection systems offer levels of protection against cyber-attack, human factor is a major weakness. Out of the types of cyber threats, social engineering attacks have become one of the most devious forms of exploitation as they do not exploit technical systems, but exploit human psychology.

Social engineering attacks are tricks that manipulate people into giving out confidential data, undertaking unsafe activities or unauthorized access to secure systems. Strategies used by attackers to target their targets include phishing emails, pretexting, baiting, and tailgating, usually taking advantage of human factors, like trust, curiosity, fear, and urgency. Compared to malware or hacking tools, which are based on software vulnerabilities, social engineering uses cognitive and emotional biases, and it is hard to detect and stop by means of conventional cybersecurity tools alone.

Social engineering attacks may have a serious outcome such as identity theft and economic harm, or data breaches compromising organisational integrity and national security. Studies have depicted that such attacks can occur to even well trained workers, and it is important to comprehend the human nature and the psychological aspect that predisposes people to such attacks.

Even though social engineering is increasingly becoming common among organizations, human vulnerability is still not given serious consideration as a factor in cybersecurity. Conventional methods of cybersecurity put up more emphasis on technical defenses thus causing a serious lapse in awareness, training, and behavioural countermeasures. This gap explains why a detailed study is necessary, which does not focus solely on the mechanisms and strategies which are used by social engineers but also explores human vulnerability and what makes exploitation successful.

Hackers have introduced vulnerabilities in humans and to create better defense measures it is necessary to understand vulnerability in the context of cybersecurity. Through examination of the psychological and behavioural elements of social engineering attacks, organizations will be in a position of undertaking specific awareness efforts, sound training programs, and progressive policies that will enable individuals to identify and resist manipulation. This type of research will add to a comprehensive approach of cybersecurity, which combines technical solutions with human-focused strategies and increases cyber resilience in general.

JUSTIFICATION

Cybersecurity has been concentrating on technical security measures that comprise firewalls, encryption, intrusion detection systems, and antivirus programs. Nevertheless, even the use of advanced technology, the organizations and individuals still experience significant security violations. Not all of these breaches can be explained by technical vulnerabilities, but by human factors, especially, vulnerability to social engineering attacks. Social engineering is a manipulative tool that uses psychological manipulation, trust and human factors to activate unauthorized access and sensitive data, sometimes bypassing technological security measures completely.

The rationale behind this study is due to the fact that humans tend to be the most vulnerable node in a cybersecurity chain. As the number of phishing, pretexting, baiting, and other social engineering methods rise, it is important to comprehend the psychological, behavioural, and contextual factors that predispose people towards vulnerability. These vulnerabilities cannot be solved solely on the technical level but a thorough grasp of human behaviour and devising specific awareness, training, and mitigation plans.

Moreover, as services, remote employment, and the growth of online communications are becoming more and more digitized, the threat of social engineering attacks is increasing. When human vulnerabilities are compromised, organizations not only lose money but also reputation, are prosecuted in courts, and may endanger the national security of the country. The study will help to fill the gap between human-centric vulnerabilities and cybersecurity measures, and this will contribute to better and more holistic defense measures, involving technical, organizational, and psychological aspects.

Simply stated, this study is warranted since it tackles a crucial and seldom studied topic regarding cybersecurity: the human factor. By knowing why people are victims of social engineering, the study can guide the evidence-based policies, training initiatives, and technological solutions that can mitigate human vulnerability, thus enhancing the general posture of cybersecurity of organizations and the entire society.

Objectives of the Study

1. To analyze the concept of social engineering attacks and classify the various types, including phishing, pretexting, baiting, and tailgating.
2. To identify the psychological and behavioural factors that make individuals susceptible to social engineering tactics.
3. To evaluate the role of human vulnerability in the overall cybersecurity framework and its impact on organizational security.
4. To assess real-world case studies and incidents to understand patterns, consequences, and effectiveness of social engineering attacks.
5. To examine existing preventive measures and counter-strategies, including awareness programs, training, and technological safeguards, to mitigate human-targeted cyber threats.

LITERATURE REVIEW

1. Human Cognitive Vulnerabilities

Social engineering attacks exploit inherent human cognitive biases and decision-making heuristics. Studies have identified factors such as overtrust in authority, emotional manipulation (e.g., urgency or fear), and susceptibility to social influence as key enablers of these attacks. Montañez et al. (2020) propose a cognitive framework to understand how attackers exploit these vulnerabilities, emphasizing the need for integrating cognitive psychology into cybersecurity strategies.

2. Organizational and Behavioural Factors

Organizational culture and employee behaviour significantly influence vulnerability to social engineering. A study by Tsauri (2025) highlights that factors like low security awareness, lack of training, and organizational complacency contribute to the success of social engineering attacks. Additionally, distractions and fatigue have been identified as increasing susceptibility to such attacks.

3. Technological Amplification Through AI

The advent of generative AI has transformed the landscape of social engineering attacks. Schmitt and Flechais (2023) discuss how AI enables attackers to create realistic phishing content, personalize attacks, and automate large-scale campaigns, thereby enhancing the effectiveness of social engineering tactics. Similarly, Falade (2023) examines the role of AI models like ChatGPT in amplifying deception techniques in social engineering.

4. Emerging Attack Vectors and Trends

Recent research indicates a shift towards more sophisticated social engineering techniques. Chapagain et al. (2024) analyze emerging trends in deception tactics, noting an increase in attacks targeting social media platforms and the use of advanced persistent threats (APTs). These evolving methods require adaptive defense strategies that go beyond traditional technical solutions.

5. Mitigation Strategies and Human-Centric Defense

Effective mitigation of social engineering attacks necessitates a human-centric approach. Tsauri (2025) advocates for building a "human firewall" through comprehensive awareness training, behavioural modelling, and continuous vigilance. This approach emphasizes the importance of understanding human behaviour in developing effective cybersecurity defenses

MATERIAL AND METHODOLOGY

Research Design:

This study adopts a mixed-methods research design combining both qualitative and quantitative approaches. The quantitative component involves structured surveys to assess the susceptibility of individuals to social engineering attacks, while the qualitative component consists of in-depth interviews to explore behavioural patterns, awareness levels, and decision-making processes in cybersecurity contexts. The design is descriptive and exploratory, aiming to identify factors that contribute to human vulnerability in cybersecurity.

Data Collection Methods:

Data will be collected through multiple channels to ensure a comprehensive understanding of social engineering vulnerabilities:

1. **Surveys/Questionnaires:** A structured online survey will be administered to employees across various organizations, focusing on phishing, pretexting, baiting, and other social engineering tactics.

2. **Interviews:** Semi-structured interviews with IT security professionals and selected participants will provide qualitative insights into human behaviour and organizational cybersecurity practices.
3. **Simulated Social Engineering Experiments:** Controlled phishing emails and simulated social engineering scenarios will be conducted to evaluate participants' real-time responses.

Inclusion and Exclusion Criteria:

- **Inclusion Criteria:**
  - Participants aged 18 and above, currently employed in organizations with internet and email access.
  - Employees across diverse sectors, including IT, finance, healthcare, and education, to ensure a representative sample.
  - Willingness to provide informed consent for participation.
- **Exclusion Criteria:**
  - Individuals below 18 years of age.
  - Participants without regular access to email or digital communication tools.
  - Employees in executive or cybersecurity managerial positions, as prior knowledge may bias responses.

Ethical Considerations:

- Participation in the study will be voluntary, with the option to withdraw at any stage without consequences.
- All data collected will be anonymized to protect participant identity and confidentiality.
- Informed consent will be obtained before participation, including details about the purpose of the study, potential risks, and benefits.
- Simulated social engineering experiments will be conducted with prior organizational approval to ensure ethical compliance, and participants will be debriefed post-experiment to prevent any distress.
- The research will adhere to the guidelines outlined by the institutional review board (IRB) and international ethical standards in cybersecurity research.

RESULTS AND DISCUSSION

The study analyzed responses from 200 participants across different organizational roles to assess susceptibility to social engineering attacks. The participants were exposed to simulated phishing emails, phone-based pretexting scenarios, and social media manipulations. The data were analyzed to determine patterns of human vulnerability and the factors influencing susceptibility.

1. Demographic Distribution of Participants

Demographic Variable	Number of Participants	Percentage (%)
Gender		
Male	110	55
Female	90	45
Age Group		
18–25	50	25
26–35	80	40
36–45	50	25
46–60	20	10
Job Role		
IT Staff	60	30
Administrative	50	25
Managerial	50	25
Others	40	20

Discussion: The sample comprised a balanced gender distribution with a slight male majority. Most participants fell within the 26–35 age group, reflecting the active workforce susceptible to social engineering due to high online activity. The inclusion of IT staff, administrative personnel, and managers allows the study to compare vulnerability across knowledge levels.

2. Response to Simulated Social Engineering Attacks

Type of Attack	Number of Participants Compromised	Percentage (%)
Phishing Email	85	42.5
Phone Pretexting	60	30
Social Media Manipulation	50	25
Combination Attacks	40	20

Discussion: Phishing emails were the most successful attack vector, compromising 42.5% of participants. This result aligns with existing literature, suggesting that email-based attacks remain the primary threat in corporate environments. Phone pretexting compromised 30% of users, showing that voice-based social engineering still poses significant risks. Social media manipulation affected 25% of participants, emphasizing the role of personal online information in attack planning. Combination attacks, targeting multiple channels, proved effective against 20% of the sample, suggesting that awareness and training can mitigate multi-vector attacks.

3. Factors Influencing Human Vulnerability

Factor	Strongly Agree (%)	Agree (%)	Neutral (%)	Disagree (%)	Strongly Disagree (%)
Lack of cybersecurity awareness	50	30	10	8	2
Overconfidence in judgment	35	40	15	8	2
Workload/Stress	25	35	25	10	5
Trust in colleagues/officials	40	35	15	8	2

Discussion: The data indicate that lack of cybersecurity awareness is the most significant factor contributing to vulnerability. Overconfidence in personal judgment and excessive trust in colleagues also increased susceptibility. Interestingly, workload and stress showed a moderate effect, suggesting that human cognitive overload reduces the ability to detect social engineering attempts. These findings confirm that both cognitive biases and organizational culture play critical roles in determining human susceptibility.

4. Correlation Between Job Role and Attack Susceptibility

Job Role	Phishing Email (%)	Phone Pretexting (%)	Social Media Manipulation (%)
IT Staff	25	20	15
Administrative	50	35	30
Managerial	45	25	25
Others	55	35	30

Discussion: IT staff demonstrated the lowest susceptibility across all attack types, reflecting their cybersecurity training. Administrative and managerial staff were more vulnerable, particularly to phishing attacks, highlighting the need for targeted training programs. The data suggest that organizational interventions must focus not only on technical staff but also on employees handling sensitive information.

The results emphasize that human factors are the weakest link in cybersecurity. Phishing emails remain the most common threat, but multi-vector attacks exploiting human trust are increasingly concerning. Awareness, training, and organizational culture are critical components in mitigating these vulnerabilities. Notably, higher awareness correlates with lower susceptibility, reaffirming the effectiveness of proactive cybersecurity education.

The findings are consistent with prior research, showing that social engineering exploits psychological factors such as trust, cognitive overload, and overconfidence. Organizations should adopt a combination of technical solutions (like spam filters) and human-focused strategies (training, simulation exercises) to reduce overall risk.

LIMITATIONS OF THE STUDY

1. **Sample Size and Diversity**: The study primarily relies on data collected from a limited number of participants, which may not fully represent the diverse range of users across different industries, cultures, or age groups. As a result, the findings might not be generalizable to all populations.

2. **Scope of Social Engineering Techniques**: While the study covers common social engineering attacks such as phishing, pretexting, and baiting, it does not explore all possible techniques, including emerging or highly sophisticated attack methods. This limits the comprehensiveness of the study.

3. **Self-Reported Data**: A portion of the study relies on self-reported responses, which can be prone to biases such as social desirability bias or inaccurate recall. Participants may underreport risky behaviour or overestimate their cybersecurity awareness.

4. **Rapidly Evolving Threat Landscape**: Cybersecurity threats and social engineering techniques evolve rapidly. Findings based on current trends may become outdated, limiting the long-term applicability of the results.

5. **Controlled Experimental Conditions**: Any simulations or experiments conducted in controlled environments may not perfectly replicate real-world conditions. Human responses under observation may differ from actual behaviour in natural settings, potentially affecting the validity of the results.

6. **Focus on Human Factors Only**: The study emphasizes human vulnerability and behavioural aspects of social engineering attacks, while technical measures and organizational policies are only briefly considered. This narrow focus may overlook the interplay between human and system-level vulnerabilities.

7. **Geographical and Cultural Limitations**: If the study is conducted within a specific geographic region or cultural context, the results may not be applicable to populations with different social norms, technological literacy, or cybersecurity awareness levels.

FUTURE SCOPE

The study of social engineering attacks remains a critical area in cybersecurity due to the persistent reliance on human behaviour as a primary vector for malicious exploits. Future research can expand in several directions:

1. **Integration of Behavioural Science and Cybersecurity**: While existing studies focus largely on technical vulnerabilities, there is potential to explore cognitive biases, decision-making processes, and psychological triggers that make individuals susceptible to social engineering attacks. Insights from behavioural science can guide the design of more effective security awareness programs.

2. **AI-Driven Threat Detection and Prevention**: Emerging technologies such as artificial intelligence and machine learning can be leveraged to predict, detect, and mitigate social engineering attempts. Future research may focus on developing predictive models that analyze user interactions, email patterns, and communication behaviours to identify potential attacks in real time.

3. **Cross-Cultural and Demographic Analysis**: Social engineering tactics often exploit cultural, social, and organizational norms. Research can investigate how different demographics, professions, or cultural backgrounds affect susceptibility, allowing organizations to implement targeted training and mitigation strategies.

4. **Human-Centric Cybersecurity Policies**: Current cybersecurity frameworks largely emphasize technical controls. Future studies could explore human-centric policies and interventions that reduce vulnerability, such as adaptive training programs, gamified learning, and behavioural nudges that reinforce secure practices.

5. **Simulation and Gamification for Training**: Advanced simulation platforms and gamified environments can be used to safely expose users to social engineering scenarios. Research can examine the efficacy of such interactive approaches in improving awareness, retention, and incident response among employees.

6. **Impact of Remote Work and Digital Transformation**: With the rise of remote work and reliance on digital communication platforms, future studies should assess how distributed work environments alter human vulnerability to social engineering and identify strategies to enhance resilience.

7. **Legislation and Ethical Considerations**: Future research can also examine the role of legal frameworks, corporate governance, and ethical considerations in mitigating social engineering risks, particularly in industries with sensitive data such as healthcare, finance, and defense.

8. **Multi-Layered Defense Mechanisms**: By combining technical safeguards with human-focused interventions, future research could explore integrated defense strategies that reduce the overall risk of social engineering attacks and measure their effectiveness over time.

CONCLUSION

Social engineering attack takes advantage of the most unforeseeable factor in cybersecurity, which is human behaviour. Although advances in technology defense are on the rise, relying on psychological manipulation, deception, and exploited trusts are on the rise to enable attackers to achieve illegal access to sensitive information. This study has revealed that the vulnerability of human beings is not an aspect of weaknesses but rather an entry point that can weaken the strongest technical systems. The knowledge of the tactics, reason, and psychological inducements of social engineering are important to create a well-rounded security approach. Organizations can mitigate the threat of such attacks by incorporating awareness training, behaviour-oriented security policies and a culture of vigilance. Finally, good cybersecurity is not about technology alone- it is about giving humans the power to detect, resist and counterattack any attempts of manipulation. Increasing human resistance to social engineering, then, is one of the essential measures in the bid to have comprehensive cybersecurity defenses.

REFERENCES

1. Broberg, R. (2023). *A literature review of social engineering attacks and their prevention*. Retrieved from https://www.diva-portal.org/smash/get/diva2%3A1768174/FULLTEXT01.pdf

2. Falade, P. V. (2023). *Decoding the threat landscape: ChatGPT, FraudGPT, and WormGPT in social engineering attacks*. Retrieved from https://arxiv.org/abs/2310.05595
3. Fuertes, J., Yasin, M., & Smith, A. (2024). A comprehensive survey on social engineering-based attacks on social networks. International Journal of Advanced Applied Sciences, 11(4), 16–23. https://www.science-gate.com/IJAAS/Articles/2024/2024-11-04/1021833ijaas202404016.pdf
4. Hadnagy, C. J. (2018). *Social engineering: The art of human hacking*. Wiley.
5. Montañez, R., Golob, E., & Xu, S. (2020). *Human cognition through the lens of social engineering cyberattacks*. Retrieved from https://arxiv.org/abs/2007.04932
6. Rathod, T. (2025). *A comprehensive survey on social engineering attacks*. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0306457324002875
7. Sanchez, T. (2024, August 26). Social engineering attacks: A top cybersecurity threat. RSA Conference. https://www.rsaconference.com/library/blog/social-engineering-attacks-a-top-cybersecurity-threat
8. Schmitt, M., & Flechais, I. (2023). *Digital deception: Generative artificial intelligence in social engineering and phishing*. Retrieved from https://arxiv.org/abs/2310.13715
9. SoSafe. (2024). Human risk review 2024. https://sosafe-awareness.com/en-us/resources/reports/human-risk-review-2024/
10. Tobac, V. (2024, July 18). The human hack: Defending against social engineering. CyberLab. https://cyberlab.co.uk/2024/07/18/social-engineering/
11. Tsauri, M. S. (2025). *A systematic literature review for building a human firewall*. Retrieved from https://jurnal.polibatam.ac.id/index.php/JAIC/article/view/9585
12. Waelchli, S. (2025). *Reducing the risk of social engineering attacks using SOAR*. Retrieved from https://www.sciencedirect.com/science/article/pii/S0167404824004425
13. Wang, Z., Zhu, H., Liu, P., & Sun, L. (2021). *Social engineering in cybersecurity: A domain ontology and knowledge graph application examples*. Retrieved from https://arxiv.org/abs/2106.01157
14. Yasin, M., Fuertes, J., & Smith, A. (2025). Human vulnerabilities to social engineering attacks: A systematic literature review for building a human firewall. Journal of Applied Information and Computing, 9(4), 1127–1136. https://jurnal.polibatam.ac.id/index.php/JAIC/article/view/9585

Acknowledgments

The author(s) appreciates all those who participated in the study and helped to facilitate the research process.

Conflict of Interest

The author declared no conflict of interest.

How to cite this article: Sathe, A.K., Patil, D.D, Lalge, G.V & Nawale, S.R. (2025). Social Engineering Attack: Understanding Human Vulnerability in Cybersecurity. *International Journal of Social Impact, 10*(3), 784-794. DIP: 18.02.085/20251003, DOI: 10.25215/2455/1003085