

AI-DRIVEN SOCIAL ENGINEERING IN BUSINESS ENVIRONMENTS: A REVIEW OF CURRENT RESEARCH

VASILE-DANIEL PĂVĂLOAIA

*Alexandru Ioan Cuza University of Iași
Iași, Romania
danpav@uaic.ro*

VALERICĂ GREAVU-ȘERBAN

*Alexandru Ioan Cuza University of Iași
Iași, Romania
valy.greavu@outlook.com*

Abstract

Social Engineering (SE) continues to be a major threat in many sectors as well as Business, by manipulating human behaviour to breach organizational defences. With the integration of Artificial Intelligence (AI) techniques and principles, these attacks have become more targeted, scalable, and difficult to detect – especially for the business domain. This manuscript builds a literature review which highlights the major findings from representative peer-reviewed articles published within 2020 and 2025, retrieved from the Web of Science (WoS) and Scopus databases. The research examines how AI technologies, including Machine Learning, Natural Language Processing, and Deepfake technology, are being leveraged to enhance phishing, impersonation, and behavioural profiling techniques. Preliminary findings indicate a significant rise in the use of AI-driven tools for spear-phishing and executive impersonation within corporate contexts, where the Small and Medium-Sized Enterprises (SMEs) are mostly affected. Additionally, the study highlights a growing gap between the sophistication of attacks and current defensive measures. These insights underscore the need for adaptive, AI-aware security frameworks tailored to evolving SE threats.

Keywords: *artificial intelligence; social engineering; business cybersecurity; phishing attacks; deepfake technology.*

JEL Classification: M15; G19; H75.

1. INTRODUCTION

The digital transformation of business environments has brought unprecedented opportunities for efficiency and growth, but it has also expanded the attack surface for malicious actors. Organizations of all sizes are increasingly reliant on interconnected systems and data, making them vulnerable to a wide range of cyber threats. Among these threats, social engineering remains a

significant concern, exploiting human psychology to manipulate individuals into divulging confidential information or performing actions that compromise security.

Social engineering, in the context of cybersecurity, refers to the psychological manipulation of people to perform actions or divulge confidential information. It is a technique that relies heavily on human interaction and involves deceiving people by exploiting human weaknesses, such as trust, helpfulness, and lack of awareness. Attackers may use various methods, including but not limited to, phishing, pretexting, baiting, and tailgating. Unlike traditional hacking, which relies on technical skills to breach systems, social engineering focuses on exploiting human behavior to gain access to information or systems (Okdem and Okdem, 2024; Nobles, 2024).

1.1. Background on social engineering in business environments

Social engineering attacks are not a new phenomenon, but their prevalence and sophistication have increased in recent years. These attacks, which often involve phishing, pretexting, baiting, and other manipulative tactics, target the weakest link in the security chain: human behavior (Nobles, 2024; Okdem and Okdem, 2024). In business environments, the consequences of successful social engineering can be particularly devastating, leading to financial losses, data breaches, reputational damage, and disruption of operations. The rise of remote work and the increasing reliance on digital communication channels have further exacerbated these vulnerabilities, creating new opportunities for attackers to exploit (Hijji and Alam, 2021; Abdulla *et al.*, 2023).

The landscape of social engineering is constantly evolving, with attackers employing increasingly sophisticated techniques to deceive their victims. Attackers are continuously finding new ways to exploit human vulnerabilities in an increasingly digital world.

1.2. The role of AI in social engineering

AI is playing a dual role in the realm of social engineering. On the one hand, AI is being weaponized by malicious actors to enhance the effectiveness and scale of their attacks (Elsadig, 2024; Nobles, 2024; Toapanta *et al.*, 2024). AI can be used to craft more convincing phishing emails, automate the generation of persuasive deepfake content, and analyze victim behavior to tailor attacks for maximum impact. Large language models (LLMs) like ChatGPT can generate human-like text for phishing and business email compromise attacks and can be used to create fake profiles and automate the grooming of victims (Gupta *et al.*, 2023).

Conversely, AI also offers promising avenues for improving cybersecurity defenses and mitigating the risk of social engineering attacks. Machine learning algorithms can analyze vast amounts of data to detect patterns indicative of social

engineering attempts, such as anomalous email activity, suspicious communication patterns, and deceptive language (Alsufyani and Alzahrani, 2021). AI-powered tools can also be used to enhance security awareness training, personalize interventions, and provide real-time support to employees in identifying and responding to potential threats (Shahzadi *et al.*, 2025).

1.3. Scope of the review

This paper aims to provide a comprehensive review of the current research on AI-driven social engineering in business environments. The review will examine how AI is being used to both enhance social engineering attacks and develop more effective defense mechanisms. It will focus on studies that investigate the intersection of AI, social engineering, and cybersecurity within the context of business organizations.

2. METHODOLOGY

This section outlines the methodology used to conduct this review, detailing the search strategy, study selection process, and data extraction and synthesis methods employed.

The paper explores the following four hypotheses.

H1: AI-driven solutions offer enhanced capabilities in proactively detecting and mitigating diverse cyber threats, including social engineering.

H2: AI plays a dual role in social engineering attacks, both by enhancing the sophistication of attacks and offering potential avenues for improved detection and prevention.

H3: The application of AI in cybersecurity varies across different domains, with the financial sector and tourism/hospitality facing unique challenges and requiring tailored AI-based solutions.

H4: Emerging AI techniques, including intention recognition and machine learning, show promise in addressing specific cybersecurity challenges such as password attacks and improving overall security awareness.

2.1. Search strategy

A systematic search of relevant literature was conducted using the Scopus and WoS databases. These databases were chosen for their comprehensive coverage of peer-reviewed research in the fields of computer science, cybersecurity, and business. The following search query was used:

"TITLE-ABS-KEY ("Artificial Intelligence" AND "Social Engineering" AND ("Cybersecurity" OR "Business")) AND PUBYEAR > 2019 AND PUBYEAR < 2026"

This query was designed to identify studies published between 2020 and 2025 that investigated the role of AI in social engineering within a business context.

2.2. Study selection

The study selection process followed the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines. The study selection process is illustrated in the PRISMA flow diagram (see Figure 1), which details the number of studies identified, included, and excluded at each stage.

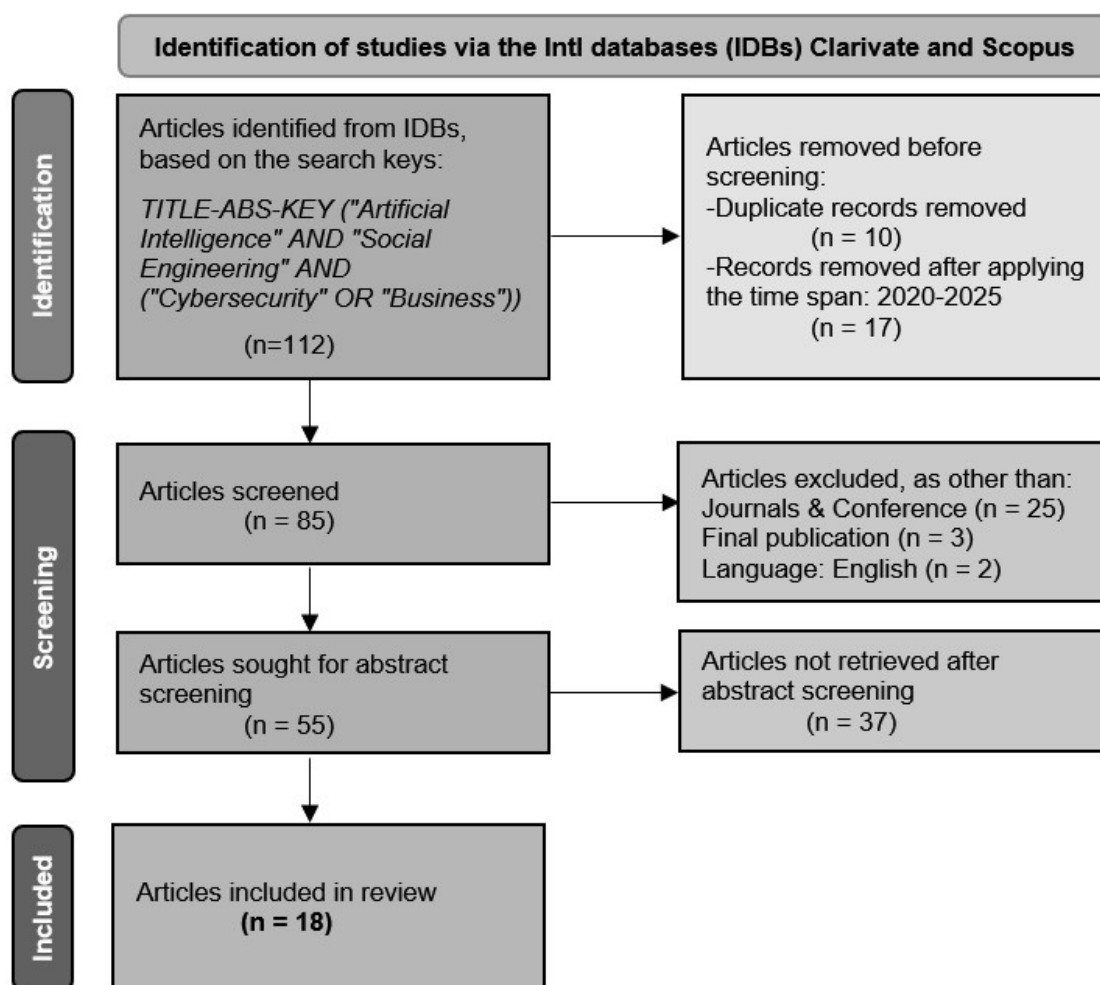


Figure 1. Article selection procedure

The inclusion criteria were studies published in peer-reviewed journals or conference proceedings, written in English, and that explicitly address the use of AI in Social engineering within business environments. After applying the inclusion criteria, 112 articles remained. Exclusion criteria were articles not published in peer-reviewed journals or conference proceedings (e.g., books, book chapters, reports), studies not written in English, and that do not focus on the intersection of AI, social engineering, and business, and duplicate studies. The remaining 55 articles were read and 37 were removed as they did not fit the scope

of the review. The final number of articles included in the study is 18 and the papers were read in full and analyzed in comparison with the hypothesis.

2.3. Data extraction and synthesis

The extracted data were then synthesized using a thematic analysis approach and based on the formulated Hypotheses. This involved identifying recurring themes and patterns in the literature related to the use of AI in social engineering within business environments. The themes were then organized into four categories:

- The Dual Role of AI in Cybersecurity
- AI-Driven Solutions for Proactive Threat Detection and Mitigation
- Applications and Challenges of AI in Cybersecurity
- Emerging AI Techniques for Specific Cybersecurity Challenges and Awareness

3. RESULTS

This review organizes the selected 18 articles based on thematic connections to the proposed research hypotheses. Each section will highlight the original contributions of the papers in relation to the overarching theme.

3.1. The dual role of AI in cybersecurity: enhancing attacks and defences

Hypothesis 2 (H2) posits that AI plays a dual role in social engineering attacks, both by enhancing the sophistication of attacks and offering potential avenues for improved detection and prevention. Several articles in this review directly address this duality, exploring how AI is used by both attackers and defenders.

The weaponization of AI in cybersecurity is a significant concern, as malicious actors exploit AI and Machine Learning (ML) models (Nobles, 2024). Nobles' systematic review examines academic studies on AI weaponization and AI-driven cyberattacks, concluding that more research is necessary on weaponizing AI for offensive cybersecurity applications. Key observations from this study include: (a) a connection between AI weaponization and countermeasures, (b) AI's role in enhancing cybersecurity defences, (c) AI weaponization offering mitigation strategies, and (d) AI-driven attacks exploiting vulnerabilities, enabling automation, facilitating data poisoning, improving social engineering, and augmenting evasion (Nobles, 2024). This highlights AI's capability to make attacks more sophisticated by enabling automation, scalability, and improved social engineering tactics.

Generative AI (GenAI) models like ChatGPT have been identified as powerful tools that can be used for both offensive and defensive cybersecurity tasks, including social engineering (Gupta *et al.*, 2023; Charfeddine *et al.*, 2024). Gupta *et al.* (2023) explore the limitations, challenges, potential risks, and

opportunities of GenAI in cybersecurity and privacy. They demonstrate how vulnerabilities in models like ChatGPT can be exploited for malicious purposes (e.g., jailbreaks, reverse psychology, prompt injection attacks) and how cyber offenders can use GenAI tools to develop social engineering attacks, phishing attacks, automated hacking, and malware. Conversely, the paper also examines defensive uses of GenAI, such as cyber defence automation, threat intelligence, secure code generation, attack identification, and malware detection (Gupta *et al.*, 2023).

Similarly, Charfeddine *et al.* (2024) investigate ChatGPT's security risks and benefits, covering harmful attacker uses such as malicious prompt injection, testing brute force attacks, and preparing ransomware attacks. The authors also address proactive defensive activities, highlighting ChatGPT's significance in security operations and threat intelligence, categorized according to the National Institute of Standards and Technology (NIST) cybersecurity framework. They propose secure enterprise practices and mitigations, emphasizing clear usage standards, protection of personally identifiable information, and adversarial attack prevention (Charfeddine *et al.*, 2024). Elsadig (2024) also provides a thorough investigation and discussion of how ChatGPT can significantly support hackers in committing various attacks, concluding that ChatGPT has significantly supported hacking behaviors and can be exploited to spread malicious activities. This necessitates continuous development and enforcement of appropriate standards and for policymakers and developers to work together to prevent negative effects (Elsadig, 2024).

The work by Toapanta *et al.* (2024) provides a practical approach to AI-driven vishing (voice phishing) attacks. They demonstrate how current AI tools, including ChatGPT and three AI-enabled applications for voice synthesis, can be used to create synthetic voices similar or identical to a person to be impersonated, making vishing attacks more straightforward and precise. Their results from deploying vishing attacks in an academic environment demonstrate the effectiveness of these AI-driven attacks and the maturity level of the employed AI tools, underscoring how AI enhances the sophistication of social engineering attacks (Toapanta *et al.*, 2024).

These studies collectively support H2 by illustrating that while AI offers innovative ways to augment attacks (making them more sophisticated, automated, and personalized), it concurrently provides new mechanisms for defence, threat intelligence, and improved security measures. Golda *et al.* (2024) further contributes by offering a comprehensive survey on privacy and security concerns in Generative AI, discussing GAI architectures, model types, applications, and recent advancements, while also highlighting current security strategies and proposing sustainable solutions involving various stakeholders.

3.2. AI-driven solutions for proactive threat detection and mitigation

Hypothesis 1 (H1) suggests that AI-driven solutions offer enhanced capabilities in proactively detecting and mitigating diverse cyber threats, including social engineering. The reviewed literature provides substantial evidence supporting this.

Okdem and Okdem (2024) explore the potential of artificial intelligence as an emerging tool to enhance cybersecurity, focusing particularly on its preventative capabilities against prevalent threats like phishing, social engineering, ransomware, and malware. While acknowledging AI's recent integration into cybersecurity, they offer a comprehensive review of current AI applications and present a case study on securing communication in resource-constrained Internet of Things (IoT) networks using AI, illustrating a specific AI application in a cybersecurity context (Okdem and Okdem, 2024).

Zhang *et al.* (2025) specifically addresses the cybersecurity needs of small and midsize enterprises (SMEs) by benchmarking and evaluating Large Language Models (LLMs) in phishing detection. Their comprehensive analysis, using high-quality email datasets of human and AI-generated phishing and legitimate emails, demonstrated that the open-source Llama-3-8b-instruct model outperformed other alternatives. It achieved the highest accuracy and F1-score and offered a cost-effective and flexible solution for SMEs, emphasizing ease of implementation without additional training or fine-tuning. The proposed prompt template also enables LLMs to provide explanations and suggestions, assisting users in making informed decisions (Zhang *et al.*, 2025). This highlights LLMs' potential for robust phishing detection, a key aspect of mitigating social engineering.

Alsufyani and Alzahrani (2021) propose using natural language processing (NLP) along with machine learning techniques for text phishing detection. They started with a dataset of 6,224 emails (phishing and legitimate) and used NLP for data preparation before extracting features with the Word2Vec algorithm. They trained four models using k-nearest neighbors (KNN), Multinomial Naive Bayes (MNB), Decision Tree, and AdaBoost algorithms to classify text messages. Three of their models (KNN, Decision Tree, and AdaBoost) obtained considerable values in performance, demonstrating the practical application of ML in identifying text-based phishing attacks, even with unbalanced datasets (Alsufyani and Alzahrani, 2021).

Abualhija *et al.* (2023) propose a novel approach to detecting and preventing social engineering attacks by combining multiple security systems and utilizing the concept of Honeypots with artificial intelligence. Their study aims to merge AI and honeypots with an intrusion prevention system (IPS) to detect social engineering attacks, threaten the attacker, and restrict their session. This signifies a technological solution focused on making users more secure by providing an automated prevention mechanism against manipulation tactics (Abualhija *et al.*, 2023).

These papers illustrate the diverse ways AI, through machine learning, NLP, LLMs, and novel system designs like AI-enhanced honeypots, can enhance the proactive detection and mitigation of cyber threats, particularly social engineering attacks such as phishing.

3.3. Domain-specific applications and challenges of AI in cybersecurity

Hypothesis 3 (H3) states that the application of AI in cybersecurity varies across different domains, with sectors like finance and tourism/hospitality facing unique challenges and requiring tailored AI-based solutions. The reviewed articles provide insights into these domain-specific considerations.

The financial sector is a prime target for cyber threats, necessitating specialized AI-driven defenses. Ali *et al.* (2024) provides a comprehensive review of cybersecurity issues and mitigation measures in FinTech. They examine pressing cybersecurity issues such as privacy concerns, data breaches, malware attacks, hacking, insider threats, identity theft, and social engineering attacks that confront FinTech firms. In response, they evaluate various mitigation strategies, including technological solutions like artificial intelligence and machine learning, big data analytics, and blockchain technologies, alongside regulatory compliance and robust cybersecurity cultures. Their work emphasizes the need for a collaborative strategy to address the growing cyber threat landscape in FinTech (Ali *et al.*, 2024).

Nicholls *et al.* (2021) conduct a comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape, introducing the term "financial cybercrime" which combines financial crime, hacking, and social engineering. They highlight those cybercriminals are using a combination of hacking and social engineering techniques that bypass current security measures in financial institutions. The survey discusses different fraud methods, relevant systems and algorithms (including graph-based techniques and neural network models), their drawbacks, and the unique constraints in applying AI, such as the demand for transparency, fairness, and privacy. This underscores the specialized AI approaches needed to identify illicit transactions while minimizing disruption to genuine customers in the financial domain (Nicholls *et al.*, 2021).

Shahzadi *et al.* (2025) explore personalized and gamification-based cybersecurity risks within financial institutions. Their systematic literature review examines the use of personalized, gamification-based strategies, potentially enhanced by AI, to mitigate cyber threats in the financial domain. The paper assesses the evolving landscape of cyber threats specific to the financial industry, including traditional attacks, APTs, and threats in gaming platforms linked to financial services. They propose AI-driven measures for prevention and detection, emphasizing regular security assessments, user training, and system monitoring. This research points to tailored AI-enhanced gamification to reinforce cybersecurity protocols in finance (Shahzadi *et al.*, 2025).

The tourism and hospitality sector also presents unique cybersecurity challenges. Del Mar Alonso-Almeida and Giglio (2024) compare literature reviews on cybersecurity issues in mature business and management fields with the embryonic tourism and hospitality area. By using the general study as a benchmark, they map current trends and identify gaps specific to tourism and hospitality. Their findings suggest topic clusters for future research in this sector, including (1) machine learning, artificial intelligence, blockchain, big data; (2) fraud and reputation; (3) phishing and social engineering; and (4) human security and user education (del Mar Alonso-Almeida and Giglio, 2024). This indicates a growing need for AI-based solutions tailored to the specific operational models and customer data vulnerabilities inherent in tourism and hospitality.

These articles support H3 by demonstrating that different sectors, particularly finance and potentially tourism/hospitality, face distinct cybersecurity threats and operational constraints, thus requiring the development and application of specialized AI-based security solutions.

3.4. Emerging AI techniques for specific cybersecurity challenges and awareness

Hypothesis 4 (H4) suggests that emerging AI techniques, including intention recognition and machine learning, show promise in addressing specific cybersecurity challenges such as password attacks and improving overall security awareness.

Kassa *et al.* (2024) delve into intention recognition within digital forensics and cybercrime in their systematic literature review. Intention recognition, a subfield of AI, aims to identify agents' intentions based on their actions. The authors categorize research into logic-based, classical machine learning-based, and deep learning-based modelling approaches. They note that intention recognition is now addressing critical challenges across various subdomains, including social engineering attacks. While deep learning is dominant, its lack of transparency is a challenge for digital forensics, leading the authors to advocate for hybrid solutions that blend explainability, reasonableness, efficiency, and accuracy. Their work also proposes a taxonomy for intention recognition, highlighting its promise for predicting and understanding cybercriminal actions (Kassa *et al.*, 2024). This directly aligns with H4 by showing how an emerging AI technique can address complex cyber threats like social engineering by understanding attacker intent.

Taşçı *et al.* (2021) focus on detecting specific password attack types (brute force, dictionary, and social engineering) using a Cowrie Honeypot and machine learning. Logs obtained from these attacks were used to train various machine learning algorithms (Naive Bayes, Decision tree, Random Forest, SVM) to classify subsequent similar attacks. Their research determined that these attacks could be identified with high success rates. The authors emphasize that

determining the type of password attack is critical for implementing appropriate countermeasures. This study shows the promise of machine learning in addressing specific challenges like password attacks by classifying attack types, thus enabling more targeted defences (Taşçı *et al.*, 2021).

The importance of security awareness is highlighted by Abdulla *et al.* (2021), who analyzed social engineering awareness among students and lecturers at the University of Sulaimani. While their study primarily uses a quantitative approach (questionnaires) to gauge awareness, it notes that social engineering attacks use methods like pretexting with Artificial Intelligence or phishing, exploiting human error. The findings show a lack of knowledge of cybersecurity and that participants are inexperienced with network security systems, emphasizing the significance of SE training. Although this paper doesn't directly propose an AI solution for awareness, it underscores the need for improved awareness (Abdulla *et al.*, 2023), a domain where AI-driven training and simulation tools (as suggested by the abstract of the main review) could play a role, aligning with the latter part of H4.

Hijji and Alam (2021), in their multivocal literature review on social engineering-based cyber-attacks during the COVID-19 pandemic, identify open challenges and prospective solutions, including the use of latest technologies such as artificial intelligence, blockchain, and big data analytics. While their primary focus is on the types of SE attacks (phishing, scamming, vishing) and platforms used, the call for AI as a prospective solution to these challenges supports the idea that AI techniques can address these specific issues and potentially enhance security awareness regarding them (Hijji and Alam, 2021).

These papers support H4 by demonstrating the application and potential of specific AI techniques like intention recognition and machine learning algorithms in tackling detailed cybersecurity challenges such as password attacks and by pointing towards the need for better security awareness where AI could be leveraged.

4. CONCLUSIONS

This review of current research between 2020 and 2025 confirms the transformative and dual-edged impact of Artificial Intelligence on social engineering in business environments. The literature substantiates that AI significantly enhances the capabilities of attackers, making social engineering tactics more sophisticated, scalable, and harder to detect, particularly through the use of Generative AI for crafting convincing phishing, vishing, and malware attacks (H2). Tools like ChatGPT are noted for both their potential misuse in creating advanced attacks and their utility in bolstering defences.

Concurrently, AI-driven solutions, including machine learning, NLP, and Large Language Models, offer powerful new avenues for proactively detecting and mitigating these advanced threats (H1). Innovations such as AI-enhanced

honeypots and specialized LLMs for phishing detection provide crucial tools, especially for SMEs that are often heavily targeted.

The application of AI in cybersecurity is not uniform across sectors; domains such as FinTech and tourism/hospitality face unique challenges and require tailored AI-based strategies to combat specific threats like financial cybercrime and protect sensitive customer data (H3). Furthermore, emerging AI techniques like intention recognition and focused machine learning applications demonstrate significant promise in addressing specific vulnerabilities, such as password attacks, and offer potential for improving overall security awareness and understanding attacker motivations (H4).

Overall, the results point out that there is a fast evolving threat landscape where AI-driven social engineering is increasingly prevalent. This underscores an urgent need for businesses to adopt adaptive, AI-aware security frameworks and foster continuous research to bridge the growing gap between the sophistication of AI-powered attacks and current defensive capabilities.

5. LIMITATIONS AND FUTURE RESEARCH DIRECTIONS

This review has several limitations as depicted below. As the search was limited to the Scopus and Clarivate databases, the results may not capture all relevant studies. Further, the review focused solely on studies published in English, potentially excluding valuable research published in other languages. Moreover, the review is limited to the timespan of 2020-2025. Future research paths could tackle these limitations by expanding the search to include additional databases, considering non-English publications, and covering a broader time frame. Additionally, future research could explore the ethical implications of using AI in social engineering, both for attack and defence, in more detail. It should also investigate the effectiveness of different AI techniques in mitigating specific types of social engineering attacks.

References

- 1) Abdulla, R.M., Faraj, H.A., Abdullah, C.O., Amin, A.H. and Rashid, T.A. (2023). Analysis of social engineering awareness among students and lecturers. *IEEE Access*, 11, pp. 101098-101111.
- 2) Abualhija, M., Al-Shaf'i, N., Turab, N.M. and Hussein, A. (2023). Encountering social engineering activities with a novel honeypot mechanism. *International Journal of Electrical & Computer Engineering (2088-8708)*, 13(6).
- 3) Ali, G., Mijwil, M.M., Buruga, B.A. and Abotaleb, M. (2024). A comprehensive review on cybersecurity issues and their mitigation measures in FinTech, *Iraqi Journal for Computer Science and Mathematics*, 5(3), pp. 45–91.
- 4) Alsufyani, A.A. and Alzahrani, S.M. (2021). Social engineering attack detection using machine learning: Text phishing attack. *Indian J. Comput. Sci. Eng*, 12(3), pp. 743-751.

- 5) Charfeddine, M., Kammoun, H.M., Hamdaoui, B. and Guizani, M. (2024). Chatgpt's security risks and benefits: offensive and defensive use-cases, mitigation measures, and future implications. *IEEE Access*, 12, pp. 30263-30310.
- 6) del Mar Alonso-Almeida, M. and Giglio, C. (2024). Cybersecurity in tourism and hospitality management research: current issues, trends, and an agenda for future research. *Cuadernos de turismo*, 53, pp. 243-260.
- 7) Elsadig, M.A. (2024). ChatGPT and cybersecurity: Risk knocking the door. *Journal of internet services and information security*, 14(1), p. 115.
- 8) Golda, A., Mekonen, K., Pandey, A., Singh, A., Hassija, V., Chamola, V. and Sikdar, B. (2024). Privacy and security concerns in generative AI: a comprehensive survey. *IEEE Access*, 12, pp. 48126-48144.
- 9) Gupta, M., Akiri, C., Aryal, K., Parker, E. and Praharaj, L. (2023). From chatgpt to threatgpt: Impact of generative ai in cybersecurity and privacy. *IEEE access*, 11, pp. 80218-80245.
- 10) Hijji, M. and Alam, G. (2021). A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: challenges and prospective solutions. *IEEE Access*, 9, pp. 7152-7169.
- 11) Kassa, Y.W., James, J.I. and Belay, E.G. (2024). Cybercrime intention recognition: A systematic literature review. *Information*, 15(5), p. 263.
- 12) Nicholls, J., Kuppa, A. and Le-Khac, N.A. (2021). Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. *IEEE Access*, 9, pp. 163965-163986.
- 13) Nobles, C. (2024). The weaponization of artificial intelligence in cybersecurity: A systematic review. *Procedia Computer Science*, 239, pp. 547-555.
- 14) Okdem, S. and Okdem, S. (2024). Artificial intelligence in cybersecurity: A review and a case study. *Applied Sciences*, 14(22), p. 10487.
- 15) Shahzadi, A., Ishaq, K., Nawaz, N.A., Rosdi, F. and Khan, F.A., 2025. Unveiling personalized and gamification-based cybersecurity risks within financial institutions. *PeerJ Computer Science*, 11, p. 2598.
- 16) Taşçı, H., Gönen, S., Barışkan, M.A., Karacayılmaz, G., Alhan, B. and Yılmaz, E.N. (2021). Password attack analysis over honeypot using machine learning password attack analysis. *Turkish Journal of Mathematics and Computer Science*, 13(2), pp. 388-402.
- 17) Toapanta, F., Rivadeneira, B., Tipantuña, C. and Guamán, D. (2024). AI-Driven vishing attacks: A practical approach. *Engineering Proceedings*, 77(1), p. 15.
- 18) Zhang, J., Wu, P., London, J. and Tenney, D. (2025). Benchmarking and Evaluating Large Language Models in Phishing Detection for Small and Midsize Enterprises: A Comprehensive Analysis. *IEEE Access*, 13, 28 335–28 352.