Borneo International Journal eISSN 2636-9826; Vol.8 (2); 2025; 60-68
Published by *Majmuah Enterprise*
www.majmuah.com

The Rise of Social Engineering: How Hackers Manipulate Human Behaviour

NUR SABRINA MOHD SHAFAWI, MOHAMAD FADLI BIN ZOLKIPLI
School of Computing, College of Arts and Science, Universiti Utara Malaysia (UUM), 06010 Sintok, Kedah, MALAYSIA
Email: nursabrinams06@email.com, m.fadli.zolkipli@uum.edu.my | Tel: +60166871636 | +60177247779 |

Received: June 23, 2025
Accepted: June 26, 2025
Online Published: June 28, 2025

Abstract

Social engineering is one of the most dangerous threats in the cybersecurity landscape as this method exploits human psychology. This paper explores the evolution of social engineering techniques, from traditional phishing to sophisticated AI-driven deception. Drawing on a wide range of empirical studies and real-world cases, it examines the psychological principles that make individuals susceptible to manipulation such as authority, urgency and trust. The study also evaluates the impact on individuals and organizations because of social engineering attacks. Current preventive measures including awareness training, technical defenses and organizational policies are reviewed alongside emerging threats posed by artificial intelligence and the Internet of Things (IoT). The study also emphasizes the future research opportunities that can be studied. The findings underscore the critical need for a human-centric approach to cybersecurity, emphasizing continuous education, adaptive technologies, and proactive defense strategies to mitigate the growing threat of social engineering.

Keywords: social engineering; human behaviour; cybersecurity

1. Introduction

In the modern digital era, cybersecurity threats have progressed rapidly beyond traditional exploitation to include psychological manipulation, a tactic known as social engineering. Unlike traditional cyberattacks that usually target system vulnerabilities, social engineering exploits human behaviour, making it one of the most effective forms of cybercrime. By manipulating trust, urgency or authority, the attackers (hackers) trick the individuals into divulging sensitive information or performing actions that compromise security. It is so important to understand the mechanisms behind social engineering, as human error usually leads to security breaches. According to Abbas (2018), the human element is often the weakest link in the cybersecurity chain, making awareness and education vital components of any defense strategy. As digital communication become more advanced, the methods that attackers have used have also varied from phishing emails and fake websites to AI-driven deception. This paper aims to explore the evolution of social engineering techniques, the psychological principles that underpin them, and their impact on individuals and organizations. It also evaluates current preventive measures and anticipates future threats, particularly those driven by the development of artificial intelligence and the proliferation of smart devices. By examining both technical and human factors, this study seeks to provide a comprehensive understanding of how social engineering operates and how it can be effectively mitigated.

2. Literature Review

2.1 Evolution of Social Engineering Techniques

Social engineering has progressed rapidly over the past decades, shifted from rudimentary scams to highly sophisticated and multi-layered attacks. Early forms of social engineering rely on the basic deception methods such as impersonation, baiting and pretexting. These early methods often involve face-to-face interactions or simple phone calls, where attackers would pose as authorized person or trustworthy individuals to obtain sensitive information. With the rise of the internet and digital communication platforms, these attacks shifted online. The digital information has made it possible for attackers to take advantage of a wider variety of communication channels such as email, social media and mobile messaging apps (Fuertes et al., 2022). This shift has allowed for the automation and personalization of attacks and making it harder to be detected. According to Mamedova et al. (2019), the development of social engineering has been significantly influenced by the growing digitization of organizational and personal data. It has become simpler for attackers to create highly targeted messages due to the plenty of information available online through public records, data breaches, and social media profiles like Facebook and LinkedIn. This has given rise to spear phishing and whaling attacks, where messages are tailored to specific individuals or high-ranking executives within an organization.

The integration of artificial intelligence (AI) and machine learning (ML) has further accelerated the evolution of social engineering. Attackers can use AI to analyze user behavior, generate realistic phishing emails, and even create deepfake audio and video content. As noted by Schmitt & Flechais (2024), generative AI tools can mimic the writing style and tone of trusted individuals, significantly increasing the success rate of phishing campaigns.

Era	Technique	Key Features
Pre-Digital	Impersonation, baiting	Manual, in-person deception
Early Digital	Phishing emails, fake websites	Mass-distribution, low personalization
Post-social media	Spear phishing, whaling	Targeted, data-driven
AI & ML	Deepfakes, automated scripts	High realism, scalable

Table 1 : Evolution of Social Engineering Technique

2.2 Psychological Principles Behind Human Manipulation

At the heart of social engineering lies a deep understanding of human psychology. Unlike traditional cyberattacks that exploit software vulnerabilities, social engineering targets cognitive and emotional weaknesses. While technology may have become more secure, human behavior remains susceptible to manipulation, making it a prime target for cybercriminals. The success of social engineering attacks hinges on psychological principles that influence perception, decision-making, and trust. Social engineers exploit cognitive biases which means the mental shortcuts people use to make quick decisions. Siddiqi et al. (2022) identify several common psychological principles that have been exploited by the attackers such as authority, urgency, scarcity, and trust. These principles bypass rational thought processes and activate emotional responses that lead individuals to act without verification. One of the most exploited principles is authority. People are conditioned to comply with figures of authority, especially in hierarchical settings like workplaces. Attackers often impersonate executives, IT personnel, or law enforcement to exploit this bias. This is particularly evident in whaling attacks, where an attacker pretends to be a company executive requesting urgent financial transactions. Another principle is urgency. By creating a sense of time pressure such as emails or messages with phrases like "Your account will be suspended in 24 hours!" trigger a fear-based reaction, pushing the user to act quickly without assessing the validation of the request. This tactic is particularly effective in phishing and smishing attacks, where immediate action is demanded. Jayatilaka et al. (2024) found that urgency significantly reduces users' ability to critically evaluate messages, increasing the likelihood of falling for scams.

Scarcity is often used, especially in baiting attacks. For example, an email might offer a limited-time reward or exclusive access to a resource. This prompts users to click on malicious links. It takes advantage of the fear of missing out, a well-known psychological phenomenon. Trust is one of the key principles used in social engineering. Humans are social beings who rely on trust to navigate daily interactions. As Bobokulov (2023) points out, social engineers often exploit people's natural willingness to help others. For example, an attacker might pretend to be a new employee asking for system access or information. Most individuals feel socially compelled to assist, especially when the request seems innocent or urgent. Emotional triggers like fear, curiosity, and sympathy are also effective tools. For example, an attacker might send a message saying that a loved one is in danger or that the recipient is involved in a legal issue. These messages aim to provoke strong emotional reactions that cloud logical thinking. Siddiqi et al. (2022) emphasize that emotional arousal reduces cognitive control and makes individuals more susceptible to manipulation. Heuristics, or mental shortcuts for quick decisions, also significantly contribute to vulnerability. Jayatilaka et al. (2024) found that users often judge the legitimacy of emails based on superficial cues, such as logos, sender names, or formatting. This dependence on heuristics becomes especially risky when users are flooded with information and must make quick decisions.

2.3 Common Social Engineering Techniques

Social engineering includes various deceptive tactics that take advantage of human behavior to gain unauthorized access to systems, data, or physical locations. These methods are always changing to keep up with new technologies

and communication platforms. It is important to understand the most common tactics, such as phishing, vishing, smishing, and spoofing to grasp the real-world application of social engineering

I. Phishing
The most common type of social engineering is phishing, which usually involves sending fake emails that appear to come from trusted organizations like banks, government agencies, or established companies. These emails often contain malicious attachments or links which are designed to install malware or steal financial information or login credentials. Alkhalil et al. (2021) provide a detailed anatomy of phishing attacks, noting that attackers often use spoofed email addresses, official logos, and urgent language to create a sense of legitimacy and pressure. For example, a phishing email might claim that a user's account has been compromised and prompt them to "verify" their credentials via a fake login page.

II. Spear Phishing and Whaling
Spear phishing is a targeted form of phishing. Unlike mass phishing campaigns, spear phishing attacks use specific personal or organizational information to create believable messages. For instance, a university professor might get an email from a "student" mentioning a recent lecture and asking for access to academic records. In a corporate setting, attackers may impersonate vendors or clients, citing previous transactions to gain trust. Whaling is a type of spear phishing that focuses on high-level executives or individuals with access to sensitive data or financial systems. These attacks often involve pretending to be a CEO or CFO and asking for urgent wire transfers or confidential documents. Since they are customized and seem to come from trusted sources, they tend to succeed and can lead to significant financial losses.

III. Vishing (Video Phishing)
Vishing involves phone calls where attackers impersonate trusted entities such as IT support, banks, or government officials. The goal is to extract sensitive information like passwords, credit card numbers, or personal identification details. Chichwadia & Mpekoa (2024) highlight how vishing has become more sophisticated with the use of caller ID spoofing and AI-generated voices. For instance, an attacker might call an employee pretending to be from the company's IT department, claiming there's an urgent issue that requires immediate login verification. Real-world cases include fraudsters posing as tech support, convincing users to grant remote access to their computers under the pretense of fixing malware which ultimately leads to data theft or financial loss.

IV. Smishing (SMS Phishing)
Smishing is the practice of using text messages to trick recipients into opening malicious links or divulging private information. These messages, which indicate that quick action is required, often appear in the form of alerts from banks, delivery services, or social media platforms. For instance, many users received SMS messages claiming to be from courier services or health authorities during the COVID-19 pandemic. When the link was clicked, fake login pages or spyware-installing apps were displayed. The effectiveness of smishing, according to Chichwadia & Mpekoa (2024), is attributed to the urgency and brevity of SMS communication, which lessens the likelihood that users will consider their options carefully before acting.

V. Spoofed Websites
Spoofed websites are fraudulent sites designed to mimic legitimate ones. They are often used in conjunction with phishing emails or smishing messages. These sites may look identical to real banking, e-commerce, or corporate login pages, tricking users into entering their credentials. Lai et al. (2023) describe how attackers use techniques like typo squatting (e.g., using "amaz0n.com" instead of "amazon.com") and search engine manipulation to drive traffic to these fake sites. Information entered by users is collected and used for illegal access or identity theft.

2.4 Impact on Organizations and Individuals
The consequences of social engineering attacks are far-reaching and multifaceted, affecting both individuals and organizations in profound ways. These impacts extend beyond immediate financial losses to include long-term reputational damage, psychological distress, and systemic vulnerabilities.

I. Impact on Individuals
For individuals, social engineering attacks often result in:

(a) Financial Loss: Victims may unknowingly provide banking credentials or make payments to fraudulent accounts. These losses are often not reimbursed, especially if the individual is found to have voluntarily shared information.

(b) Identity Theft: Attackers who gather personal details such as names, addresses, national identification numbers, and login credentials can use this information to open fraudulent accounts, apply for loans, or conduct illegal activities in the victim's name.
(c) Psychological Impact: Bobokulov (2023) emphasizes that social engineering can leave emotional scars. Victims often report feelings of shame, anxiety, and betrayal after realizing they were deceived. This emotional toll can discourage victims from reporting incidents, which in turn allows attackers to continue operating undetected.
(d) Reputational Damage: On a personal level, individuals may suffer public embarrassment or lose trust within their social or professional circles, especially if they unknowingly contribute to wider breaches (e.g., forwarding malicious links or sharing company documents).
(e) Digital Vulnerability: Once compromised, victims often find themselves targeted repeatedly. Their details may be sold or shared on dark web forums, leading to repeated scams, blackmail, or harassment.

II. Impact on Organizations

Organizations face even greater risks, as social engineering attacks can compromise not just individual employees but entire systems and networks. Key impacts include:

(a) Data Breaches: Social engineering is often the initial vector for larger cyberattacks. Fuertes et al. (2022) note that phishing emails are frequently used to gain initial access, which is then leveraged to deploy malware or ransomware.
(b) Financial Damage: Whaling attacks targeting executives can result in fraudulent wire transfers amounting to millions of dollars. Additionally, the cost of incident response, legal fees, and regulatory fines can be substantial.
(c) Reputational Harm: A successful attack can erode customer trust and damage an organization's public image. This is particularly critical for sectors like finance, healthcare, and education, where trust is paramount.
(d) Operational Disruption: Attacks can lead to downtime, loss of productivity, and disruption of critical services. For example, ransomware attacks often lock users out of essential systems until a ransom is paid.
(e) Regulatory and Legal Consequences: Organizations that fail to protect sensitive data may face penalties under data protection laws such as GDPR, HIPAA, or Malaysia's PDPA. These regulations require prompt breach notification and adequate security measures.

Ogundare (2024) emphasizes that even the most advanced technical defenses can be rendered ineffective by a single human error. This highlights the importance of a holistic cybersecurity strategy that includes not only technological tools but also employee training and organizational policies.

3. Methodology

This study adopts a qualitative research methodology to explore the mechanisms, techniques, and impacts of social engineering within the context of cybersecurity. The approach is designed to provide a comprehensive understanding of how social engineering operates in real-world scenarios, how individuals and organizations respond to these threats, and what measures are most effective in mitigating them. The methodology is structured around three core components:

3.1 Analysis of Real-World Attack Vectors

A significant portion of this study is dedicated to examining real-world case studies where social engineering techniques were successfully deployed. Case-based analysis allows for a grounded understanding of how different tactics are used, how victims respond, and what psychological levers are manipulated.

Cases	Description
The 2020 Microsoft 365 Spear Phishing Campaign	In 2020, a sophisticated spear phishing campaign targeted Microsoft 365 users by mimicking official login pages. Attackers sent emails that appeared to be from Microsoft, warning recipients of suspicious activity and urging them to verify their accounts. The emails linked to fake login portals that closely resembled the real Microsoft interface. Once users entered their credentials, attackers gained unauthorized access to corporate systems. This attack exploited urgency, authority, and familiarity which is core psychological triggers that made the deception highly effective (Alkhalil et al., 2021).
COVID-19 Smishing Wave Spoofing Health Authorities	During the COVID-19 pandemic, cybercriminals launched a widespread smishing campaign that impersonated health authorities. Victims received SMS messages claiming to offer vaccine appointments or urgent health

	updates. These messages contained links that, when clicked, installed spyware or redirected users to phishing websites. The attackers capitalized on public fear, trust in government institutions, and the urgency of health-related information to manipulate behaviour and compromise mobile devices (Chichwadia & Mpekoa, 2024).
Deepfake Voice Scam Targeting a Finance Executive	In a more recent and technologically advanced case, attackers used deepfake audio to impersonate a company's CEO in a phone call to a finance executive. The AI-generated voice was convincing enough to prompt the executive to authorize a wire transfer to the attackers' account. This incident highlights the growing threat of AI-driven social engineering, where realistic voice replication can bypass traditional verification methods. The attack relied on authority, urgency, and the familiarity of the CEO's voice to deceive the victim (Vamsi et al., 2022). These examples offer insight into the evolution and effectiveness of social engineering strategies across different sectors. By studying how these attacks unfolded and why they succeeded, we can identify behavioural patterns and situational triggers that make individuals and organizations vulnerable.

Table 2 : Real-World Attack Vectors

3.2 Review of Empirical Studies and Cybersecurity Reports

To support the analysis of social engineering threats, this study incorporates a comprehensive review of empirical research and industry reports. These sources provide valuable insights into user behaviour, attack patterns, and the effectiveness of various countermeasures. By synthesizing findings from both academic and professional domains, the study aims to identify consistent trends and vulnerabilities that can inform better defense strategies. One of the key studies reviewed is by Akpachiogu (2023), which evaluates the impact of phishing awareness training on reducing susceptibility to social engineering attacks. The research found that organizations implementing regular training and simulated phishing exercises saw a measurable decline in successful attacks. This highlights the importance of continuous education and behavioural reinforcement in cybersecurity programs. Siddiqi et al. (2022) delve into the psychological mechanisms behind social engineering, examining how cognitive biases such as authority, urgency, and trust influence user decision-making. Their findings suggest that emotional triggers like fear and curiosity can override rational thinking, making users more vulnerable to manipulation. This underscores the need for training programs that not only inform but also address emotional and psychological responses to suspicious communications.

Wang et al. (2021) provide a broader analysis of social engineering in cybersecurity, identifying common attack methods and human vulnerabilities. Their study emphasizes that technical defenses alone are insufficient; human factors must be considered in any comprehensive security strategy. They also advocate for integrating behavioural analytics into security systems to detect anomalies in user actions that may indicate manipulation. In addition to academic literature, industry reports and white papers offer practical perspectives on emerging threats. For example, Fuertes et al. (2022) conducted a literature review on the impact of social engineering attacks, noting that phishing remains the most common entry point for larger cyber incidents such as ransomware and data breaches. Their work supports the argument that social engineering is not just a standalone threat but a gateway to more severe security compromises. These empirical studies collectively reinforce the idea that social engineering is a dynamic and evolving threat. They highlight the importance of understanding user psychology, implementing targeted training, and developing adaptive security measures. By grounding this research in both theory and practice, the study aims to provide actionable insights for improving cybersecurity resilience.

3.3 Framework for Evaluating Human Vulnerability

Figure 1 : CIA Triad. negg.blog Group (2024)

To systematically assess the impact of social engineering on cybersecurity, this study applies the CIA Triad which is a foundational model in information security that emphasizes three core principles: Confidentiality, Integrity, and Availability. This framework provides a structured lens through which to evaluate how social engineering compromises systems and data, and how organizations can respond effectively.

- Confidentiality: the protection of sensitive information from unauthorized access. Social engineering attacks frequently target this principle by tricking users into revealing credentials, personal data, or proprietary information. For instance, phishing emails that mimic login portals or smishing messages that request verification codes are designed to breach confidentiality. Once attackers gain access to confidential data, it can be used for identity theft, corporate espionage, or further exploitation. The Microsoft 365 spear phishing case (Alkhalil et al., 2021) is a prime example, where attackers harvested login credentials to infiltrate corporate systems.

- Integrity: Involves ensuring that data remains accurate, consistent, and trustworthy. Social engineering can compromise integrity by introducing false information or manipulating communications. Deepfake technology, for example, can be used to impersonate executives or public figures, leading to fraudulent transactions or misinformation. In the case of the AI-generated voice scam (Vamsi et al., 2022), the attacker's ability to convincingly mimic a CEO's voice undermined the integrity of internal communication, resulting in a significant financial loss. Such attacks erode trust in digital interactions and can have long-term consequences for decision-making and governance.

- Availability: Ensures that authorized users have timely and reliable access to information and systems. Social engineering can indirectly threaten availability, particularly when it serves as the entry point for ransomware or denial-of-service attacks. For example, a phishing email may be used to install malware that encrypts files or disables access to critical infrastructure. This was evident in several ransomware incidents where initial access was gained through deceptive emails or phone calls. The resulting downtime can disrupt operations, delay services, and incur substantial recovery costs.

4. Current Preventive Measures

As social engineering attacks become more sophisticated, organizations and individuals must adopt a multi-layered defense strategy that combines human awareness, technical tools, and organizational policies. This section outlines the most effective current measures used to mitigate social engineering threats.

4.1 Awareness Training and Simulations

Human error is often the weakest link in cybersecurity. Therefore, educating users about common attack techniques is a critical first line of defense. Awareness programs typically include training sessions, phishing simulations, and interactive modules that teach users how to recognize suspicious behavior. Organizations often implement phishing simulations to test and reinforce employee vigilance. These simulations mimic real-world attacks and provide immediate feedback, helping users learn from mistakes in a safe environment. According to Akpachiogu (2023), companies that conducted regular training and simulations saw a significant drop in successful phishing incidents.
Training techniques include:

- Phishing simulation exercises, which periodically send fake phishing emails to test user responses.
- Interactive e-learning modules on common attack vectors such as phishing, vishing, and smishing.

- Live workshops or seminars, often conducted during Cybersecurity Awareness Month or after an incident.

Smith et al. (2013) emphasize that training should also address the emotional and psychological aspects of social engineering, helping users understand how attackers manipulate trust, fear, and urgency.

4.2 Technical Defenses

While human awareness is essential, technical tools provide a critical safety net. These defenses are designed to detect, block, or mitigate social engineering attempts before they reach the user.

Key technical measures include:

- Email Filtering Systems: These use AI and pattern recognition to detect phishing emails, flag suspicious links, and quarantine malicious attachments.
- Multi-Factor Authentication (MFA): Even if credentials are compromised, MFA adds an extra layer of protection by requiring a second form of verification.
- Endpoint Protection Software: These tools monitor devices for unusual behavior, unauthorized access, or malware activity.
- AI-Powered Detection Tools: As Lai et al. (2023) note, AI can analyze metadata, domain history, and content structure to identify spoofed websites and phishing attempts with high accuracy.

These tools are most effective when integrated into a broader security ecosystem that includes regular updates, patch management, and network monitoring.

4.3 Organizational Policies and Incident Response

Organizations must also implement clear policies and procedures to guide employee behavior and respond to incidents. These include:

- Access control policies that limit user privileges based on roles.
- Incident response plans that outline steps to take when a social engineering attack is suspected.
- Regular audits and compliance checks to ensure adherence to security protocols.

Sundresan (2024) provides guidelines for law enforcement agencies, emphasizing the need for structured reporting mechanisms and rapid response teams to contain and investigate breaches.

5. Future Threats and Emerging Trends

The rise of artificial intelligence (AI) and the expansion of the Internet of Things (IoT) are transforming the cybersecurity landscape, introducing new threats that are more automated, personalized, and harder to detect. This section explores two major areas of concern: the integration of artificial intelligence into social engineering and the exploitation of Internet of Things (IoT) devices.

5.1 AI-Enhanced Social Engineering

Artificial intelligence is transforming the landscape of cyber threats by enabling attackers to automate and scale social engineering campaigns. AI can be used to generate highly convincing phishing emails, deepfake videos, and voice impersonations. These tools allow attackers to mimic the tone, language, and behavior of trusted individuals with alarming accuracy. For instance, Collier (2024) discusses how generative AI can craft spear phishing emails that are indistinguishable from legitimate communications. In one documented case, attackers used an AI-generated voice to impersonate a company's CEO and successfully tricked an employee into transferring funds. Schmitt & Flechais (2024) warn that as AI models become more accessible, the barrier to entry for launching sophisticated attacks will continue to lower.

5.2 Exploitation of IoT and Smart Devices

The proliferation of IoT devices such as smart home assistants, wearable tech, and connected appliances introduces new vulnerabilities that can be exploited in social engineering attacks. These devices often lack robust security features and can be used to gather personal data or serve as entry points into larger networks. Sarker et al. (2021) highlight how attackers can manipulate IoT devices to create believable scenarios for deception. For example, a compromised smart doorbell could be used to simulate a delivery notification, prompting the homeowner to click on a malicious link sent via SMS. As more devices become interconnected, the potential for multi-vector social engineering attacks increases.

6. Future Research Opportunities

As social engineering continues to evolve alongside technological advancements, there are several promising areas for future research that could deepen our understanding and improve defense mechanisms. These opportunities span across technical innovation, behavioral science, policy development, and interdisciplinary collaboration.

6.1 AI and Deepfake Detection

With the rise of AI-generated content, particularly deepfake audio and video, future research should focus on developing robust detection tools. While current methods can identify manipulated media, they often struggle with real-time analysis and scalability. Research into machine learning models that can detect subtle inconsistencies in voice patterns, facial movements, or metadata could significantly enhance early warning systems.

6.2 Behavioural Psychology and User Profiling

Although cognitive biases such as authority and urgency have been studied (Siddiqi et al., 2022), there is room to investigate how personality traits, cultural factors, and emotional states influence susceptibility. Future research could:

- Use psychometric testing to correlate user traits (e.g., agreeableness, impulsivity) with phishing vulnerability.
- Study how cultural norms affect trust, especially in multilingual or global teams.
- Explore emotional intelligence training as a protective factor against manipulation.

This line of inquiry could lead to personalized security training that adjusts content based on behavioural risk assessments.

7. Conclusion

Social engineering remains one of the most persistent and dangerous threats in the cybersecurity landscape, primarily because it targets the human element rather than technological vulnerabilities. This paper has explored the evolution of social engineering techniques, the psychological principles that make individuals susceptible, and the various attack vectors used by cybercriminals from phishing and spoofing to AI-driven deception.

The analysis reveals that while technical defenses are essential, they are not sufficient on their own. Human awareness, continuous education, and organizational preparedness are equally critical. Real-world examples, such as AI-generated voice scams and phishing campaigns targeting enterprise users, demonstrate how attackers are leveraging both technology and psychology to bypass traditional security measures. As artificial intelligence and IoT technologies continue to advance, the threat landscape will only grow more complex. Future attacks are likely to be more personalized, scalable, and difficult to detect. Therefore, a proactive, multi-layered defense strategy that combines technical tools, user training, and policy enforcement is essential. Ultimately, combating social engineering requires a shift in mindset from viewing cybersecurity as purely a technical issue to recognizing it as a human-centered challenge. Only by addressing both the technological and psychological dimensions can individuals and organizations build true resilience against these evolving threats.

Acknowledgments

The authors would like to thank all members of the School of Computing who are involved in this study. This study was carried out as part of the Hacking and Penetration Testing Project. This work was supported by Universiti Utara Malaysia.

References

Dixson, D. D., & Worrell, F. C. (2016). Formative and summative assessment in the classroom. *Theory into practice*, Abass, I. A. M. (2018). Social engineering threat and defense: A literature survey. *Journal of Information Security*, *09*(04), 257–264. https://doi.org/10.4236/jis.2018.94018

Akpachiogu, C. (2023, December 13). *Evaluating the effectiveness of phishing awareness training in mitigating social engineering attacks*. Unknown. https://www.researchgate.net/publication/376461374_Evaluating_the_Effectiveness_of_Phishing_Awareness_Training_in_Mitigating_Social_Engineering_Attacks

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*. https://doi.org/10.3389/fcomp.2021.563060

Bobokulov, A. (2023). The Impact of Social Engineering on Cybercrime: Psychological Manipulation and Prevention Methods. *International Journal of Cyber Law*, *1*(5).

Chichwadia, A. E., & Mpekoa, N. (2024). Detecting Smishing and Vishing Attacks using Machine Learning. *International Journal of Intelligent Computing Research*, *15*(1), 1234–1241. https://doi.org/10.20533/ijicr.2042.4655.2024.0151

Collier, H. (2024). AI: The future of social engineering! *European Conference on Cyber Warfare and Security*, *23*(1). https://doi.org/10.34190/eccws.23.1.2117

Fuertes, W., Arévalo, D., Castro, J. D., & Benavides, E. (2022, January 1). *Impact of Social Engineering Attacks: A literature review*. Unknown https://www.researchgate.net/publication/355754456_Impact_of_Social_Engineering_Attacks_A_Literature_Review

Jayatilaka, A., Arachchilage, N. A. G., & AliBabar, M. (2024). Why people still fall for phishing emails: An empirical investigation into how users make email response decisions. *Proceedings 2024 Symposium on Usable Security*. https://www.ndss-symposium.org/wp-content/uploads/usec2024-72-paper.pdf

Khidzir, N. Z., Guan, T. T., & Musa, Dr. A.-A.-. (202 C.E., March). *Conceptual framework of social engineering (soe)attacking risks and prevention technique*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3530267

Lai, W. L., Goh, V. T., Yap, T. T. V., & Ng, H. (2023, October 31). *Phishing and spoofing websites: Detection and countermeasures*. Insight Society https://www.researchgate.net/publication/375114122_Phishing_and_Spoofing_Websites_Detection_and_Countermeasures

Mamedova, N., Urintsov, A., Staroverova, O., Ivanov, E., & Galahov, D. (2019a). Social engineering in the context of ensuring information security. *SHS Web of Conferences*, *69*, 00073 . https://doi.org/10.1051/shsconf/20196900073

Ogundare, E. (2024, March 30). *THE HUMAN FACTOR IN CYBER SECURITY*. Unknown. https://www.researchgate.net/publication/379430784_THE_HUMAN_FACTOR_IN_CYBER_SECURITY

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021, May 1). *AI-Driven cybersecurity: An overview, security intelligence modeling and research directions*. Springer Nature. https://www.researchgate.net/publication/350421584_AI-Driven_Cybersecurity_An_Overview_Security_Intelligence_Modeling_and_Research_Directions

Schmitt, M., & Flechais, I. (2024). Digital deception: Generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review*, *57*(12). https://doi.org/10.1007/s10462-024-10973-2

Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A study on the psychology of social engineering-based cyberattacks and existing countermeasures. *Applied Sciences*, *12*(12), 6042. https://doi.org/10.3390/app12126042

Smith, A., Papadaki, M., & Furnell, S. M. (2013, January 1). *Improving awareness of social engineering attacks*. Springer Berlin Heidelberg. https://link.springer.com/chapter/10.1007/978-3-642-39377-8_29

Sundresan, P., 6. (2024). Guidelines to Prevent Social Engineering Attacks for Law Enforcement Agency. *8th International Conference on Information Technology and Society 2024*.

Tanti, R. (2024, October 19). *Study of Phishing Attack and their Prevention Techniques*. Indospace Publications. https://www.researchgate.net/publication/385083853_Study_of_Phishing_Attack_and_their_Prevention_Techniques

Vamsi, V. V. V. N. S., Shet, S. S., Reddy, S. S. M., & Shankar, S. P. (2022, April 1). *Deepfake detection in digital media forensics*. Elsevier BV. https://www.researchgate.net/publication/359708659_Deepfake_Detection_in_Digital_Media_Forensics

View of unmasking the evolution of social engineering in cybersecurity: Techniques, vulnerabilities, and countermeasures. (2024, February). https://ijemr.vandanapublications.com/index.php/j/article/view/1513/1343

Wang, Z., Zhu, H., & Sun, L. (2021). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *IEEE Access*, *9*, 11895–11910. https://doi.org/10.1109/access.2021.3051633