doi.org/10.54473/IJTRET.2025.9305
International Journal of Trendy Research in Engineering and Technology
Volume 9 Issue 3 June 2025
ISSN No. 2582-0958

SOCIAL ENGINEERING ATTACKS: TRENDS, DETECTION, AND PREVENTION

Asere Gbenga Femi[1], Innocent L. Mangbon[2], Jumbo Daniel[3]
[1]Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria
[2]Department of Statistics, Federal School of Statistics, Manchok, kaduna State, Nigeria.
[3]Department of General Studies, Federal School of Statistics, Manchok, kaduna State, Nigeria.
Corresponding Author: +2348066889326, aseregbenga@gmail.com

Received 09 February 2025 Received in revised form 14 February 2025 Accepted 17 February 2025

ABSTRACT

Social engineering attacks exploit human psychology to manipulate individuals into divulging sensitive information or performing actions that compromise security. This research explores the trends, detection methods, and prevention strategies associated with social engineering attacks, highlighting the evolving nature of these threats. As attackers increasingly use advanced technologies, including AI and deepfakes, to craft personalized and convincing attacks, the need for robust detection mechanisms is critical. Machine learning, natural language processing, and behavioral analytics are being leveraged to identify phishing emails and suspicious activities, while multi-factor authentication and honeypots serve as additional defenses. Prevention strategies, such as user education, strong password policies, and secure communication practices, remain essential in reducing vulnerability to social engineering tactics. However, challenges persist due to human susceptibility and resource limitations, especially among smaller organizations. The future of social engineering attack prevention lies in advancing AI-driven detection systems, improving behavioral training, and fostering global collaboration. By integrating technology with human-centered strategies, organizations can better safeguard against the ever-evolving landscape of social engineering threats.
Keywords: Social Engineering Attacks, Cybersecurity Trends, Phishing Detection, Human-Centric Prevention, Security Awareness.

1. INTRODUCTION

Social engineering attacks are a prevalent and evolving threat in the cybersecurity landscape. These attacks manipulate human behavior and psychology to exploit vulnerabilities, by passing even the most sophisticated technical security measures [1]. By leveraging trust, fear, curiosity, or urgency, attackers deceive individuals into disclosing sensitive information or performing actions that compromise security. Common techniques include phishing, pretexting, baiting, and vishing, all of which are becoming increasingly sophisticated due to advancements in technology and the widespread use of digital platforms [2]. In recent years, the integration of artificial intelligence (AI) and big data analytics has enabled attackers to craft highly personalized and convincing attacks. Social media platforms and other online tools provide attackers with an abundance of personal information, allowing them to tailor their approaches to specific targets [3]. For example, spear-phishing attacks use contextual knowledge to increase the likelihood of success, posing significant risks to individuals and organizations alike. Given the rising frequency and impact of social engineering attacks, it is imperative to develop effective detection and prevention mechanisms. Current detection methods, such as machine learning models for anomaly detection and natural language processing (NLP) for phishing email identification, have shown promise in mitigating these threats [4]. However, technological solutions alone are insufficient without addressing the human factor. Studies emphasize the importance of awareness training and education to equip individuals with the skills to recognize and respond to social engineering attempts [5]. Preventive strategies must adopt a multi-layered approach, combining advanced technical solutions, robust organizational policies, and comprehensive user education. Multi-factor authentication (MFA), secure communication protocols, and behavioral analytics are critical components of an effective defense strategy [6]. Additionally, fostering a culture of cybersecurity awareness within organizations can significantly reduce the likelihood of successful attacks.

This study aims to explore the trends, detection methods, and prevention strategies related to social engineering attacks. By analyzing current trends, the research identifies how attackers adapt to technological advancements and social behaviors. It evaluates existing detection tools and their limitations while emphasizing the role of human-centric prevention measures. The ultimate goal is to provide actionable insights that contribute to the development of more resilient defenses against social engineering attacks.

2. LITERATURE REVIEW

Social engineering attacks, which exploit human psychology and trust, have become one of the most significant cybersecurity threats in recent years. As the tactics employed by attackers evolve, understanding the trends, detection mechanisms, and prevention strategies is crucial for mitigating these risks. Social engineering attacks have grown more sophisticated, with a noticeable shift toward personalized and targeted methods. Spear phishing, for instance, uses information from social media and data breaches to craft convincing attacks [3]. The rise of emerging technologies, particularly artificial intelligence and machine learning has allowed attackers to automate and enhance their tactics, such as the use of deepfakes for impersonation [7]. Moreover, social media has become a key vector for these attacks, as attackers exploit personal information shared online to devise tailored phishing and pretexting schemes [5]. The COVID-19 pandemic further exacerbated these trends, with attackers exploiting remote work environments to launch phishing campaigns [8]. Additionally, the blending of social engineering with technical exploits, such as delivering malware via phishing emails, has become more prevalent [1]. Detection of social engineering attacks is increasingly reliant on technological advancements such as machine learning, natural language processing (NLP), and AI. These technologies analyze patterns, behaviors, and anomalies to identify phishing emails and other fraudulent communications. For example, Chen et al [4] have demonstrated that machine learning algorithms could achieve high accuracy in phishing email detection. Behavioral analytics and AI-powered systems are also used to monitor user activities and detect unusual behaviors indicative of social engineering attacks. The use of honeypots and deception techniques has proven effective in gathering intelligence on attackers' methods, as illustrated by [9]. Multi-factor authentication (MFA) and behavioral profiling are further employed to detect and block suspicious activities before they escalate. Prevention of social engineering attacks is a multifaceted approach, focusing on both technological solutions and human-centered strategies. One of the most effective measures is user education and awareness training, which helps employees recognize and resist common attack techniques. Research by Kumaraguru et al [10] and case studies such as the NHS phishing simulation campaigns (NHS Digital, 2020) have demonstrated the efficacy of these programs. Implementing multi-factor authentication (MFA) has been shown to significantly reduce the success rate of phishing attacks, as confirmed by Verizon's 2023 Data Breach Investigations Report. Secure email gateways, anti-phishing tools, and strong password policies also form part of a robust defense system. Insider threats, often exploited in social engineering attacks, require specialized detection methods, including behavioral analytics and effective access controls [11]. Furthermore, organizations must have clear incident response plans to limit the impact of attacks and improve future defenses. Despite these preventive and detective measures, challenges remain. The evolving nature of social engineering tactics, human vulnerabilities, and the growing sophistication of attackers make it difficult to achieve complete protection. Moreover, smaller organizations may lack the resources to implement advanced security measures effectively. Future directions in addressing social engineering attacks include enhancing AI-driven detection systems, integrating behavioral science into training programs, and promoting global collaboration for threat intelligence sharing. Policy frameworks and regulations will also play a critical role in addressing social engineering threats on a broader scale.

3. METHODOLOGY

This study for follows the below mentioned methodology Process:

Literature Review: A systematic review of academic articles, industry reports, and relevant cybersecurity frameworks were conducted to gather insights into the current state of social engineering attacks. Understanding how social engineering tactics have evolved over time, especially with the introduction of new technologies such as artificial intelligence and machine learning, analyzing existing detection methodologies, including the use of AI, behavioral analytics, NLP, and machine learning to identify social engineering attacks and Reviewing best practices, user education, multi-factor authentication, and incident response strategies used by organizations to prevent social engineering attacks.

Case Study Analysis: In-depth case studies of recent social engineering attacks (e.g., 2021 SolarWinds incident) was analyzed. This provides real-world examples of how attacks were carried out, detected, and prevented, offering valuable insights into effective strategies. These case studies also highlight the gaps and challenges faced by organizations in addressing social engineering attacks.

4. RESULTS AND DISCUSSION

4.1. Trends in Social Engineering Attacks

Social engineering attacks exploit human psychology rather than technical vulnerabilities to manipulate individuals into revealing confidential information or granting unauthorized access. These attacks include phishing, pretexting, baiting, and tailgating, among others [1]. Research shows that social engineering is a major factor in cybersecurity breaches, making it critical to understand its impact through empirical studies and real-world case studies.

4.1.1.Types of Social Engineering Attacks

a. Phishing Attacks: Phishing involves fraudulent messages that trick individuals into revealing sensitive information. Empirical studies highlight the growing sophistication of phishing techniques: A ***Data Breach Investigations Report [12]*** shows that 82% of all breaches involved the human element, with phishing being a primary method. Attackers leverage urgency, fear, and authority to deceive victims. A large-scale study by **Mitnick & Simon** [6] analyzed user susceptibility to phishing and found that younger users and those with limited cybersecurity knowledge were more likely to fall for phishing attempts. The 2016 Democratic National Committee (DNC) hack occurred when Russian hackers used spear-phishing emails to gain access to confidential data [13].

b. Pretexting Attacks: Pretexting involves attackers fabricating a scenario to obtain sensitive information. [5] conducted an empirical study showing that individuals who exhibit high trust in authority figures are more vulnerable to pretexting attacks. In 2017, an attacker impersonated the CEO of an energy company and convinced an employee to transfer €220,000 using deepfake technology [14].

c. Baiting Attacks: Baiting lures victims with something desirable, such as free software or infected USB drives. **Hadnagy& Fincher** [1] have demonstrated that over 60% of individuals would pick up and connect an unknown USB drive found in public spaces, showing how curiosity leads to security breaches. In 2016, IBM researchers conducted a field experiment where 297 USB drives were left in public places, and 48% were plugged into computers, demonstrating high susceptibility to baiting [15].

d. Tailgating and Impersonation: Tailgating occurs when an unauthorized individual gains access to restricted areas by following an authorized person. **Parsons et al** [16] have conducted an experiment showing that 67% of employees held doors open for strangers without verifying their credentials. In 2014, an intruder dressed as an IT technician gained access to a secure data center by convincing employees that they were conducting maintenance, resulting in a major security breach [6].

4.2. Empirical Studies on Social Engineering Vulnerabilities

Several studies have examined factors influencing social engineering vulnerability:

- **Psychological Factors:** Workman [17] found that individuals who exhibit high levels of agreeableness and conscientiousness are more susceptible to social engineering tactics.
- **Workplace Training and Awareness:** Junger et al [18] found that organizations that implemented regular security training programs saw a 35% reduction in phishing attack success rates.
- **Cultural and Societal Influences:** Bakhshi et al [19] have demonstrated that employees from collectivist cultures were more likely to fall for social engineering due to their high levels of trust in authority.

4.3. Detection of Social Engineering Attacks

Detecting social engineering attacks requires advanced tools, behavioral analysis, and human training due to their psychological and contextual nature. Modern detection techniques combine technical approaches with user-focused strategies to identify and mitigate these threats before they cause damage. 1. **Machine Learning and Artificial Intelligence (AI):** Machine learning models are increasingly used to detect social engineering attacks by analyzing patterns, behaviors, and anomalies. AI-powered systems analyze linguistic patterns, sender metadata, and link behaviors. A study by [4] Chen et al demonstrated that natural language processing (NLP) combined with supervised machine learning achieved high accuracy in detecting phishing emails. Also, AI systems monitor user behavior, identifying deviations such as unusual login locations or atypical email interactions. For example, Google's Safe Browsing technology uses AI to identify fraudulent websites and alert users in real time. The anti-phishing platform used by Microsoft Office 365 employs AI and heuristic algorithms to detect phishing attempts and block suspicious messages before they reach users' inboxes [20].

2. **Natural Language Processing (NLP):** NLP techniques identify fraudulent communications by analyzing text for phishing indicators, such as urgent language, grammatical errors, or suspicious requests. Research by Abdelhamid et al [21] highlights the effectiveness of NLP in identifying deceptive content, especially in phishing emails. Rao & Ali [22] tested NLP algorithms to differentiate phishing emails from legitimate ones, achieving over 90% accuracy by analyzing semantic and syntactic patterns.

3. Honeypots and Deception Techniques: Honeypots are systems designed to lure attackers, gathering intelligence and identifying attack methods. Social engineering-specific honeypots simulate human interaction, such as email responses or chatbot interactions, to detect and log attempts. A 2018 study by Sadeh et al. described the deployment of phishing honeypots in corporate email networks, helping organizations gather data on attackers' methods while improving future detection.

4. Multi-Factor Authentication (MFA) Logging: Although primarily a prevention measure, MFA can also help detect social engineering attacks. Login attempts flagged as unauthorized due to unusual MFA triggers (e.g., a failed push notification) can serve as early warning signs of an attack attempt. The 2021 SolarWinds breach highlighted the role of MFA systems in detecting anomalous access attempts, aiding early incident response [23].

5. Social Network Behavior Monitoring: Detecting manipulation on social networks involves monitoring account activities for signs of social engineering, such as mass phishing campaigns or unusual message patterns. A study by Albladi & Weir [5] highlighted the use of network behavior analysis tools to flag fake accounts used in phishing campaigns. These tools detect anomalies in messaging frequency, friend requests, and content sharing.

6. User Awareness Tools: Interactive training systems simulate social engineering scenarios, allowing users to experience and identify attack attempts in a controlled environment. For example, phishing simulation platforms like KnowBe4 test employees' ability to spot phishing attempts and improve overall awareness. The National Health Service (NHS) in the UK deployed phishing simulations, reducing successful phishing click rates by 55% within six months [24].

4.4. Prevention Strategies for Social Engineering Attacks

Preventing social engineering attacks requires a multi-layered approach that combines technological solutions, user education, and organizational policies. These strategies aim to minimize the human and technical vulnerabilities that attackers exploit.

1. User Education and Awareness Training: One of the most effective prevention strategies is empowering users to recognize and resist social engineering tactics. Training programs and phishing simulations educate employees about common attack techniques, such as phishing, pretexting, and baiting. A study by Kumaraguru et al [10] demonstrated that users trained through simulated phishing attacks showed a 40% improvement in identifying phishing emails. Interactive tools like KnowBe4 and PhishMe have become popular for building organizational resilience. In 2020, the UK's National Health Service (NHS) used phishing simulation campaigns and training, reducing successful phishing attempts by 55% within six months [24].

2. Implementation of Multi-Factor Authentication (MFA): MFA adds an additional layer of security by requiring users to provide two or more forms of verification. This significantly reduces the risk of credential theft being exploited. Data Breach Investigations Report [25] revealed that MFA could prevent 99.9% of account compromise attempts stemming from phishing. Google implemented mandatory MFA for its employees in 2019, reporting zero account compromises due to phishing attacks afterward.

3. Use of Secure Email Gateways and Anti-Phishing Tools: Secure email gateways (SEGs) and anti-phishing tools filter out malicious emails before they reach users. These tools use machine learning and heuristic analysis to detect phishing attempts and block them. Chen et al [4] demonstrated that AI-driven email security tools could detect phishing emails with an accuracy rate of over 95%. Microsoft Defender for Office 365 uses advanced threat protection (ATP) to scan for suspicious emails and links, significantly reducing exposure to phishing [20].

4. Strong Password Policies and Credential Management: Organizations can enforce strong password policies, including complexity requirements and regular updates. Password managers also help users create and store secure credentials. The Colonial Pipeline ransomware attack in 2021 revealed the dangers of poor password hygiene when attackers exploited a reused password to access critical systems [23].

5. Behavioral Analytics and Threat Monitoring: Behavioral analytics tools monitor user activity to detect anomalies, such as unusual login locations or rapid data transfers. Early detection of unusual behavior can mitigate social engineering attacks before they escalate. A study by Kirda & Kruegel [11] showed that behavioral analytics tools reduced insider threats by 60% when combined with regular audits. Amazon Web Services (AWS) incorporates user activity monitoring into its security framework, flagging unusual activity and triggering automated responses to protect accounts.

6. Organizational Policies and Incident Response Plans: Robust policies and incident response plans are essential for preventing and mitigating social engineering attacks. Organizations should define acceptable use policies, mandate cybersecurity training, and establish clear procedures for reporting incidents. After the 2020 Twitter breach, the company implemented stricter internal access controls and mandatory social engineering training for employees to prevent similar attacks [26].

7. Secure Communication Channels: Organizations should use encrypted communication tools and discourage employees from sharing sensitive information over unsecured platforms. Tools like end-to-end encrypted messaging apps and secure file-sharing platforms can reduce exposure. In 2021, a law firm avoided data leakage during a spear-phishing campaign by strictly enforcing the use of secure communication platforms for client interactions.

4.5. Challenges and Future Directions in Addressing Social Engineering Attacks

Challenges

1. **Evolving Attack Tactics** Social engineering attacks are constantly evolving, becoming more sophisticated and difficult to detect. Attackers now use advanced techniques such as deepfakes, AI-generated phishing emails, and multi-vector attacks. According to Conti et al [7], AI-powered attacks can bypass traditional security systems, increasing the complexity of mitigation.
2. **Human Vulnerabilities** The reliance on human interaction makes social engineering inherently challenging to address. Despite training efforts, users remain prone to cognitive biases, stress, and manipulation. Studies by Conti et al [27] show that even well-trained individuals may fall victim to cleverly crafted social engineering schemes.
3. **Lack of Awareness and Training** Many organizations, especially small and medium enterprises (SMEs), lack the resources or expertise to provide comprehensive employee training. Data Breach Investigations Report [25] highlighted that human error remains the primary cause of 74% of breaches, underscoring the gap in awareness.
4. **Insider Threats** Social engineering attacks often exploit insiders, whether malicious or unintentional, who have legitimate access to sensitive systems. Identifying and mitigating insider threats requires complex behavioral monitoring and robust access control mechanisms [11].
5. **Resource Limitations** Deploying advanced tools like AI-based threat detection and behavioral analytics requires significant financial and technical resources, which may be out of reach for smaller organizations. This creates a disparity in organizational preparedness against these attacks.

Future Directions

1. **Advancing AI and Machine Learning in Detection** Future advancements in AI and machine learning can help detect and mitigate social engineering attacks more effectively. For example, real-time monitoring systems powered by AI could identify suspicious behaviors or fraudulent communications with higher precision. Studies by Chen et al [4] suggest integrating deep learning models into cybersecurity systems to improve detection rates for complex attack vectors like spear phishing.
2. **Human-AI Collaboration** A key direction is developing tools that enhance human decision-making. Augmented intelligence systems can provide users with contextual information or warnings, enabling them to recognize potential social engineering attempts more effectively.
3. **Global Collaboration and Information Sharing** Cybersecurity agencies, governments, and organizations must collaborate to share threat intelligence and best practices. Initiatives like the EU's ENISA (European Union Agency for Cybersecurity) provide a framework for sharing data on social engineering trends and mitigations globally.
4. **Policy and Regulatory Measures** Governments and regulators could enforce stricter cybersecurity policies, including mandatory social engineering training, regular phishing simulations, and standardized reporting of breaches. A global framework for combating social engineering would also help unify prevention efforts.
5. **Improved Incident Response Plans** Organizations must develop and refine incident response plans to handle the aftermath of social engineering attacks effectively. Rapid response protocols and post-incident reviews can limit damage and provide valuable insights for future prevention efforts.

5. CONCLUSION

Social engineering attacks pose a persistent and growing threat in the cybersecurity landscape, exploiting human psychology and trust to bypass technological defenses. The increasing sophistication of these attacks, including AI-driven tactics and multi-vector approaches, demands a proactive and comprehensive response from individuals, organizations, and governments. Key prevention and detection strategies include leveraging advanced technologies such as artificial intelligence, machine learning, and behavioral analytics, while also fostering a strong culture of user education and awareness. Case studies and empirical research underscore the effectiveness of multi-factor authentication, phishing simulations, and robust incident response plans in mitigating these threats. Additionally, global collaboration, policy frameworks, and regulatory measures are critical to addressing the challenges of social engineering on a broader scale. Looking ahead, future research and efforts should focus on enhancing AI-driven detection systems, integrating insights from behavioral science into training programs, and promoting global information-sharing initiatives. By combining technological innovation with human-centered approaches, it is possible to build resilience against social engineering attacks and safeguard critical systems and sensitive information in an increasingly interconnected world.

REFERENCES

[1]. Hadnagy, C., & Fincher, M. (2018). Social engineering: The science of human hacking (2nd ed.). Wiley.
[2]. Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. Technology in Society, 32(3),183–196. https://doi.org/10.1016/j.techsoc.2010.07.001
[3]. Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and Applications, 22,113–122. https://doi.org/10.1016/j.jisa.2014.09.005
[4]. Chen, Y., Luo, X., & Long, J. (2021). Social engineering attack detection based on machine learning algorithms. Computers & Security, 109, 102370. https://doi.org/10.1016/j.cose.2021.102370
[5]. Albladi, S. M., & Weir, G. R. S. (2018). Predicting individuals' vulnerability to social engineering in social networks. Cybersecurity, 1(1), 1–12. https://doi.org/10.1186/s42400-018-0009-5
[6]. Mitnick, K. D., & Simon, W. L. (2011). The art of deception: Controlling the human element of security. Wiley.
[7]. Conti, M., Gangwal, A., & Ruj, S. (2021). Deepfakes in cybersecurity: Threats and countermeasures. IEEE Communications Surveys & Tutorials,23(2),1223–1251. https://doi.org/10.1109/COMST.2021.3067326
[8]. Proofpoint. (2021). The human factor report: Social engineering tactics and trends. https://www.proofpoint.com
[9]. Sadeh, N., Tomasic, A., & Fette, I. (2018). Phishing honeypots: Lessons from deployment. Journal of Information Security, 37(3), 45–55. https://doi.org/10.1016/j.cose.2018.07.003
[10]. Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Protecting people from phishing: The design and evaluation of an embedded training email system. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,905–914. https://doi.org/10.1145/1753326.1753459
[11]. Kirda, E., & Kruegel, C. (2016). Behavioral profiling for insider threat detection. Journal of Computer Security, 24(6), 673–695. https://doi.org/10.3233/JCS-160009
[12]. Verizon. (2022). 2022 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/
[13]. Rid, T. (2020). Active measures: The secret history of disinformation and political warfare. Farrar, Straus and Giroux.
[14]. Tidy, J. (2019). Fraudsters used AI to mimic CEO's voice in unusual cybercrime case. BBC News. https://www.bbc.com/news/technology-48990374
[15]. McAlaney, J., Taylor, J., & Faily, S. (2020). The psychology of social engineering: The role of influence and persuasion in cyber attacks. Computers & Security, 88, 101645. https://doi.org/10.1016/j.cose.2019.101645
[16]. Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. Computers & Security, 66, 40–51. https://doi.org/10.1016/j.cose.2017.01.004
[17]. Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. Journal of the American Society for Information Science and Technology, 59(4), 662–674. https://doi.org/10.1002/asi.20779
[18]. Junger, M., Montoya, L., & Overink, F. J. (2017). Priming and warnings are not effective to prevent social engineering attacks. Computers in Human Behavior,66,75–87. https://doi.org/10.1016/j.chb.2016.09.012
[19]. Bakhshi, T., Papadaki, M., & Furnell, S. (2019). A practical assessment of social engineering susceptibility within organizations. Computers & Security,83,256–273. https://doi.org/10.1016/j.cose.2019.03.010
[20]. Microsoft. (2022). Protecting against phishing with Microsoft Defender for Office 365. https://www.microsoft.com
[21]. Abdelhamid, N., Ayesh, A., & Thabtah, F. (2014). Phishing detection: A recent intelligent machine learning comparison based on models content and features. Procedia Computer Science, 60, 676–682. https://doi.org/10.1016/j.procs.2014.09.379
[22]. Rao, R. S., & Ali, S. T. (2015). Phishing detection using text and image analysis. International Journal of Computer Applications, 123(5), 1–5. https://doi.org/10.5120/ijca2015905686
[23]. CISA. (2021). Alert (AA21-133A): Avoiding social engineering and phishing attacks. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov
[24]. [NHS Digital. (2020). Cyber awareness and simulation case study. https://digital.nhs.uk
[25]. Verizon. (2023). Data Breach Investigations Report. https://www.verizon.com/dbir
[26]. BBC News. (2020, July 31). Twitter hack: What went wrong, and why it matters. https://www.bbc.com/news
[27]. Wright, R. T., Jensen, M. L., Thatcher, J. B., & Dinger, M. (2014). Influence techniques in phishing attacks: An examination of vulnerability and resistance. Information Systems Research, 25(2),385–400. https://doi.org/10.1287/isre.2014.0522