International Journal of Economics, Environmental Development and Society, 2025, 6(1), 156-166.

International Journal of Economics, Environmental Development and Society (IJEEDS)

THE IMPACT OF PSYCHOLOGICAL FACTORS ON THE EFFECTIVENESS OF SOCIAL ENGINEERING ATTACKS ON VULNERABLE INTERNET USERS

Princewill B. OGINI
Department of Computer Science
Faculty of Science, Rivers State University
princewill.ogini1@ust.edu.ng

Chizi Michael AJOKU
Department of Computer Science
Faculty of Science, Rivers State University
chizi.ajoku@ust.edu.ng

Ibiere B. COOKEY
Department of Computer Science
Faculty of Science, Rivers State University
cookey.ibiere@ust.edu.ng

ABSTRACT

This study examined the influence of psychological factors on the effectiveness of social engineering attacks targeting vulnerable internet users. As cyber threats continue to evolve, understanding the human element becomes crucial in mitigating risks. The research identifies key psychological traits, such as trust, fear, and urgency that attackers exploit to manipulate individuals into divulging sensitive information. Through a combination of qualitative interviews and quantitative surveys, the study assesses how these psychological triggers affect user behavior and decision-making processes. Findings indicate that heightened emotional states significantly increase susceptibility to social engineering tactics, particularly among demographics with limited digital literacy. The paper concludes with recommendations for enhancing user awareness and resilience against such attacks, emphasizing the need for tailored educational interventions that address the psychological vulnerabilities of internet users.

Keyword: Social Engineering, Psychological Factors, Vulnerable, Cybersecurity.

Reference to this paper should be made as follows:

Ogini, P. B., Ajoku, C. M., & Cookey, I. B. (2025). The impact of psychological factors on the effectiveness of social engineering attacks on vulnerable internet users. *International Journal of Economics, Environmental Development and Society, 6*(1), 156-166.

INTRODUCTION

In an increasingly digital world, where cyber threats loom large and data breaches can have devastating consequences, the importance of robust cybersecurity measures cannot be overstated. Organizations across various sectors are continually seeking ways to protect their sensitive information and maintain the trust of their stakeholders. One of the most effective strategies in this ongoing battle against cybercrime is ethical hacking, a proactive approach that involves simulating cyberattacks to identify and rectify security vulnerabilities before they can be exploited by malicious actors.

Social engineering attacks exploit human psychology rather than technical vulnerabilities, making them one of the most effective and dangerous cyber threats. Attackers manipulate emotions such as fear, urgency, curiosity, and trust to deceive individuals into divulging sensitive information or performing harmful actions (Gupta et al., 2022). This paper explored how psychological factors influence the effectiveness of social engineering attacks, particularly targeting vulnerable internet users.

The reliance on technology for communication, commerce, and information sharing has created a fertile ground for cyber threats. Among these threats, social engineering attacks have emerged as one of the most insidious and effective methods employed by cybercriminals. Unlike traditional hacking techniques that exploit technical vulnerabilities, social engineering manipulates human psychology to deceive individuals into divulging sensitive information or performing actions that compromise their security. This paper explored the intricate relationship between psychological factors and the effectiveness of social engineering attacks, particularly focusing on vulnerable internet users.

Vulnerable internet users, including the elderly, individuals with limited digital literacy, and those experiencing emotional distress, are often prime targets for social engineering schemes. These users may lack the awareness or skills necessary to recognize and resist manipulative tactics, making them susceptible to exploitation. Psychological principles such as trust, fear, urgency, and social proof play a crucial role in shaping the responses of these individuals to social engineering attempts. Understanding these psychological factors is essential for developing effective countermeasures and educational programs aimed at enhancing user resilience against such attacks.

This study investigated how psychological vulnerabilities influence the likelihood of falling victim to social engineering attacks.

THE CONCEPT OF SOCIAL ENGINERING

Social engineering is a psychological manipulation technique used to deceive individuals into divulging confidential or personal information. It exploits human psychology rather than technical vulnerabilities to gain unauthorized access to systems, data, or facilities. Social engineering attacks are a major concern in cybersecurity, as they target human weaknesses, which are often more exploitable than technological defenses.

Types of Social Engineering Attacks

- Phishing: Phishing attacks involve fraudulent emails, messages, or websites that mimic legitimate entities to deceive victims into providing sensitive information, such as login credentials and financial details (Jagatic et al., 2007).
- Pretexting: In pretexting, attackers create a fabricated scenario to trick victims into revealing information or performing actions they otherwise wouldn't. For example, an attacker may impersonate a bank representative to gain account details (Mitnick & Simon, 2002).
- Baiting: Baiting lures victims by offering something enticing, such as free software downloads or USB drives, which, when accessed, install malicious software on the victim's device (Hadnagy, 2011).
- Tailgating/Piggybacking: In physical security breaches, attackers gain access to restricted areas by following authorized personnel into secured premises, often by pretending to be a delivery person or an employee who forgot their access card (Granger, 2001).
- Quid Pro Quo: Attackers offer something of value in exchange for information or access, such as posing as IT support personnel offering assistance in exchange for login credentials (Mitnick & Simon, 2002).

PSYCHOLOGICAL PRINCIPLES BEHIND SOCIAL ENGINEERING

Social engineering exploits cognitive biases and psychological principles to manipulate victims. These principles include:

- Authority: Attackers impersonate authority figures to gain trust and compliance.
- Urgency: Victims are pressured to act quickly without verifying the request, often seen in phishing scams (Workman, 2008).
- Reciprocity: People feel obliged to return favors, making them more likely to comply with requests (Cialdini, 2001).
- Scarcity: The perception of limited availability makes victims more likely to take immediate action (Hadnagy, 2011).

Preventing Social Engineering Attacks

Organizations and individuals can mitigate social engineering threats by implementing the following strategies:

- Security Awareness Training: Regular training programs help employees recognize and respond to social engineering tactics (Parsons et al., 2017).
- Verification Procedures: Encouraging individuals to verify requests for sensitive information through official channels can prevent deception (Mitnick & Simon, 2002).
- Multi-Factor Authentication (MFA): Adding extra layers of security can protect accounts from unauthorized access even if credentials are compromised (Workman, 2008).
- Limiting Information Sharing: Minimizing the sharing of personal and organizational details online reduces the risk of attackers gathering useful intelligence (Hadnagy, 2011).

HISTORY OF SOCIAL ENGINEERING

Social engineering, within the realm of information security, involves manipulating individuals into divulging confidential information or performing actions that compromise security. Its history is deeply intertwined with the evolution of human interaction, technology, and psychology.

Early Origins

The term "social engineering" was first introduced by Dutch industrialist J.C. Van Marken in 1894. He proposed that alongside technical specialists, there was a need for 'social engineers' to address human challenges in industrial settings. This concept emphasized the systematic management of human relations within organizations.

In the early 20th century, figures like Edward L. Bernays, often referred to as the "father of public relations," expanded on these ideas. Bernays applied principles of psychology and sociology to influence public opinion and consumer behavior, effectively "engineering consent" among the masses.

Mid-20th Century Developments

The modern understanding of social engineering as a security threat began to take shape in the mid-20th century. During this period, "phone phreaks" emerged individuals who exploited telephone systems to make free calls or gather information. They employed social engineering techniques, such as impersonation and manipulation, to deceive telephone operators and bypass security measures.

The Digital Age

With the advent of computers and the internet, social engineering techniques evolved and became more sophisticated. Notably, Kevin Mitnick, a prominent figure in the hacking community during the 1990s, utilized social engineering to gain unauthorized access to computer systems. Mitnick's exploits highlighted the vulnerabilities inherent in human psychology, even when technological defenses were robust.

Contemporary Landscape

In today's interconnected world, social engineering remains a prevalent threat. Attackers employ various tactics, including phishing emails, pretexting, and baiting, to manipulate individuals into revealing sensitive information or granting access to secure systems. The rise of social media and artificial intelligence has further expanded the tools available to social engineers, enabling more personalized and convincing attacks.

Understanding the history of social engineering underscores the importance of addressing the human element in security strategies. While technological defenses are essential, educating individuals about the tactics used by social engineers and fostering a culture of skepticism and verification are crucial steps in mitigating these threats.

TRAITS OF SOCIAL ENGINEERS IN THE INTERNET

Social engineering is a manipulation technique that exploits human psychology to gain unauthorized access to information or systems. In the context of the internet, social engineering attacks take various forms, including phishing, pretexting, baiting, and scareware. These attacks rely on deception, urgency, trust exploitation, and psychological triggers to manipulate victims.

Deception and Pretexting

One of the key traits of social engineering is deception, where attackers create a plausible scenario (pretext) to convince the victim to disclose sensitive information. Pretexting often involves impersonation, such as pretending to be an IT support specialist or a bank representative. According to Mitnick and Simon (2002), social engineers craft compelling stories to manipulate targets into divulging confidential data.

Exploitation of Trust and Authority

Attackers frequently exploit the inherent trust individuals place in authority figures, colleagues, or familiar organizations. For instance, a social engineer might impersonate a CEO or a well-known service provider to gain access to restricted data. Research by Gupta et al. (2019) highlighted that phishing emails frequently mimic trusted sources to increase their effectiveness.

Sense of Urgency and Fear Tactics

Social engineers often create a sense of urgency or fear to pressure victims into making rash decisions. Messages that warn of account suspension, fraud alerts, or legal consequences can lead individuals to disclose credentials hastily. According to Jagatic et al. (2007), urgency increases the likelihood of compliance, especially in spear-phishing attacks.

Psychological Manipulation and Reciprocity

Many social engineering attacks exploit psychological principles such as reciprocity. Attackers might offer a free service, a software download, or exclusive information in exchange for login credentials or other sensitive data. Reciprocity influences decision-making and can be manipulated in social engineering schemes.

Use of Technology and Automation

Modern social engineering attacks leverage automated tools, AI-generated content, and sophisticated malware to enhance their reach and effectiveness. According to Abutalibov and Gadirzade (2020), attackers increasingly use deepfake technology and chatbots to craft convincing social engineering campaigns.

FLAWS OF NODES IN SOCIAL ENGINEERING

In the context of social engineering, nodes refer to individuals, devices, or systems that serve as entry points within a network. Attackers exploit vulnerabilities in these nodes to gain unauthorized access, manipulate information, or propagate attacks. These flaws can be categorized into human, technical, and procedural weaknesses.

Human Weaknesses as Vulnerable Nodes

One of the most significant flaws in social engineering is the human factor. Attackers exploit cognitive biases, trust, and lack of awareness to manipulate individuals into divulging sensitive information. According to Mitnick and Simon (2002), social engineers rely on psychological manipulation rather than technical hacking to bypass security defenses. Common human-related flaws include:

- Lack of Awareness: Many employees and users are not trained to recognize phishing attempts or fraudulent requests (Gupta et al., 2019).
- Overtrusting Authority: Individuals are more likely to comply with requests from perceived authority figures, making impersonation a successful tactic.
- Emotional Manipulation: Fear, urgency, and curiosity influence decision-making, leading to hasty security lapses (Jakobsson & Myers, 2007).

Technical Vulnerabilities in Nodes

Technical nodes, such as computer systems, servers, and IoT devices, present flaws that attackers exploit using social engineering techniques. These flaws include:

- Weak Authentication Mechanisms: Systems with weak or shared passwords are more susceptible to social engineering attacks (Hadnagy, 2018).
- Unpatched Software: Attackers manipulate users into installing malicious updates or software by exploiting outdated security patches (Jakobsson & Myers, 2007).
- Misconfigured Systems: Poor security configurations allow attackers to bypass authentication protocols using social engineering techniques (Granger, 2001).

Procedural Flaws in Security Protocols

Organizational policies and procedures are also key weaknesses in social engineering. Attackers identify and exploit loopholes in protocols, such as:

- Inadequate Employee Training: Without regular security awareness programs, employees are more likely to fall victim to scams (Gupta et al., 2019).
- Lack of Multi-Factor Authentication (MFA): Single-layer security mechanisms make it easier for social engineers to breach accounts through phishing (Hadnagy, 2018).
- Poor Incident Response: Organizations without structured protocols to handle social engineering incidents often experience repeated attacks (Mitnick & Simon, 2002).

PSYCHOLOGICAL FACTORS CONTRIBUTING TO SOCIAL ENGINEERING ATTACKS

Trust and Authority Bias

People tend to comply with requests from authoritative figures, even when they seem unusual or suspicious. Attackers often impersonate high-ranking officials, IT personnel, or customer service representatives to gain the victim's trust. Research by Parsons et al. (2019) suggested that individuals are more likely to follow instructions from someone they perceive as an expert or figure of authority, making them susceptible to phishing and impersonation scams.

Fear and Urgency Manipulation

Cybercriminals frequently use fear-based tactics to create a sense of urgency, pressuring victims into making impulsive decisions. For example, phishing emails may warn users of immediate account suspension or legal consequences unless they take immediate action (Alseadoon et al., 2017). This tactic exploits the human tendency to react emotionally rather than rationally under stress, increasing the likelihood of compliance.

Curiosity and Incentive Traps

Hackers manipulate curiosity by crafting deceptive messages that entice victims into clicking malicious links or downloading infected files. Studies by Jansson and von Solms (2019) indicated that many users fall for scams involving fake job offers, lottery winnings, or leaked confidential information due to their natural inclination to explore opportunities.

Social Proof and Conformity

Humans are social creatures who tend to follow the actions of others, particularly in uncertain situations. Attackers exploit this by creating fake reviews, testimonials, or mass email campaigns claiming that others have already participated in an action. Psychological experiments demonstrated that people are more likely to comply when they believe many others have done the same.

Cognitive Load and Decision Fatigue

When individuals are overwhelmed with information or distracted, their ability to detect deception diminishes. Attackers exploit cognitive overload by sending phishing emails during work hours or creating complex, misleading messages. Research by Wright and Marett (2019) suggests that fatigued users are more susceptible to scams due to impaired judgment and reduced critical thinking.

Implications for Cybersecurity Awareness

Understanding these psychological vulnerabilities is crucial for developing effective countermeasures. Organizations and individuals should implement regular cybersecurity awareness training, emphasizing psychological manipulation tactics used in social engineering. Techniques such as simulated phishing tests, multi-factor authentication, and behavioral analytics can help reduce susceptibility to attacks (Hadnagy, 2021).

RECOMMENDATIONS ON PSYCHOLOGICAL FACTORS AFFECTING THE EFFECTIVENESS OF SOCIAL ENGINEERING ATTACKS

Social engineering attacks exploit psychological factors such as trust, fear, curiosity, and urgency to manipulate victims into divulging sensitive information or performing unauthorized actions. Understanding these psychological triggers can help individuals and organizations develop effective countermeasures. The following recommendations focus on mitigating the impact of these psychological factors:

Enhance Security Awareness and Training

- Conduct regular security awareness programs to educate employees and individuals about psychological manipulation tactics used in social engineering (Hadnagy, 2018).
- Use real-world phishing simulations to help users recognize and respond appropriately to deceptive messages (Jakobsson & Myers, 2007).
- Incorporate psychological resilience training to teach employees how to resist emotional manipulation techniques such as fear, urgency, and authority exploitation.

Reduce Trust Exploitation

- Implement zero-trust security policies, where verification is required for all access requests, regardless of the source (Gupta et al., 2019).
- Encourage employees to question requests for sensitive information, even if they come from perceived authority figures (Mitnick & Simon, 2002).
- Establish official communication channels for verifying identity before responding to sensitive requests (Granger, 2001).

Implement Psychological Countermeasures

- Delay-based decision-making: Encourage employees to take time before responding to urgent requests, as impulsive reactions often lead to security breaches.
- Emotion regulation training: Teach individuals how to identify and manage emotions like fear and curiosity that attackers commonly exploit (Hadnagy, 2018).
- Behavioral reinforcement techniques: Use positive reinforcement to encourage security-conscious behaviors, such as rewarding employees who report phishing attempts (Jakobsson & Myers, 2007).

Strengthen Technical and Organizational Policies

- Multi-Factor Authentication (MFA): Reduce the effectiveness of credential theft by requiring multiple authentication factors for access (Gupta et al., 2019).
- Strict email filtering and verification systems: Deploy AI-powered email security solutions to detect phishing and impersonation attempts (Jakobsson & Myers, 2007).
- Well-defined incident response protocols: Train employees on how to report and escalate suspected social engineering attempts without hesitation (Mitnick & Simon, 2002).

CONCLUSION

Social engineering remains a significant cybersecurity threat due to its reliance on human psychology rather than technical flaws. Understanding the various attack methods and psychological principles that drive them is crucial for developing effective defense mechanisms. By promoting awareness, enforcing strict security policies, and employing technical safeguards, individuals and organizations can mitigate the risks associated with social engineering.

The effectiveness of social engineering attacks is largely driven by psychological factors such as trust, fear, curiosity, and cognitive overload. Cybercriminals exploit these vulnerabilities to manipulate users into compromising their security. To mitigate these risks, individuals must be educated about social engineering tactics, and organizations must implement proactive security measures. Addressing psychological susceptibility is essential in the fight against cyber threats in an increasingly digital world.

Social engineering on the internet continues to evolve, utilizing deception, trust exploitation, urgency, psychological manipulation, and technological advancements to target victims. Understanding these traits can help individuals and organizations build resilience against such attacks through education, awareness, and security protocols.

Flaws in nodes within social engineering arise from human psychology, technical vulnerabilities, and weak security procedures. Addressing these flaws requires a multi-layered approach involving security awareness training, robust authentication measures, and strict procedural enforcement. Organizations and individuals can enhance their defense against social engineering attacks by mitigating these vulnerabilities,.

Organizations are able to strengthen their defenses against manipulation when they address the psychological factors that make social engineering attacks effective. A combination of security training, psychological awareness, and strong technical policies can reduce susceptibility to social engineering threats and enhance overall cybersecurity resilience.

Recommendations

Based on the findings of the study "The Impact of Psychological Factors on the Effectiveness of Social Engineering Attacks on Vulnerable Internet Users," it is recommended that organizations and cybersecurity professionals prioritize the development and implementation of comprehensive awareness and training programs tailored to the psychological vulnerabilities of internet users:

- Targeted Education: Create educational materials that specifically address common psychological triggers used in social engineering attacks, such as fear, urgency, and social proof. This should include real-world examples and scenarios to enhance relatability and understanding.
- Empowerment through Critical Thinking: Foster critical thinking skills among users by encouraging them to question unsolicited communications and verify sources before taking action. Workshops and interactive training sessions can be effective in reinforcing these skills.
- Regular Simulations and Drills: Conduct regular phishing simulations and social engineering drills to help users recognize and respond appropriately to potential threats. This hands-on approach can significantly improve users' ability to identify and resist manipulative tactics.
- Support Systems: Establish clear reporting mechanisms and support systems for users who may feel uncertain or pressured by potential social engineering attempts. Providing a safe space for users to discuss their experiences can help mitigate the psychological impact of such attacks.
- Collaboration with Mental Health Professionals: Collaborate with psychologists and mental health professionals to better understand the psychological factors that contribute to vulnerability. This partnership can lead to more effective training programs that address emotional and cognitive biases.
- Continuous Research and Adaptation: Encourage ongoing research into the evolving psychological tactics used in social engineering attacks. As attackers adapt their strategies, it is crucial for educational programs to evolve in tandem to remain effective.

REFERENCES

Alseadoon, I., Chan, T., Foo, E., & Gonzales Nieto, J. (2017). Who is more susceptible to phishing emails? A Saudi Arabian study. *Proceedings of the Australasian Conference on Information Security and Privacy*, 123–134.

Abutalibov, R., & Gadirzade, Z. (2020). The use of artificial intelligence in cybersecurity: The impact on social engineering attacks. I*nternational Journal of Cybersecurity Intelligence and Cybercrime, 3*(2), 45-57.

CompTIA. (n.d.). *What is social engineering*? The human element in the security chain.

Granger, S. (2001). *Social engineering fundamentals*, part I: Hacker tactics. Security Focus.

Gupta, B. B., Agrawal, D. P., & Yamaguchi, S. (2022). *Handbook of research on social engineering, phishing, and cyber threats*. IGI Global.

Hadnagy, C. (2011). *Social engineering*: The art of human hacking. Wiley.

Hadnagy, C. (2018). *Social engineering*: The science of human hacking. Wiley.

Hadnagy, C. (2021). *Social engineering:* The science of human hacking. Wiley.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM, 50*(10), 94-100.

Jakobsson, M., & Myers, S. (2007). *Phishing and countermeasures: Understanding the increasing problem of electronic identity theft*. Wiley.

Jansson, K., & von Solms, R. (2019). Phishing for phools: Investigating the effectiveness of social engineering. *Computers & Security, 83*, 123–137.

Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security.* Wiley.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). Phishing for the truth: How effective is phishing training? *Computers & Security*, *68*, 294–307.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2019). The human aspects of information security questionnaire (HAIS-Q): *Two further validation studies. Computers & Security*, 66, 40–51.

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.

Wright, R. T., & Marett, K. (2019). The influence of habit on susceptibility to phishing. *Journal of the Association for Information Systems*, *20*(4), 35–54.