INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING, MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XI, November 2025

Strengthening Human Resilience: The Role of Education in Preventing Social Engineering Attacks

AbdulBasir Momand,Osama Zain

Rana University, Afghanistan

DOI: https://doi.org/10.51583/IJLTEMAS.2025.1411000046

Received: 10 November 2025; Accepted: 20 November 2025; Published: 08 December 2025

ABSTRACT

With the rapid growth of information technology and the widespread use of digital devices, social engineering has become one of the most pressing challenges in today's cybersecurity landscape. In simple terms, social engineering involves manipulating people by exploiting human psychology to carry out harmful activities. This review explores different types of social engineering threats across various environments, emphasizing how people rather than systems or technologies are often the weakest link in security. As a result, there's a growing need to boost awareness among users. One of the most effective ways to tackle this issue is through targeted training and educational programs. This paper discusses how creative and well-structured information security education can significantly improve user awareness and help reduce the number of cyber incidents.

Keywords -social engineering, phishing, cybersecurity awareness, human factor, information security training.

INTRODUCTION

As technology continues to evolve at a rapid pace, so do the risks and threats associate with it. Cybercriminals are becoming more skilled in using advanced techniques to exploit systems, making it increasingly challenging to stay ahead of potential dangers. Cyber-attacks can target both technological systems—through malware or viruses—and people—through tactics like social engineering or cyberbullying [1][2]. Interestingly, many of today's fastest-growing corporate crimes no longer focus solely on exploiting technical vulnerabilities. Instead, they target people, who are often seen as the weakest link in an organization's security chain [3][6]. The digital age has reshaped the cybersecurity landscape significantly. Now, more than ever, individuals and businesses are vulnerable to social engineering attacks. Social engineering involves manipulating human behavior and psychological weaknesses to achieve malicious objectives [7]. These types of attacks have become more common, largely because they exploit personal vulnerabilities that can't be easily fixed with technology alone [8]. Research shows that social media platforms often serve as a launchpad for such attacks. Attackers tend to present their messages in ways that appear trustworthy, increasing the chances that individuals will comply [9]. This sense of legitimacy is shaped by various psychological cues and persuasion tactics that make the source seem credible [10]. In cybersecurity, attackers often bypass technical defenses by targeting people directly, tricking them into handing over sensitive information. These breaches can lead to serious consequences, such as blackmail or further attacks [11]. To combat social engineering, organizations are encouraged to implement clear policies and detailed procedures [12]. Studies emphasize the importance of robust information security programs, including awareness and training initiatives, to help protect valuable data and ensure business resilience [12][13]. Increasing awareness and providing regular training can empower employees to recognize and defend against these threats [3][11][13] [18]. This literature review explores how social engineering impacts different institutions and highlights the role of information security awareness programs in helping employees detect and prevent cyber-attacks.

BACKGROUND

In today's digital age, information security has become a critical area within the field of information technology. Interestingly, the biggest threat to security often isn't the technology itself—but the people using it. Studies have shown that most security breaches are caused by human error, despite having strong systems and well-defined

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XI, November 2025

processes in place [19, 20]. Experts agree that effective information security relies on three main pillars: people, processes, and technology. Even when an organization has advanced systems and well-organized procedures, the human element is often the weakest link. This is especially important because employees are present across all types of organizations—from small businesses to large corporations—making them key targets in cyber-attacks, especially those carried out through social engineering. Research has consistently shown that many computer users lack basic knowledge about cybersecurity, largely due to poor awareness. Both governments and educational institutions have recognized this gap and are working to increase public understanding of cyber threats [16]. For example, the Anti-Phishing Work Group (APWG) is a non-profit that offers anti-phishing training, and the U.S. Computer Emergency Readiness Team provides free online resources to educate users about common cyber risks. Social engineering attacks happen when hackers manipulate people into giving up confidential information or access. These attackers carefully choose their targets—often large telecom companies or organizations that manage vast amounts of personal data—because they stand to gain a lot from a successful attack [20]. Universities are also attractive targets due to their powerful computer systems and generally open access policies [21]. Another growing concern is the use of social media within workplace networks. Employees accessing social media at work has opened up new ways for cybercriminals to infiltrate systems. Studies have shown that this trend poses serious challenges to IT security teams in managing people, processes, and technology [22]. In fact, social engineers are increasingly using social media to gather sensitive information from employees and gain unauthorized access to organizational data [23]. A joint study by Google, the University of California, Berkeley, and the International Computer Science Institute shed light on just how serious the situation has become [24]. They analyzed billions of stolen credentials and found that 788,000 users were potential victims of keyloggers, over 12 million were targeted by phishing kits, and around 2 billion usernames and passwords were exposed through social engineering. These alarming numbers highlight the urgent need to train and educate employees at every level so they can better protect the valuable data they handle.

Understanding Key Terms in Context

Phishing is one of the most common and dangerous types of social engineering attacks. It typically involves tricking someone into thinking a message is from a trusted source—like a bank, company, or government agency—when it's actually from a cybercriminal. The goal is to deceive users into giving up sensitive information, such as passwords or financial details. Although phishing messages can be delivered in many ways, like through text messages or phone calls (VoIP), email and fake websites are still the most widely used methods [25]. In the context of this study, phishing refers to pretending to be a trustworthy source in order to steal private information. To better understand phishing, it helps to look at how it works. A phishing attack often involves a link that appears to be safe—maybe a Google Doc or another familiar-looking webpage. But when the user clicks it, they're taken to a fake version of a legitimate website and asked to enter personal details. Once they do, that information goes straight to the attacker. What makes phishing particularly dangerous is that it doesn't rely on breaking into systems or finding technical vulnerabilities. Instead, it targets human behavior and trust, which is why it's such a widespread and effective social engineering tactic [16, 26].

REVIEW METHODOLOGY

This paper aims to bring together existing research on social engineering and information security awareness. To do that, a two-step approach was used. In the first stage, relevant studies were collected from both areas—specifically focusing on social engineering tactics and educational programs designed to improve cybersecurity awareness. The second stage involved carefully reviewing and analyzing those studies to identify the most common types of social engineering threats. The goal is to highlight how awareness and training programs can make a real difference in helping users understand and avoid these threats. By doing so, this research hopes to support organizations in protecting themselves from cyber-attacks that exploit human behavior.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XI, November 2025

Table I. Average Year and Number of Citations For References Used Per Section

Research Area	Average Year	Average Number of Citations
III - Social Engineering (SE) in a Cyber Security Context	2012	29
IV-Information Security Awareness (ISA)	2012	49
V- ISA on SE	2012	44

Social Engineering in Cybersecurity

Social engineering refers to the manipulation of people to gain access to confidential information or systems by using deception [8][27]. According to the Centre for the Protection of National Infrastructure, different organizations and experts have defined social engineering in terms of both security and psychology [28]. One study describes it as a security breach caused by interactions with an organization's employees [29], while Kevin Mitnick explains it as taking advantage of someone's naivety through influence and persuasion to access valuable information [30]. Essentially, social engineering involves manipulating people to bypass security measures, either physically or digitally [19][28]. For the purpose of this paper, social engineering is defined as the act of persuading or manipulating individuals into revealing sensitive information or granting unauthorized access to restricted systems. Reports like Verizon's "Data Breach Investigations Report 2012" [31] confirm that social engineering poses a threat not only to government organizations and large enterprises but also to individuals, leading to identity theft and other breaches. A well-known case in the news involved Edward Snowden, who used social engineering to persuade several colleagues to grant him access to NSA accounts in Hawaii, resulting in the leak of classified information [32]. This incident highlights how social engineering can bypass even the most secure digital and physical security measures by targeting human vulnerabilities [8]. Social engineering attacks can be carried out in various ways, including face-to-face interactions or through digital means. In the case of online attacks, cybercriminals can automate malicious efforts, making it easier and cheaper to carry out large-scale phishing campaigns, for example, which exploit digital channels [25][33]–[36]. Other studies have explored different aspects of social engineering, such as testing university students for weaknesses [25], analyzing individual vulnerabilities [35], or understanding the characteristics of victims [36]. One notable technique is "automated social engineering," in which attackers gather information from social networks and use these platforms to manipulate individuals into revealing personal details [37]. Many scholars focus on how social engineers exploit trust and emotions to succeed, while others study the effectiveness of privacy training and education in defending against these attacks [19][38]. Social engineering is also a key tactic in Advanced Persistent Threat (APT) attacks [40]. Typically, social engineering attacks follow a common cycle, beginning with information gathering from publicly available sources like social media, phone books, job portals, and websites. The attacker uses this information to build a rapport with the target and eventually gets them to disclose sensitive data, such as login credentials or financial information [28]. This data can either be the attacker's end goal or the first step in a larger cyber-attack. Social engineering can take many forms, from direct face-to-face interactions (like a phone call) to indirect communication through electronic means (like email). Regardless of the method, the goal remains the same: to deceive others into revealing valuable information, committing fraud, or gaining unauthorized access to systems [42].

Information Security Awareness

Information security awareness is a critical part of any organization’s overall security strategy. Employees are key assets because they play a major role in making important security decisions when necessary [15]. Information security awareness programs are designed to help employees develop the knowledge and skills needed to make these decisions. In this paper, information security awareness is defined as ensuring that everyone in an organization understands their role in protecting sensitive data and information. It’s essential that organizations make sure all staff are clear about their responsibilities when it comes to safeguarding the information they handle. In recent years, the importance of protecting information has gained widespread

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XI, November 2025

recognition. More than ever, organizations are focusing on securing their information to protect intellectual property and ensure smooth business operations without interruptions. Research shows that information security professionals agree that employees play a vital role in an organization's overall security [43][44]. However, this responsibility depends on users' ability to make informed security decisions. Therefore, all employees must be educated about potential security threats and understand their role in keeping the organization secure [21]. With proper education and awareness, employees can shift from being a potential vulnerability to an active part of the solution. Experts recommend that organizations develop security strategies that include information security awareness programs and provide proper training for all users. By ensuring that everyone has the right knowledge, organizations can create a culture of security.

Table Ii. List of Articles on Awareness and Training

[13]	Awareness and education programs positively influence staff attitude and behavior towards information security
[51]	Information security is in continuous need for higher levels of awareness and education
[52]	Information security awareness is a lot more effective than other methods
[53]	Implementing information security awareness programs is probably the greatest countermeasure for its efficiency, as it increases understanding and awareness
[54]	Information security training has a positive effect on employees' behavior for compliance
[55]	Employee contribution and knowledge conception integrate positive changes regarding information security awareness and behavior in organizations
[56]	Information security awareness has a significant effect on staff compliance and attitude

The rapid growth of technology and its widespread use has significantly changed how society operates [45]. As information technology continues to evolve quickly, businesses are increasingly turning to solutions like encryption, access control, and CCTV to protect their data [46]. However, many modern security breaches are caused by human error, often due to a lack of awareness about information security [16][47][48]. This highlights that technical solutions alone aren't enough. It's equally important to focus on training and raising awareness among users about how to handle the human aspects of security. While adding more technical tools won't fix user mistakes, providing proper awareness training can lead to much better results [15][49]. Table II summarizes several studies that emphasize the importance of information security awareness. These publications also explore how education and adherence to security protocols improve the effectiveness of security efforts. The research supports the idea that information security awareness programs help organizations create a safer digital environment, protecting valuable data from malicious attacks. By training staff, organizations ensure that employees follow good cybersecurity practices, and these awareness programs work hand-in-hand to shape users' security behaviors and better equip them to handle potential cyber threats [3][6][21][50].

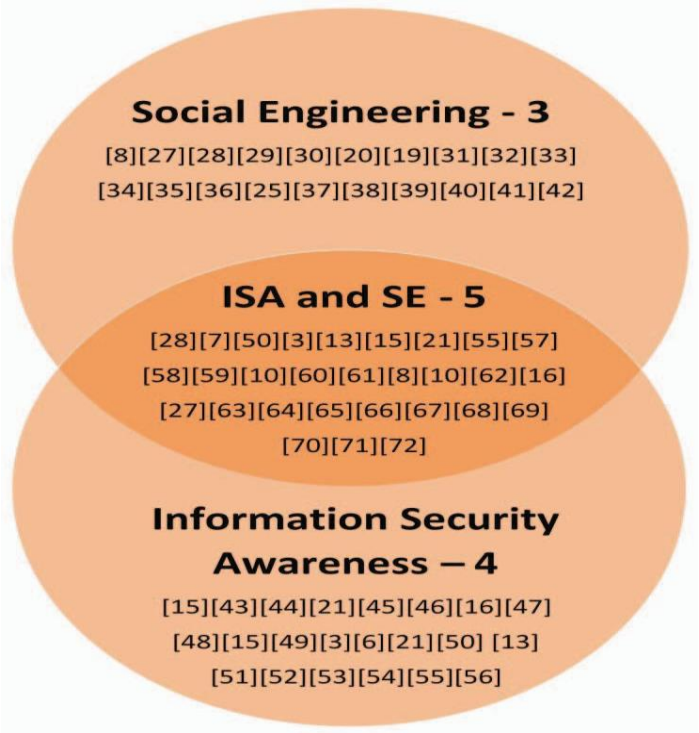
Information Security Awareness in the Context of Social Engineering

Technical attacks and social engineering attacks differ primarily in the level of expertise required to carry them out. Technical attacks typically involve IT staff who are trained to handle security issues. In contrast, social engineering attacks target employees at all levels of an organization, from janitors working after hours to high-level executives. These individuals may lack the technical knowledge or awareness of social engineering threats. For example, many employees don't understand how to classify the information they handle—whether it's general use, sensitive, or classified. It's clear that preventing social engineering breaches requires more than just technical solutions; improving information security awareness across all levels of staff is crucial. A combination of technical security measures and comprehensive awareness training is necessary to build a strong defense

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XI, November 2025

against social engineering attacks [28]. Research suggests that information security awareness programs can protect employees from falling victim to social engineering tactics. For example, Mouton et al. [7] recommend that organizations provide training to all employees to foster a security-conscious culture. They stress the importance of helping employees recognize the various methods that attackers use. Similarly, [50] emphasizes the need for organizations to instill a strong awareness of security to prevent the leakage of confidential information. Numerous other studies [3][13][15][21][55][57]–[59] confirm that without an informed staff, technical defenses alone are inadequate to protect against social engineering attacks. In terms of individual awareness of social engineering threats, several studies have highlighted that users often lack understanding of the security risks associated with their personal devices. For example, research indicates that users of e-health devices are often unaware of the social engineering tactics that could exploit their personal data [10]. Additional

Fig. 1. References used in core sections.



studies, such as those by Bellekens et al. [60], surveyed students and professionals across U.S. universities to explore the privacy risks associated with social engineering in personal e-health services. Participants showed poor understanding of the technologies they used, suggesting the need for new security measures focused on increasing users' awareness of potential threats [60][61]. Human factors play a significant role in safeguarding valuable information, and trust is one of the most important elements in the security equation. Researchers argue that trust is critical to the functioning of an information security system and can greatly influence security behaviors [8][10][62]. A study by [16] found that many computer users lack security awareness and are overly trusting of strangers. This research, along with others, concluded that increasing users' awareness of potential threats and teaching them to recognize the signs of a security risk can significantly improve their ability to protect themselves.

There have been several studies that focus on the effectiveness of teaching methods used in information security awareness programs as a way to prevent social engineering attacks. According to the literature, information security training should be designed to capture users' attention and help them retain the knowledge for a long time [27]. The training process should not only focus on acquiring knowledge but also on ensuring that users can remember and apply it when needed. Effective training programs should give users the chance to regularly engage with the material, making learning a continuous process. In other words, organizations today have a greater responsibility to make sure their employees are fully aware of the potential consequences of social engineering. Offering a variety of information security awareness programs can help companies maintain a baseline level of security to protect their intellectual property. It's widely accepted in the literature that information security awareness plays a critical role in any comprehensive security strategy [52][57][62]–[70].

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XI, November 2025

As a result, implementing a well-structured awareness program can help reduce the risks associated with social engineering attacks, especially those that exploit trust. To sum up, the most effective way to defend against social engineering is through education and awareness, which should be prioritized in any organization. In terms of developing new learning technologies for information security education, there are several methods that show promise:

1. **Online delivery:** This can include email broadcasts, social media campaigns, online discussions (both synchronous and asynchronous), blogging, and animations.

2. **Game-based learning:** Games can challenge, motivate, and engage employees, making the learning process more enjoyable.

3. **Video-based and self-paced learning:** These methods allow employees to learn at their own pace, which can be more flexible for them.

4. **Simulation-based training:** Simulated phishing emails, for example, can be used to assess how susceptible employees are to attacks and measure their awareness levels.

Several studies have proposed innovative learning platforms that move away from traditional classroom training to e-learning techniques. For example, [46] suggests an e-learning platform to track employees' progress through a learning management system. Additionally, Beckers et al. [71] introduced the use of gamification to increase employees' awareness of information security. This gamified approach draws on principles of human behavior that social engineers often exploit, helping employees experience and recognize potential threats. The combination of gamification with security awareness programs creates an interactive and engaging learning experience. Using gamification has been shown to be an effective way for employees to learn about social engineering threats in a structured manner [72]. Through this approach, employees become more aware of the threats they may encounter and develop a greater sense of caution and suspicion when faced with potential attacks. By implementing these modern training methods, organizations can better equip their employees to protect their data and reduce the risks of falling victim to cyber threats.

Research Limitations

This research has some limitations regarding the search methods used to gather relevant literature. Only English search terms were employed, meaning any relevant publications in other languages were excluded from this study. Additionally, some important contributions may not have been covered, especially those found in books, which were not extensively explored in this review. Another challenge identified in the field of information security research is the inconsistent use of terms to describe similar concepts. For instance, terms like "information security education (ISE)," "information security training (IST)," and "information security awareness (ISA)" have been defined differently by various researchers, each with its own emphasis and purpose. Decker [73] highlights the lack of correlation between these concepts due to unclear and varied definitions.

CONCLUSION AND FUTURE WORK

In today's world, organizations are heavily reliant on information systems, which makes them vulnerable to various information security threats. Additionally, social engineering fraud has increased significantly with technological advancements, as criminals find more sophisticated ways to launch attacks. As a result, organizations have been increasing their investments in cybersecurity initiatives to protect their data. This paper has provided an overview of the main social engineering threats and discussed how implementing information security education programs can effectively raise user awareness and help reduce, or even prevent, cybercrimes. Some governments, such as those in Australia and the U.S., have begun legislating laws and regulations to protect citizens and organizations from cyber criminals and social engineering attacks. Organizations, in turn, are adjusting their security policies to address the current social engineering threats that could disrupt their operations. However, staying ahead of cybercriminals remains a challenge. Information security awareness is a critical step toward ensuring a secure digital environment where individuals of all ages can use technology safely and productively. It is considered the most effective approach to combating social engineering threats, especially

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XI, November 2025

as technology has made individuals prime targets for hackers and cybercriminals. Future research could explore additional factors that influence employees' awareness and behavior related to information security, filling a noticeable gap in the current literature. While most of the existing research is quantitative, qualitative studies, such as interviews, could provide deeper insights into this area. Moreover, more attention should be paid to understanding the gap between employees' intentions and their actual social engineering security behaviors. Conducting experiments and case studies will improve our understanding of the limitations of self-reporting and offer a clearer picture of employees' true behaviors in real-world scenarios.

ACKNOWLEDGMENT

The author, Abdul Basir Momand and Osama Zain, would like to acknowledge their position as a faculty lecturer in the Computer Science Department at Rana University of Science and Information Technology, Kabul, Afghanistan. They are also a Certified Ethical Hacker (CEH), certified by EC-Council, with certification number ECC9240761835.

REFERENCES

1. D. Sarathchandra, K. Haltinner, and N. Lichtenberg, "College students' cybersecurity risk perceptions, awareness, and practices," in Proc. Cybersecurity 3rd Symp. (CYBERSEC '16), Coeur d'Alene, ID, 2016, pp. 68–73.
2. S. S. Tirumala, H. Sathu, and V. Naidu, "Analysis and prevention of account hijacking based incidents in cloud environment," in Proc. Int. Conf. Information Technology (ICIT '15), Singapore, 2015, pp. 124–129.
3. B. Lebek, J. Uffen, M. H. Breitner, M. Neumann, and B. Hohler, "Employees' information security awareness and behavior: A literature review," in Proc. 46th Hawaii Int. Conf. System Sciences (HICSS '13), Wailea, HI, 2013, pp. 2978–2987.
4. F. L. Greitzer, J. R. Strozer, S. Cohen, A. P. Moore, D. Mundie, and J. Cowley, "Analysis of unintentional insider threats deriving from social engineering exploits," in Proc. IEEE Security and Privacy Workshops (SPW '14), San Jose, CA, 2014, pp. 236–250.
5. N. Sohrabi Safa, R. Von Solms, and S. Furnell, "Information security policy compliance model in organizations," Comput. & Security, vol. 56, pp. 70–82, Feb. 2016.
6. A. Tsohou, M. Karyda, and S. Kokolakis, "Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs," Comput. & Security, vol. 52, pp. 128–141, Jul. 2015.
7. F. Mouton, M. M. Malan, L. Leenen, and H. S. Venter, "Social engineering attack framework," in Information Security for South Africa (ISSA '14), Johannesburg, South Africa, 2014, pp. 1–9.
8. S. Uebelacker and S. Quiel, "The social engineering personality framework," in Proc. 8th Workshop on Socio–Technical Aspects in Security and Trust (STAST '14), San Juan, PR, 2014, pp. 24–30.
9. J.–W. H. Bullée, L. Montoya, W. Pieters, M. Junger, and P. H. Hartel, "The persuasion and security awareness experiment: reducing the success of social engineering attacks," J. Experimental Criminology, vol. 11, no. 1, pp. 97–115, Jan. 2015.
10. W. Kearney and H. Kruger, "Considering the influence of human trust in practical social engineering exercises, in Proc. Information Security for South Africa (ISSA '14), Johannesburg, South Africa, 2014, pp. 1–6.
11. S. Mohammed and E. Apeh, "A model for social engineering awareness program for schools," in Proc. 10th Int. Conf. Software, Knowledge, Information Management & Applications (SKIMA '16), Chengdu, China, 2016, pp. 392–397.
12. Y. Chen, K. Ramamurthy, and K.–W. Wen, "Impacts of comprehensive information security programs on information security culture," J. Comput. Inform. Syst., vol. 55, no. 3, pp. 11–19, Dec. 2015.
13. K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," Comput. & Security, vol. 42, pp. 165–176, May 2014.
14. M. M. Al-Daeef, N. Basir, and M. M. Saudi, "Security awareness training: A review," in Lecture Notes in Engineering and Computer Science, 2017, vol. 2229, pp. 446–451.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XI, November 2025

15. E. Amankwa, M. Loock, and E. Kritzinger, "A conceptual analysis of information security education, information security training and information security awareness definitions," in Proc. 9th Int. Conf. Internet Technology and Secured Transactions (ICITST '14), London, UK, 2014, pp. 248–252.
16. N. A. G. Arachchilage and S. Love, "Security awareness of computer users: a phishing threat avoidance perspective," Comput. Human Behavior, vol. 38, pp. 304–312, Sep. 2014.
17. W. Ashford, "Lack of cyber security awareness putting UK organisations at risk," ComputerWeekly.com, Mar. 2016.
18. B. K. Eyong, "Recommendations for information security awareness training for college students," Inform. Manage. & Comput. Security, vol. 22, no. 1, pp. 115–126, 2014.
19. G. L. Orgill, G. W. Romney, M. G. Bailey, and P. M. Orgill, "The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems," in Proc. 5th Conf. Information Technology Education (CITC5 '04), Salt Lake City, UT, 2004.
20. Z. L. Svehla, I. Sedinić, and L. Pauk, "Going white hat: Security check by hacking employees using social engineering techniques," in Proc. 39th Int. Conv. Information and Communication Technology, Electronics and Microelectronics (MIPRO '16), Opatija, Croatia, 2016, pp. 1419–1422.
21. A. Farooq, J. Isoaho, S. Virtanen, and J. Isoaho, "Information security awareness in educational institution: an analysis of students' individual factors," in Proc. 13th IEEE Int. Symp. Parallel and Distributed Processing with Applications (ISPA '15), Helsinki, Finland, Aug. 2015, vol. 1, pp. 352–359.
22. H. Wilcox and M. Bhattacharya, "A framework to mitigate social engineering through social media within the enterprise," in Proc. 11th IEEE Conf. Industrial Electronics and Applications (ICIEA '16), Hefei, China, Oct. 2016, pp. 1039–1044.
23. R. Heartfield, G. Loukas, and D. Gan, "An eye for deception: A case study in utilizing the human-as-a-security-sensor paradigm to detect zero-day semantic social engineering attacks," in Proc. 15th IEEE Int. Conf. Software Engineering Research, Management and Applications (SERA '2017), London, UK, Jun. 2017, pp. 371–378.
24. K. Thomas et al., "Data breaches, phishing, or malware? Understanding the risks of stolen credentials," in Proc. ACM SIGSAC Conf. Computer and Communications Security, Dallas, TX, Oct. 2017, pp. 1421–1434
25. J. G. Mohebzada, A. E. Zarka, A. H. Bhojani, and A. Darwish, "Phishing in a university community: Two large scale phishing experiments," in Proc. Int. Conf. Innovations in Information Technology (IIT '12), Abu Dhabi, UAE, Jun. 2012, pp. 249–254.
26. T. Kathirvalavakumar, K. Kavitha, and R. Palaniappan, "Efficient harmful email identification using neural network," British J. Math. & Comput. Sci., vol. 7, no. 1, p. 58, 2015.
27. A. S. Alazri, "The awareness of social engineering in information revolution: Techniques and challenges," in Proc. 10th Int. Conf. Internet Technology and Secured Transactions (ICITST '15), London, UK, Dec. 2015, pp. 198–201.
28. I. Ghafir, V. Prenosil, A. Alhejailan, and M. Hammoudeh, "Social engineering attack strategies and defence approaches," in Proc. 4th IEEE Int. Conf. Future Internet of Things and Cloud (FiCloud '16), Vienna, Austria, Aug. 2016, pp. 145–149.
29. M. Bezuidenhout, F. Mouton, and H. S. Venter, "Social engineering attack detection model: SEADM," in Proc. Information Security for South Africa (ISSA '14), Johannesburg, South Africa, Aug. 2010, pp. 1–8.
30. K. D. Mitnick and W. L. Simon, The Art of Deception: Controlling the Human Element of Security. Indianapolis, IN: Wiley, 2011.
31. V. R. Team, "Data breach investigations report (2012)," ed, 2012.
32. M. Hosenball and W. Strobel. (2013, Nov. 7). Exclusive: Snowden persuaded other NSA workers to give up passwords – sources. [Online]. Available: https://www.reuters.com/article/net-us-usa-security-snowden/exclusive-snowden-persuaded-other-nsa-workers-to-give-up-passwords-sources-idUSBRE9A703020131108
33. M. Workman, "Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security," J. Assoc. Inform. Sci. Technol., vol. 59, no. 4, pp. 662–674, 2008.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XI, November 2025

34. J. L. Parrish Jr., J. L. Bailey, and J. F. Courtney, "A personality-based model for determining susceptibility to phishing attacks," in Proc. Southwest Decision Sciences Institute Annu. Meeting (SDSI '09). Oklahoma City, OK, 2009, pp. 285–296.
35. A. Vishwanath, T. Herath, R. Chen, J. Wang, and H. R. Rao, "Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model," Decision Support Syst., vol. 51, no. 3, pp. 576–586, Jun. 2011.
36. A. Darwish, A. El Zarka, and F. Aloul, "Towards understanding phishing victims' profile," in Proc. Int. Conf. Comput. Sys and Industrial Informatics, Sharjah, UAE, Dec. 2012, pp. 1–5.
37. M. Huber, S. Kowalski, M. Nohlberg, and S. Tjoa, "Towards automating social engineering using social networking sites," in Proc. Int. Conf. Computational Science and Engineering, Vancouver, Canada, Aug. 2009, vol. 3, pp. 117–124.
38. S. Abraham and I. Chengalur-Smith, "An overview of social engineering malware: Trends, tactics, and implications," Technol. in Soc., vol. 32, no. 3, pp. 183–196, 2010.
39. J. W. Scheeres, "Establishing the human firewall: reducing an individual's vulnerability to social engineering attacks," MS thesis, Dept. Elec. & Comput. Eng., Air Inst. Technol., Dayton, OH, 2008.
40. I. Ghafir and V. Prenosil, "Proposed approach for targeted attacks detection," in Advanced Computer and Communication Engineering Technology: Proceedings of ICOCOE 2015 (Lecture Notes in Elect. Eng, vol. 362), H. A. Sulaiman, M. A. Othman, M. F. I. Othman, Y. A. Rahim, and N. C. Pee, Eds. Cham, Switzerland: Springer, 2016, pp. 73–80.
41. A. Algarni, Y. Xu, T. Chan, and Y.-C. Tian, "Social engineering in social networking sites: Affect-based model," in Proc. 8th Int. Conf. Internet Technology and Secured Transactions (ICITST '13), London, UK, Dec. 2013, pp. 508–515
42. A. Kumar, M. Chaudhary, and N. Kumar, "Social engineering threats and awareness: a survey," European J. Advances Eng. & Technol., vol. 2, no. 11, pp. 15–19, 2015.
43. E. Albrechtsen and J. Hovden, "The information security digital divide between information security managers and users," Comput. & Security, vol. 28, no. 6, pp. 476–490, Sep. 2009.
44. A. Da Veiga and J. H. Eloff, "A framework and assessment instrument for information security culture," Comput. & Security, vol. 29, no. 2, pp. 196–207, Mar. 2010.
45. J. Abawajy, "User preference of cyber security awareness delivery methods," Behavior & Inform. Technol., vol. 33, no. 3, pp. 237–248, Aug. 2014.
46. J. Holdsworth and E. Apeh, "An effective immersive cyber security awareness learning platform for businesses in the hospitality sector," in Proc. 25th IEEE Int. Requirements Engineering Conf. Workshops (REW '17), Lisbon, Portugal, Sep. 2017, pp. 111–117.
47. K. Korpela, "Improving cyber security awareness and training programs with data analytics," Inform. Security J.: A Global Perspective, vol. 24, no. 1–3, pp. 72–77, Jun. 2015.
48. M. Junger, L. Montoya, and F. J. Overink, "Priming and warnings are not effective to prevent social engineering attacks," Comput. Human Behavior, vol. 66, pp. 75–87, Jan. 2017.
49. R. Butler, "Investigation of phishing to develop guidelines to protect the internet consumer's identity against attacks by phishers, " South African J. Inform.Manage., vol. 7, no. 3, Sep. 2005.
50. W. Rocha Flores and M. Ekstedt, "Shaping intention to resist social engineering through transformational leadership, information security culture and awareness," Comput. & Security, vol. 59, pp. 26–44, Jun. 2016.
51. M. E. Whitman, " In defense of the realm: understanding the threats to information security," Int. J. Inform. Manage., vol. 24, no. 1, pp. 43–57, Feb. 2004.
52. J. Merete Hagen, E. Albrechtsen, and J. Hovden, "Implementation and effectiveness of organizational information security measures," Inform. Manage.& Comput. Security, vol. 16, no. 4, pp. 377–397, 2008.
53. Q. Ma, M. B. Schmidt, and J. M. Pearson, "An integrated framework for information security management," Rev. Bus., vol. 30, no. 1, p. 58, 2009.
54. P. Puhakainen and M. Siponen, "Improving employees' compliance through information systems security training: An action research study," MIS Quarterly, pp. 757–778, 2010.
55. E. Albrechtsen and J. Hovden, "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study," Comput. & Security, vol. 29, no. 4, pp. 432–445, Jun. 2010.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XI, November 2025

56. M. Siponen, M. A. Mahmood, and S. Pahnila, "Employees' adherence to information security policies: an exploratory field study," Inform. & Manage., vol. 51, no. 2, pp. 217–224, 2014.
57. B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," MIS Quarterly, vol. 34, no. 3, pp. 523–548, 2010.
58. P. Kathryn, M. Agata, P. Malcolm, B. Marcus, and J. Cate, "A study of information security awareness in Australian government organisations," Inform. Manage. & Comput. Security, vol. 22, no. 4, pp. 334–345, 2014.
59. A. Wilk, "Cyber security education and law," in Proc. IEEE Int. Conf. Software Science, Technology and Engineering (SWSTE '16), Beer- Sheva, Israel, Jun. 2016, pp. 94–103.
60. X. Bellekens, A. Hamilton, P. Seeam, K. Nieradzinska, Q. Franssen, and A. Seeam, "Pervasive eHealth services a security and privacy risk awareness survey," in Proc. Int. Conf. Cyber Situational Awareness, Data Analytics and Assessment (CyberSA '16), London, UK, Jun. 2016, pp. 1–4.
61. R. Alavi, S. Islam, and H. Mouratidis, "Human factors of social engineering attacks (SEAs) in hybrid cloud environment: Threats and risks," in Proc. Int. Conf. Global Security, Safety, and Sustainability, London, UK, Sep. 2015, pp. 50–56.
62. C. Colwill, "Human factors in information security: The insider threat– who can you trust these days?," Inform. Security Tech. Rep., vol. 14, no. 4, pp. 186–196, Nov. 2009.
63. N. F. Doherty, L. Anastasakis, and H. Fulford, "The information security policy unpacked: A critical study of the content of university policies," Int. J. Inform. Manage., vol. 29, no. 6, pp. 449–457, Dec. 2009.
64. H. Mouratidis, H. Jahankhani, and M. Z. Nkhoma, "Management versus security specialists: An empirical study on security related perceptions," Inform. Manage. & Comput. Security, vol. 16, no. 2, pp. 187–205, 2008.
65. K. J. Knapp, T. E. Marshall, R. Kelly Rainer, and F. Nelson Ford, "Information security: management's effect on culture and policy," Inform. Manage. & Comput. Security, vol. 14, no. 1, pp. 24–36, 2006.
66. E. McFadzean, J.-N. Ezingeard, and D. Birchall, "Perception of risk and the strategic impact of existing IT on information security strategy at board level," Online Inform. Rev., vol. 31, no. 5, pp. 622–660, 2007.
67. J. L. Spears and H. Barki, "User participation in information systems security risk management," MIS Quarterly, pp. 503–522, Sep. 2010.
68. M. Siponen and A. Vance, "Neutralization: new insights into the problem of employee information systems security policy violations," MIS Quarterly, pp. 487–502, 2010.
69. F. Cervone, "Understand the big picture so you can plan for network security," Comput. in Libraries, vol. 25, no. 3, pp. 10–15, 2005.
70. D. Tse, Z. Xie, and Z. Song, "Awareness of information security and its implications to legal and ethical issues in our daily life," in Proc. IEEE Int. Conf. Industrial Engineering and Engineering Management (IEEM'17), 2017, pp. 1236–1240.
71. K. Beckers and S. Pape, "A serious game for eliciting social engineering security requirements," in Proc. 24th IEEE Int. Conf. Requirements Engineering (RE'16), Beijing, China, Sep. 2016, pp. 16–25.
72. G. Jin, M. Tu, T.-H. Kim, J. Heffron, and J. White, "Game based cybersecurity training for high school students," in Proc. 49th ACM Tech. Symp. Comp. Sci. Educ. (SIGCSE '18), Baltimore, MD, Feb. 2018, pp. 68–73.
73. L. Decker, "Factors affecting the security awareness of end-users: A survey analysis within institutions of higher learning," PhD dissertation, School of Bus. & Technol., Cappella Univ., Minneapolis, MN, 2008.