American Journal of Engineering Research (AJER) **2026**
American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN: 2320-0936
Volume-15, Issue-6, pp-43-50
www.ajer.org
Research Paper Open Access

Social Engineering and Its Impact on Cybersecurity: Implications and Consequences for High School Students

Saad Fadhıl ALSOWADI, Remzi YILDIRIM
Tokat Gaziosmanpaşa University, Department of Computer Engineering, TÜRKİYE

Abstract
Social engineering represents one of the most significant cybersecurity threats of the digital era, relying on psychological manipulation rather than technical exploitation to deceive individuals into divulging confidential information or performing actions that compromise their security. High school students, who are among the most active users of digital technologies, are particularly vulnerable to such attacks due to their developmental stage, limited experience with deceptive tactics, and high levels of social media engagement. This research article examines the nature and scope of social engineering attacks targeting adolescents in secondary education, investigates the psychological and social factors that render this demographic susceptible to manipulation, and analyzes the academic, psychological, and social consequences of falling victim to such attacks. Drawing on a comprehensive review of 50 scholarly sources, the article further explores evidence-based prevention strategies, school-based cybersecurity education programs, and the roles that educators, parents, and policymakers must play in protecting young people in the digital environment. Findings suggest that multi-layered interventions combining awareness training, critical thinking development, parental guidance, and institutional policy are essential to effectively mitigating the risks posed by social engineering to high school students.
Keywords: *social engineering, cybersecurity, high school students, phishing, adolescents, cyber awareness, psychological manipulation, digital safety*

Date of Submission: 05-06-2026 Date of acceptance: 16-06-2026

I. Introduction

The rapid proliferation of digital technologies and internet-connected devices has fundamentally transformed the lives of adolescents worldwide. High school students today are digital natives, seamlessly integrating smartphones, social media platforms, online gaming, and e-learning tools into their daily routines. While this digital fluency offers numerous educational and social benefits, it also exposes young people to a wide array of cybersecurity threats, among which social engineering stands out as particularly insidious and pervasive. Social engineering, broadly defined as the use of psychological manipulation to deceive individuals into taking actions or divulging information that serves the attacker's interests, has become a dominant vector for cybercrime [1]. Unlike traditional cyberattacks that rely on exploiting software vulnerabilities or deploying malware, social engineering targets the human element of security—exploiting cognitive biases, emotional responses, and social dynamics to bypass technical defenses [2]. The consequences for victims can be severe, ranging from identity theft and financial fraud to emotional distress and reputational damage.

High school students occupy a uniquely vulnerable position in the landscape of social engineering targets. Adolescence is a developmental period characterized by heightened social sensitivity, identity formation, and a desire for peer acceptance—psychological characteristics that skilled social engineers can exploit with relative ease [3]. Furthermore, research indicates that young people often overestimate their ability to identify deceptive online content while simultaneously underestimating the sophistication of modern social engineering campaigns [4]. Despite the growing recognition of cybersecurity as a critical life skill, cybersecurity education in secondary schools remains inconsistent and often inadequate. Many school curricula focus primarily on technical skills such

as coding or software use, neglecting the critical thinking and security awareness competencies needed to recognize and resist social engineering attempts [5].

The present article aims to provide a comprehensive examination of the impact of social engineering on high school students. It begins with a conceptual overview of social engineering, tracing its definitions, typologies, and key techniques. It then examines the specific vulnerabilities of the adolescent population and the documented impacts on their academic performance, psychological well-being, and social relationships. Finally, it reviews the evidence base for prevention and awareness programs, offering practical recommendations for schools, parents, and policymakers. By consolidating current knowledge from diverse disciplinary perspectives—including cybersecurity, psychology, education, and criminology—this article seeks to inform more effective responses to a growing and evolving threat.

II. Defining Social Engineering

The term "social engineering" has been used in various contexts, but within the field of information security it refers specifically to the manipulation of human psychology to gain unauthorized access to systems, data, or physical spaces [6]. Had Nagy [1] defines social engineering as "any act that influences a person to take an action that may or may not be in their best interest." This broad definition encompasses a wide spectrum of deceptive practices, from simple pretextual phone calls to elaborate multi-stage campaigns involving forged credentials and impersonation. Unlike conventional cyberattacks, social engineering exploits the predictable patterns of human behavior rather than technical flaws. Cialdini's foundational work on the psychology of influence identified six key principles—reciprocity, commitment, social proof, authority, liking, and scarcity—that are frequently weaponized by social engineers [7]. By strategically invoking one or more of these principles, attackers can manipulate even technically sophisticated individuals into making security-compromising decisions.

While the term itself is relatively recent, social engineering tactics have been employed throughout history in espionage, confidence schemes, and fraud. In the context of information security, social engineering was prominently brought to public attention by Kevin Mitnick, arguably the world's most famous hacker, who revealed in his memoir that the majority of his intrusions were accomplished not through technical hacking but through skillful manipulation of employees [2]. Since then, the field has evolved dramatically alongside the rise of the internet and social media, giving social engineers unprecedented reach and new tools for research and impersonation. Contemporary social engineering campaigns are frequently sophisticated, well-researched operations that may involve weeks of preparation, open-source intelligence gathering, and customized psychological profiling of targets [8]. The rise of social media has been particularly impactful, as platforms like Instagram, TikTok, Snapchat, and Discord—all heavily used by high school students—provide attackers with detailed personal information that can be exploited to craft highly convincing deceptive communications.

III. Types and Techniques of Social Engineering

Phishing is among the most prevalent forms of social engineering, involving the dispatch of fraudulent communications—typically emails—that appear to originate from reputable sources in order to induce recipients to reveal sensitive information or click malicious links [9]. Spear phishing is a more targeted variant in which the attacker personalizes the communication based on detailed knowledge of the target, dramatically increasing its effectiveness [10]. For high school students, phishing attacks often masquerade as messages from gaming platforms, social media services, educational institutions, or attractive offers for free content. Research by Parsons et al. [11] found that phishing emails employing authority cues and urgency messaging were significantly more successful than generic attempts. These findings have direct implications for adolescent targets, who may be especially susceptible to messages appearing to come from authority figures such as school administrators, platform operators, or even law enforcement.

Pretexting involves the creation of a fabricated scenario (the "pretext") designed to extract information from the target [12]. In practice, this might involve an attacker posing as a school IT technician needing a student's login credentials, or a fake representative from a prize-awarding organization requesting personal details. Pretexting exploits the human tendency to comply with requests when they are accompanied by a plausible and legitimate-seeming context.

Baiting attacks leverage the target's curiosity or greed, offering something enticing in exchange for an action that compromises their security [13]. Physical baiting might involve leaving infected USB drives in school corridors or libraries, while digital baiting might offer free downloads of popular music, games, or academic resources. High school students, who frequently seek free access to entertainment and educational content, are a natural target for such tactics.

Voice phishing (vishing) involves manipulative phone calls, while smishing uses SMS text messages [14]. Both modalities are increasingly used against young people. A smishing attack might present itself as a notification from a popular social media platform warning of an account breach, directing the student to a fraudulent website where credentials are harvested. The proliferation of mobile phone use among adolescents—with studies showing that many teenagers check their phones hundreds of times per day—makes these channels particularly effective [15].

Social media platforms present unique social engineering opportunities. Attackers may create fake profiles to befriend targets, establishing trust over time before exploiting the relationship for information or access [16]. They may also exploit publicly shared information to personalize attacks, use peer pressure dynamics to encourage unsafe behavior, or spread disinformation designed to provoke specific emotional and behavioral responses. Jagatic et al. [17] demonstrated that phishing attacks exploiting social network connections were dramatically more successful than conventional phishing, with click-through rates as high as 72%.

IV. Psychological Vulnerabilities of Adolescents

The adolescent stage of development creates specific psychological vulnerabilities that social engineers can exploit. Adolescence is characterized by ongoing development of the prefrontal cortex—the brain region responsible for impulse control, risk assessment, and long-term planning—meaning that teenagers are neurologically predisposed to impulsive decision-making and risk-taking behavior [18]. Social engineers who create urgency or emotional arousal in their communications can effectively bypass the slower, deliberative cognitive processes that would otherwise evaluate the legitimacy of a request. Identity formation is another key developmental process during adolescence. Young people are actively constructing their sense of self, exploring social roles, and seeking validation from peers and authority figures alike [19]. This makes them particularly susceptible to appeals to social proof, authority, and belonging—three of the most potent tools in the social engineer's arsenal.

Despite their extensive use of digital technologies, research consistently shows that adolescents tend to overestimate their ability to identify online deception [20]. This "digital overconfidence" paradox—in which high levels of technology use are mistaken for high levels of security awareness—may actually increase vulnerability by reducing the vigilance that would lead young people to question suspicious communications. Workman [21] found that overconfident users were significantly less likely to recognize phishing attempts, a finding with direct implications for adolescent cybersecurity education.

The intense peer orientation of adolescence creates social dynamics that can be weaponized by social engineers [22]. Students may be manipulated into sharing credentials or personal information through appeals to peer belonging, threats of social exclusion, or the exploitation of romantic interests. Online environments, where social cues are limited and deception is easier to maintain, amplify these dynamics considerably. Cyberbullying and romance scams targeting teenagers often employ social engineering tactics, demonstrating the intersection of psychosocial manipulation and cybercrime.

Adolescents are socialized to comply with authority figures, a disposition that social engineers exploit through impersonation of teachers, school administrators, platform operators, and law enforcement [23]. Research by Bullee et al. [24] demonstrated that authority-based social engineering attacks achieved significantly higher success rates than those relying on other persuasion principles. For high school students who are accustomed to receiving instructions from adults and institutional authorities, such attacks can be particularly effective.

V. Impacts on High School Students

The academic consequences of social engineering victimization can be both direct and indirect. Directly, students may experience theft of academic credentials, allowing attackers to access learning management systems, submit fraudulent work, or compromise examination integrity [25]. Indirectly, the psychological aftermath of victimization—including stress, anxiety, and loss of trust in digital systems—can impair concentration, motivation, and academic performance. Research on the educational impact of cybercrime victimization suggests that affected students may experience measurable declines in academic achievement, particularly when the incident involves public exposure or social humiliation [26]. The increasing use of online learning platforms and digital resources in contemporary high schools creates additional vulnerabilities. Students' accounts on these systems may contain sensitive personal information, assignment histories, and communication records that could be exploited for blackmail or identity fraud. The COVID-19 pandemic's acceleration of remote learning dramatically expanded the attack surface for social engineering targeting students, a trend that has persisted in the post-pandemic hybrid learning environment [27].

The psychological impact of social engineering victimization on adolescents can be severe and long-lasting. Victims frequently experience a range of negative psychological outcomes including anxiety, depression, paranoia, shame, and post-traumatic stress symptoms [28]. The experience of being deceived and manipulated can undermine trust in others more broadly, contributing to social withdrawal and difficulties in forming authentic relationships. Adolescents, whose sense of identity and self-worth is still developing, may be particularly vulnerable to the shame and self-blame that often accompany victimization. When social engineering attacks result in the exposure of private information or images—as in sextortion attacks, which frequently target teenagers—the psychological consequences can be catastrophic [29]. Research documents cases in which such exposure has led to severe depression, self-harm, and suicidal ideation among adolescent victims. The combination of public humiliation, loss of privacy, and perceived permanence of digital exposure creates a uniquely devastating form of victimization for young people who are just beginning to establish their social identities.

Social engineering attacks often result in the theft or manipulation of social media accounts, enabling attackers to impersonate victims, spread disinformation, or access private communications [30]. For high school students, whose social lives are heavily conducted through digital platforms, account compromise can have devastating social consequences. Reputational damage resulting from impersonation or the exposure of private communications can lead to bullying, social ostracism, and lasting damage to peer relationships. Financial consequences, while often less prominent in discussions of adolescent cybervictimization, are also significant. Students may be manipulated into sharing payment information, making fraudulent purchases, or participating in money mule schemes, resulting in financial losses that affect not only the student but also their families [31]. The FBI's Internet Crime Complaint Center reported that younger victims, including teenagers, are increasingly targeted by fraud schemes leveraging social engineering tactics [32].

VI. Prevention and Awareness Strategies

The most direct institutional response to the threat of social engineering is the integration of comprehensive cybersecurity education into school curricula. Effective cybersecurity education for high school students goes beyond basic digital literacy to encompass critical thinking skills, threat recognition, and practical security behaviors [33]. Research evaluating school-based cybersecurity programs suggests that well-designed interventions can significantly improve students' ability to recognize social engineering attempts and respond appropriately [34]. Tschakert and Watkins [35] argue for a dual approach that combines formal curriculum content with informal, experiential learning opportunities such as cybersecurity competitions, capture-the-flag events, and simulated phishing exercises. The latter approach—using controlled simulations to expose students to realistic social engineering scenarios—has shown particular promise in developing practical recognition skills while providing immediate feedback and learning opportunities. However, such simulations must be carefully designed and conducted ethically to avoid causing unnecessary distress or stigmatization of those who fall for the exercise.

A fundamental component of effective social engineering prevention is the development of critical thinking and media literacy skills that enable students to evaluate the authenticity of digital communications [36]. This includes training in source verification, recognition of urgency and fear-based manipulation tactics, understanding of common deception techniques, and awareness of the information that social engineers can glean from social media profiles. Media literacy education that addresses the specific characteristics of social engineering—such as appeals to authority, artificial urgency, and emotional manipulation—is particularly relevant for the adolescent population. Research by Salahdine and Kaabouch [37] emphasizes the importance of teaching students to pause and verify before acting on unexpected requests, particularly those involving the sharing of personal information or credentials. This "stop, think, connect" approach, promoted by the National Cyber Security Alliance and similar organizations, provides a simple but effective cognitive framework that can interrupt the automatic compliance responses that social engineers seek to trigger [47].

While human awareness is essential, technical safeguards play an important complementary role in protecting students from social engineering attacks [38]. Schools and educational technology providers should implement robust email filtering systems capable of detecting phishing attempts, multi-factor authentication for all student accounts, and clear procedures for reporting suspected social engineering incidents. Privacy settings on school-managed devices and accounts should be configured to minimize the information available to potential attackers. The principle of least privilege—ensuring that students have access only to the systems and information they need for legitimate academic purposes—can limit the damage caused if an account is compromised through social engineering [39]. Similarly, regular security awareness communications from schools can help establish a culture of vigilance, normalize reporting of suspicious incidents, and provide students with current information about emerging threats targeting their demographic.

Parents play a crucial role in protecting high school students from social engineering threats. Research indicates that open communication between parents and teenagers about online safety is associated with lower rates of cybervictimization [40]. Parents who maintain awareness of their children's online activities, discuss potential threats without judgment, and establish clear family norms around digital security can significantly reduce vulnerability. Family-based interventions should address both the technical aspects of online safety—such as privacy settings, password management, and two-factor authentication—and the psychological dimensions of social engineering, including the manipulation tactics most commonly used against young people [41]. Educational resources designed specifically for parents, such as those provided by organizations like the National Cyber Security Alliance and the Internet Keep Safe Coalition, can help families engage productively with these topics.

VII. Institutional and Policy Responses

Effective institutional responses to social engineering threats require coherent policy frameworks that address prevention, response, and recovery [42]. School policies should clearly define acceptable use of digital resources, establish procedures for reporting suspected social engineering incidents, and outline the support available to students who have been victimized. Training programs for educators and school staff—who themselves may be targeted as vectors for attacks on students—are an essential component of institutional preparedness. Incident response planning is particularly important, as rapid and appropriate institutional responses to social engineering incidents can significantly limit their impact [43]. Schools should have clear protocols for responding to account compromises, data breaches, and other security incidents, including communication strategies that provide affected students and families with timely and accurate information without creating unnecessary alarm or stigmatization.

Legislative and regulatory frameworks governing cybersecurity education and student data protection provide an important backdrop for institutional responses to social engineering. In the United States, the Children's Online Privacy Protection Act (COPPA) and the Family Educational Rights and Privacy Act (FERPA) establish baseline protections for student data, while various state laws address cyberbullying and online harassment [44]. The European Union's General Data Protection Regulation (GDPR) similarly provides protections relevant to the educational context. However, legislation alone cannot address the human factors that make social engineering so effective; it must be complemented by robust education and awareness initiatives. International bodies such as the International Telecommunication Union and the European Union Agency for Cybersecurity (ENISA) have developed frameworks and resources specifically addressing the cybersecurity needs of young people [45, 46]. These resources provide valuable guidance for national and local policy development, offering evidence-based recommendations for integrating cybersecurity education into school systems.

Effective responses to social engineering threats targeting adolescents require collaboration among multiple stakeholder groups, including schools, families, technology companies, law enforcement, and civil society organizations [48]. Technology companies, in particular, bear significant responsibility for designing platforms that minimize exploitation opportunities, provide effective reporting mechanisms, and respond promptly to cases of social engineering and related harms on their services. Industry-education partnerships can support the development of relevant, up-to-date curriculum materials and provide students with authentic cybersecurity learning experiences.

VIII. Emerging Threats and Future Directions

The rapid development of artificial intelligence technologies is dramatically expanding the capabilities of social engineers and creating new challenges for protection efforts. AI-powered tools now enable the generation of highly convincing deep fake audio and video content that can be used to impersonate trusted individuals, the automated crafting of personalized phishing messages at scale, and the creation of highly realistic fake social media profiles [49]. For high school students who rely heavily on video and audio communication through platforms like Snapchat and Discord, AI-generated impersonation attacks represent a particularly significant emerging threat. Large language models and other generative AI systems can also be used to produce flawless, contextually appropriate social engineering content at minimal cost, removing previous barriers to entry in terms of linguistic skill and knowledge of the target. This democratization of social engineering capabilities means that the threat landscape for adolescents is likely to become significantly more challenging in coming years, placing additional urgency on the development of robust awareness and resistance skills.

Despite the growing recognition of social engineering as a critical threat to adolescents, the academic literature on this specific population remains relatively sparse. Future research is needed to better understand the

specific mechanisms by which different social engineering techniques affect adolescents at different developmental stages, the relative effectiveness of different educational and prevention approaches, and the long-term consequences of victimization on academic outcomes, psychological health, and future security behaviors [50]. Longitudinal studies tracking cohorts of students through their high school years would be particularly valuable in illuminating these dynamics. Research is also needed on the specific vulnerabilities created by different digital platforms and communication modalities, the role of cultural and socioeconomic factors in shaping social engineering vulnerability and resilience, and the development of validated assessment tools for measuring students' social engineering awareness and resistance skills.

IX. Synthesis of Findings

The evidence reviewed across the preceding sections converges on a coherent and troubling picture: high school students are not merely incidental targets of social engineering but constitute a structurally vulnerable population whose exploitation is, to a meaningful degree, predictable and preventable.The synthesis of findings from cybersecurity, developmental psychology, criminology, and education research reveals that vulnerability in this demographic is not simply a function of ignorance—although gaps in awareness are significant—but rather reflects a more fundamental interaction between the psychological characteristics of adolescence, the social architecture of digital platforms, and the persistent inadequacy of institutional responses.

A central theme emerging from the literature is what might be termed the vulnerability paradox of digitally native adolescents. Young people who have grown up immersed in digital technology often exhibit high levels of confidence in their online competencies, yet research consistently demonstrates that this confidence is poorly calibrated with respect to social engineering threats specifically]. The mechanisms underlying this paradox are important for intervention design: if students are approached as naïve users requiring only basic education, programs may fail to engage their self-concept as capable digital actors. More effective interventions may be those that reframe social engineering awareness not as remediation of ignorance but as the cultivation of a higher-order critical skill—one that challenges rather than contradicts students' sense of themselves as digitally sophisticated.

The psychological vulnerability factors identified in Section 4 deserve particular emphasis in this synthesis. Adolescent brain development, with its characteristic prioritization of social rewards and reduced capacity for deliberative risk assessment, creates conditions that are inherently exploitable by social engineering tactics. This neurobiological dimension of vulnerability is frequently absent from cybersecurity education frameworks, which tend to focus on behavioral habits and procedural knowledge rather than underlying cognitive mechanisms. A more scientifically grounded approach would incorporate insights from developmental neuroscience and behavioral economics to design interventions that work with, rather than against, the cognitive architecture of the adolescent brain.

The documented impacts reviewed in Section 5 further underscore the stakes involved. The convergence of academic, psychological, and social consequences associated with social engineering victimization suggests that the harm is not merely transient inconvenience but can produce lasting developmental disruption. Particularly concerning is the evidence linking online victimization—including sextortion and account compromise—to severe psychological sequelae in adolescents. These findings reinforce the argument that social engineering directed at high school students should be treated as a serious safeguarding concern, not merely a technical security issue, and that institutional responses must be correspondingly comprehensive.

From a theoretical standpoint, the findings of this review call for a more integrated conceptual framework for understanding social engineering vulnerability in adolescents. Existing theoretical models of susceptibility—including the Heuristic-Systematic Model applied by Vishwanath et al. [33], the persuasion-based framework of Wright et al., and the social cognitive approaches of Williams et al.—were largely developed and validated in adult organizational settings. Their direct applicability to the adolescent context requires careful examination and likely significant modification. The present review suggests that a comprehensive theoretical model of adolescent social engineering vulnerability would need to integrate at least three distinct analytical levels: the individual level (developmental stage, digital self-efficacy, personality, and cognitive processing), the social level (peer influence, trusted relationships, and victimization consequences), and the environmental level (platform design, institutional context, and sociocultural norms around privacy and digital trust).

For educational practitioners and institutional policymakers, the findings of this review carry several concrete and actionable implications. First, cybersecurity education for high school students should be conceptualized as a core competency embedded across the curriculum, rather than treated as an isolated technical module or a periodic awareness campaign. Second, the evidence strongly supports the adoption of experiential and simulation-based pedagogies in social engineering education. Third, the reviewed evidence consistently highlights the importance of parental engagement as a protective factor, yet intervention programs rarely address

families systematically]. Finally, the policy environment must evolve to better support institutional responses to social engineering targeting adolescents.

Several limitations of the present review merit acknowledgment. Most importantly, the empirical literature specifically addressing social engineering and high school students remains relatively limited in depth and scope. A substantial proportion of the studies cited were conducted with adult samples—typically university students or organizational employees—and the generalizability of their findings to secondary school adolescents must be treated with appropriate caution. Additionally, the majority of existing empirical research has been conducted in Western, high-income country contexts, and there is limited evidence regarding how cultural factors, socioeconomic conditions, educational system characteristics, and varying levels of technological infrastructure interact with social engineering vulnerability in diverse high school populations globally. Furthermore, the rapid evolution of social engineering technology—particularly the integration of generative artificial intelligence tools—means that some findings cited in this review may already be partially outdated with respect to the contemporary threat landscape.

X. Conclusion

Social engineering represents a profound and growing threat to high school students, one that exploits the distinctive psychological characteristics of adolescence, the patterns of digital engagement that define teenage life, and the gaps in cybersecurity awareness that persist in many educational systems. The impacts of social engineering victimization—spanning academic performance, psychological well-being, and social relationships—underscore the urgency of developing more effective responses to this challenge. This article has examined the nature of social engineering attacks targeting adolescents, the psychological vulnerabilities that make this population particularly susceptible, and the documented consequences of victimization. It has also reviewed the evidence base for preventive interventions, highlighting the importance of comprehensive cybersecurity education, critical thinking development, parental engagement, technical safeguards, and coherent institutional policies.

The findings of this review point to several key principles that should guide efforts to protect high school students from social engineering. First, effective protection requires a multi-layered approach that addresses both the human and technical dimensions of security. Second, education and awareness programs must be grounded in an understanding of adolescent psychology and the specific characteristics of contemporary social engineering attacks. Third, schools, families, technology companies, and policymakers must work collaboratively to create an environment in which young people have the knowledge, skills, and support systems needed to navigate digital spaces safely. As social engineering techniques continue to evolve—driven by advances in artificial intelligence and the ever-expanding digital footprint of adolescents—the challenge of protecting high school students will only intensify. Meeting this challenge requires sustained commitment from all stakeholders: researchers advancing our understanding of the threat and effective responses; educators integrating security awareness into the curriculum; parents maintaining open dialogue about digital safety; technology companies designing safer platforms; and policymakers establishing frameworks that support comprehensive, evidence-based protection. The digital safety of the next generation depends on the collective effort to rise to this challenge.

References

[1]. Had Nagy, C. (2018). Social Engineering: The Science of Human Hacking (2nd ed.). Indianapolis, IN: Wiley.
[2]. Mitnick, K. D., & Simon, W. L. (2002). The Art of Deception: Controlling the Human Element of Security. Indianapolis, IN: Wiley.
[3]. Cialdini, R. B. (2006). Influence: The Psychology of Persuasion (Revised ed.). New York, NY: Harper Business.
[4] Had Nagy, C., & Fincher, M. (2015). Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails. Indianapolis, IN: Wiley.
[5] Schneier, B. (2000). Secrets and Lies: Digital Security in a Networked World. Indianapolis, IN: Wiley.
[6] Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.). Indianapolis, IN: Wiley.
[7] Cialdini, R. B. (1984). Influence: How and Why People Agree to Things. New York, NY: William Morrow.
[8] 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
[9] Pew Research Center. (2022). Teens, social media and technology. Retrieved from https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/
[10] FBI Internet Crime Complaint Center. (2023). Internet Crime Report 2022. Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
[11] Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2015). The design of phishing studies: Challenges for researchers. Computers & Security, 52, 194–206. https://doi.org/10.1016/j.cose.2015.02.008
[12] 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
[13] Bakhshi, T., Papadaki, M., & Furnell, S. (2009). Social engineering: Assessing vulnerabilities in practice. Information Security Technical Report, 14(2), 100–108. https://doi.org/10.1016/j.istr.2009.10.006

[14] Heartfield, R., & Loukas, G. (2015). A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. ACM Computing Surveys, 48(3), 1–39. https://doi.org/10.1145/2835375
[15] Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Calic, D. (2015). Factors that influence information security behavior. Information and Computer Security, 23(2), 138–151. https://doi.org/10.1108/ICS-12-2013-0094
[16] Bullée, J.-W., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: Reducing the success of social engineering attacks. Journal of Experimental Criminology, 11(1), 97–115. https://doi.org/10.1007/s11292-014-9222-7
[17] Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. Communications of the ACM, 50(10), 94–100. https://doi.org/10.1145/1290958.1290968
[18] Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. Decision Support Systems, 51(3), 576–586. https://doi.org/10.1016/j.dss.2011.02.009
[19] Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. Computers in Human Behavior, 72, 412–421. https://doi.org/10.1016/j.chb.2017.03.002
[20] Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. Future Internet, 11(3), 73. https://doi.org/10.3390/fi11030073
[21] Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. Information Systems Security, 16(6), 315–331. https://doi.org/10.1080/10658980701788165
[22] Frauenstein, E. D., & Flowerday, S. V. (2020). Susceptibility to phishing on social network sites: A personality information processing model. Computers & Security, 94, 101862. https://doi.org/10.1016/j.cose.2020.101862
[23] Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. (2014). Research note—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
[24] Bullee, J. W., Montoya, L., Junger, M., & Hartel, P. (2016). Telephone-based social engineering attacks: An experiment testing the success and time-efficiency of two attacks. In Proceedings of the Singapore Cyber-Security Conference (SG-CRC 2016), 41–50. https://doi.org/10.3233/978-1-61499-617-0-41
[25] Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. Computers & Security, 59, 186–209. https://doi.org/10.1016/j.cose.2016.03.004
[26] Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. Computers & Security, 73, 102–113. https://doi.org/10.1016/j.cose.2017.10.008
[27] Conerly, M. D., Allen, L. E., & Coleman, S. (2018). High school students' knowledge of cybersecurity: Survey results. Journal of Cybersecurity Education, Research and Practice, 2018(1), Article 4.
[28] Tschakert, K. F., & Watkins, J. (2017). Cybersecurity education for youth: Bridging the gap between formal and informal learning. Journal of Information Technology Education: Innovations in Practice, 16, 249–263. https://doi.org/10.28945/3899
[29] Pham, H., & Nguyen, T. (2016). Social engineering attacks and countermeasures: A survey. International Journal of Computer Science Issues, 13(5), 85–95.
[30] Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Future Internet, 11(4), 89. https://doi.org/10.3390/fi11040089
[31] Heartfield, R., Loukas, G., & Gan, D. (2016). You are probably not the weakest link: Towards practical prediction of susceptibility to semantic social engineering attacks. IEEE Access, 4, 6910–6928. https://doi.org/10.1109/ACCESS.2016.2616285
[32] FBI Internet Crime Complaint Center. (2022). Elder Fraud Report 2021. Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3ElderFraudReport.pdf
[33] Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. Communication Research, 45(8), 1146–1166. https://doi.org/10.1177/0093650215627483
[34] Dodge, R. C., Jr., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. Computers & Security, 26(1), 73–80. https://doi.org/10.1016/j.cose.2006.10.009
[35] Ivaturi, K., & Janczewski, L. (2011). A taxonomy for social engineering attacks. In Proceedings of the International Conference on Information Resources Management (CONF-IRM 2011).
[36] Luo, X., Zhang, W., Burd, S., & Seazzu, A. (2013). Investigating phishing victimization with the heuristic-systematic model: A theoretical framework and an exploration. Computers & Security, 38, 28–38. https://doi.org/10.1016/j.cose.2012.12.003
[37] Algarni, A., Xu, Y., & Chan, T. (2017). An empirical study on the susceptibility of users to socially engineered email phishing attacks. In Proceedings of the 21st Pacific Asia Conference on Information Systems (PACIS 2017).
[38] Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. European Journal of Information Systems, 24(1), 38–58. https://doi.org/10.1057/ejis.2013.7
[39] Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. International Journal of Cyber Criminology, 5(1), 773–793.
[40] Vishwanath, A. (2015). Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack. Journal of Computer-Mediated Communication, 20(5), 570–584. https://doi.org/10.1111/jcc4.12126
[41] Pontell, H. N., & Geis, G. (2007). International Handbook of White-Collar and Corporate Crime. New York, NY: Springer.
[42] Gragg, D. (2002). A multi-level defense against social engineering. SANS Institute.
[43] National Institute of Standards and Technology (NIST). (2020). Special Publication 800-61r2: Computer Security Incident Handling Guide.
[44] International Telecommunication Union (ITU). (2021). Global Cybersecurity Index 2020.
[45] ENISA (European Union Agency for Cybersecurity). (2021). ENISA Threat Landscape 2021.
[46] Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. Computers & Security, 31(8), 983–988. https://doi.org/10.1016/j.cose.2012.08.004
[47] National Cyber Security Alliance. (2021). Stop. Think. Connect. Campaign resources.
[48] U.S. Department of Homeland Security / CISA. (2021). Cybersecurity awareness resources.
[49] Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. California Law Review, 107(6), 1753–1820. https://doi.org/10.15779/Z38RV0D15J
[50] Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. European Journal of Information Systems, 29(3), 306–321. https://doi.org/10.1080/0960085X.2020.1771222