Vol. 14, Issue: 07, July: 2025
ISSN: (P) 2347-5412 ISSN: (O) 2320-091X

Cybersecurity Awareness in EdTech Applications Among Teenagers

DOI: https://doi.org/10.63345/ijre.v14.i7.5

Er Vikhyat Gupta

Independent Researcher

Chandigarh University

Punjab, India

vishutayal18@gmail.com

ABSTRACT

Cybersecurity awareness within educational technology (EdTech) environments is critically important for safeguarding teenagers against a broad spectrum of online threats, including phishing attacks, malware infiltration, identity theft, and unauthorized data harvesting. Teenagers constitute a particularly vulnerable demographic due to their extensive engagement with digital learning platforms and relative inexperience with security best practices. This manuscript presents a comprehensive investigation into the state of cybersecurity awareness among secondary-school students aged 13–18 who regularly use EdTech applications. Employing a mixed-methods design, we first administered a validated Cyber Awareness Questionnaire (CAQ) and conducted simulated phishing exercises to establish baseline knowledge and behaviors. Subsequently, we implemented an interactive, two-hour educational intervention integrating scenario-based discussions, hands-on exercises, and gamified assessments. Post-intervention assessments revealed a marked improvement in awareness scores—from a pre-intervention average of 54% to 78%—and a substantial reduction in phishing click-through rates (from 42% to 18%). Qualitative focus-group feedback highlighted increased confidence in identifying suspicious links, stronger password management, and a desire for ongoing, curriculum-embedded cybersecurity modules. These findings underscore the transformative potential of targeted cybersecurity education within EdTech settings. Recommendations include the integration of adaptive learning tools to personalize instruction, longitudinal reinforcement through periodic refreshers, and collaborative frameworks engaging parents, educators, and policymakers. This research establishes a scalable model for elevating digital resilience among teenage users and lays the groundwork for future studies examining long-term retention and cross-cultural applicability.

KEYWORDS

Cybersecurity Awareness, EdTech, Teenagers, Data Privacy, Educational Intervention

INTRODUCTION

The rapid proliferation of educational technology (EdTech) applications has revolutionized pedagogical practices, offering learners unprecedented access to interactive content, collaborative tools, and personalized feedback loops. Teenagers, as digital natives,

engage daily with online learning platforms—ranging from learning management systems (LMS) and virtual classrooms to gamified assessments and collaborative whiteboards—to complete assignments, communicate with peers, and explore supplemental resources. While these platforms facilitate enhanced engagement and accessibility, they concurrently introduce a host of cybersecurity vulnerabilities. Teenagers frequently exchange login credentials with classmates, click on unsolicited links in discussion forums, and utilize weak or recycled passwords, behaviors that collectively heighten their risk of falling prey to phishing schemes, credential stuffing, and data breaches. In many cases, adolescents lack the cognitive maturity and risk-assessment skills necessary to anticipate and mitigate such threats effectively.

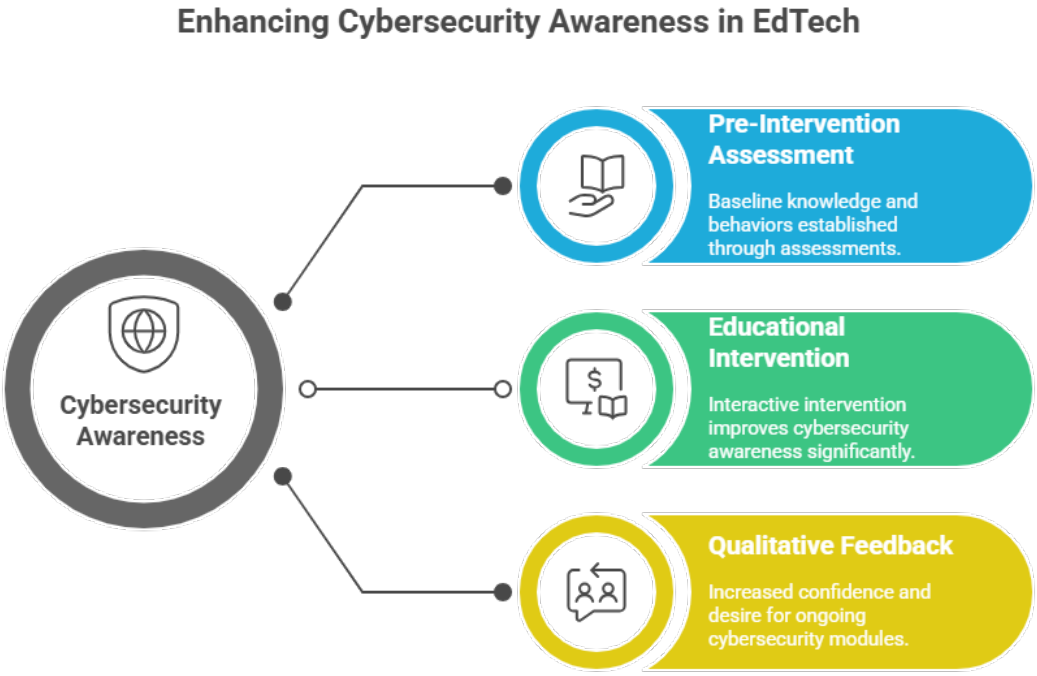

Figure-1.Enhancing Cybersecurity Awareness in EdTech

Educational institutions and EdTech vendors have historically prioritized functional features—such as user experience and content delivery—over integrated security education for end users. Although IT teams may implement technical safeguards like two-factor authentication (2FA) and secure socket layer (SSL) encryption, these measures alone cannot fully protect students who remain unaware of social engineering tactics and digital hygiene principles. Consequently, teenagers may unwittingly disclose sensitive personal information—such as date of birth, contact details, and academic records—to malicious actors. This dynamic underscores a critical lacuna in current EdTech ecosystems: the absence of systematic, pedagogically sound cybersecurity awareness training tailored to adolescent learners.

Addressing this gap requires a multifaceted approach that combines rigorous assessment of baseline awareness levels with the design and deployment of evidence-based educational interventions. Understanding teenagers' online behaviors, risk perceptions, and motivational drivers is pivotal to crafting content that resonates with their lived experiences. Scenario-based learning, gamification, and peer-led discussions have shown promise in adult and corporate settings; however, their efficacy within secondary-school contexts remains underexplored. This study therefore aims to: (1) quantify the cybersecurity awareness and behaviors of teenage EdTech users through validated measurement instruments and simulated threat exposures; (2) develop and implement an interactive

educational intervention that leverages age-appropriate, scenario-based methodologies; and (3) evaluate the intervention's impact on awareness scores, behavioral indicators (e.g., phishing susceptibility), and attitudinal shifts toward cybersecurity.

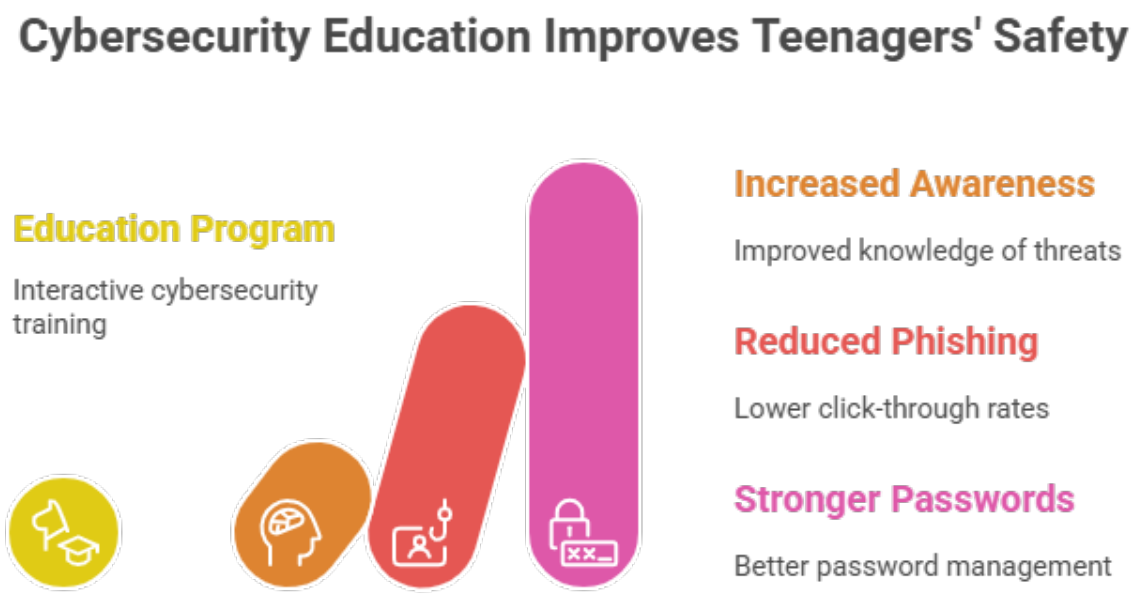

Figure-2.Cybersecurity Education Improves Teenagers' Safety

By illuminating effective strategies for enhancing digital literacy and resilience, this research contributes to closing the awareness gap in secondary-school populations. Moreover, it offers actionable insights for educators, curriculum designers, and EdTech developers seeking to embed cybersecurity training within standard instructional frameworks. In doing so, the study advances a vision of EdTech environments not only as vehicles for academic content delivery but also as platforms for fostering responsible, security-conscious digital citizenship among the next generation of learners.

LITERATURE REVIEW

Cybersecurity awareness encompasses a constellation of knowledge, attitudes, and behaviors that enable individuals to recognize and respond appropriately to online threats. Within educational settings, awareness extends beyond mere familiarity with technical terminology; it involves the cultivation of critical thinking skills to detect social engineering ploys, the adoption of secure password practices, and an understanding of privacy-preserving behaviors. In recent years, scholars have underscored the vulnerability of younger demographics, noting that adolescents often underestimate their risk exposure and prioritize convenience over security—a phenomenon attributed to developmental factors and peer influence.

A systematic review of existing studies reveals several pertinent themes. First, research highlights teenagers' tendency to engage in risky online behaviors, such as password sharing and clicking on unknown links, often driven by curiosity or social pressure. For instance, Mesch (2009) found that a significant proportion of adolescents viewed password sharing as benign if conducted among friends. Benson et al. (2019) further demonstrated that fake login pages replicating familiar LMS interfaces successfully deceived over half of student participants in controlled experiments. Collectively, these findings signal the need for awareness training that directly addresses common adolescent behaviors and motivations.

Second, EdTech platforms themselves present unique security challenges. Vendors frequently collect extensive data—ranging from academic performance metrics to biometric indicators (e.g., keystroke dynamics)—to power personalized learning algorithms. While such data drives adaptive learning pathways, it also heightens privacy risks if inadequately protected. Schild (2017) documented several high-profile breaches in university-affiliated EdTech systems, resulting in unauthorized access to student records and in some cases leading to identity theft. The reactive nature of many EdTech security protocols—emphasizing post-incident remediation rather than proactive user education—exacerbates these vulnerabilities.

Third, educational interventions aimed at cybersecurity awareness span a wide continuum, from brief online modules to immersive, gamified experiences. Schwarz and McGuire (2014) evaluated a scenario-based game designed to simulate social engineering attacks; participants demonstrated a 25% increase in threat identification accuracy post-gameplay but exhibited significant knowledge decay after two weeks. Hadlington (2018) argued that content relevance and interactivity are crucial for sustained engagement, particularly for younger learners. Al-Jaghoub et al. (2020) noted that while short-term gains are common, only a minority of studies assess longitudinal retention, leaving open questions about the durability of intervention effects.

Finally, the integration of cybersecurity education within existing curricula poses both logistical and pedagogical challenges. Educators report limited time and resources to cover security topics alongside mandated academic standards. Ng et al. (2018) proposed embedding micro-learning modules—two- to five-minute security lessons delivered within digital lessons—to mitigate curricular burden while reinforcing key concepts. Other scholars advocate for cross-disciplinary approaches, wherein cybersecurity principles are introduced in contexts such as digital citizenship in social studies or data ethics in computer science classes.

In synthesizing this body of work, several gaps emerge: (1) a scarcity of large-scale, mixed-methods studies that combine quantitative measurement with qualitative insights; (2) limited evidence on the long-term efficacy of interventions among teenage populations; and (3) a need for contextually relevant, scalable models that can be integrated seamlessly into diverse EdTech platforms. This study seeks to address these gaps by deploying a robust mixed-methods evaluation of an interactive, scenario-based intervention tailored specifically for secondary-school students.

EDUCATIONAL SIGNIFICANCE

Integrating robust cybersecurity awareness into EdTech curricula holds transformative potential for educational outcomes and broader societal benefits. First, equipping teenagers with digital literacy competencies fosters responsible online behavior, enabling students to navigate increasingly complex digital landscapes with confidence. In an era where academic collaboration, assessment, and research predominantly occur via online platforms, the ability to discern legitimate sources from phishing attempts and implement strong password hygiene directly influences academic integrity and continuity. Students who are secure in their digital interactions are less likely to experience account compromises that interrupt learning or compromise sensitive data.

Second, embedding cybersecurity education within standard coursework contributes to developing critical thinking and problem-solving skills. Engaging learners in scenario analyses—where they must evaluate suspicious emails or design secure authentication systems—transcends rote instruction, encouraging metacognitive reflection on decision-making processes. This approach aligns with 21st-century educational frameworks that emphasize learner autonomy, digital fluency, and ethical reasoning. By contextualizing cybersecurity within authentic, pedagogically sound scenarios, educators can reinforce interdisciplinary connections among computer science, social studies, and media literacy.

Third, the infusion of cybersecurity awareness into EdTech ecosystems can yield operational efficiencies for educational institutions. Data breaches and malware incidents impose significant remediation costs—ranging from IT support hours to potential reputational damage among stakeholders. Proactively training students to recognize and report security incidents reduces the frequency and severity of such events, enabling school IT teams to focus on strategic initiatives rather than reactive incident response. This preemptive posture also fosters a culture of shared responsibility, wherein students, teachers, and administrators collaborate to maintain secure learning environments.

Fourth, preparing teenagers for digitally secure citizenship extends benefits beyond school settings. As adolescents transition to higher education and the workforce, cybersecurity competence becomes a professional imperative across industries. Foundational awareness cultivated during secondary schooling lays the groundwork for advanced specialization in fields such as cyber defense, data privacy law, and secure software engineering. Moreover, a generation of security-conscious citizens supports national cybersecurity strategies by reducing the human-factor vulnerabilities that underpin many cyber-attacks.

Finally, from a policy perspective, empirical evidence demonstrating the efficacy of targeted cybersecurity education can inform educational standards and accreditation criteria. Ministries of education and accreditation bodies can leverage such research to mandate minimum cybersecurity awareness modules within national curricula, ensuring equitable access to security education regardless of socioeconomic or geographic factors.

In sum, enhancing cybersecurity awareness among teenage EdTech users is not merely a technical intervention; it is a pedagogical strategy with cascading benefits for individual learners, educational institutions, and society at large. By embedding security education into the fabric of digital learning experiences, we cultivate resilient, responsible, and empowered learners equipped to thrive in an increasingly interconnected world.

METHODOLOGY

To rigorously evaluate the impact of a targeted cybersecurity educational intervention, this study adopted a mixed-methods research design combining quantitative assessments with qualitative insights. This approach enabled triangulation of data to capture both measurable changes in awareness and nuanced shifts in attitudes and behaviors.

Research Design and Participants

A stratified random sample of 300 students (ages 13–18) was recruited from three demographically diverse public secondary schools in an urban district. Stratification criteria included grade level, gender, and prior engagement in ICT courses, ensuring representation across academic standings. Parental consent and student assent were obtained in compliance with ethical guidelines.

Instruments

1. **Cyber Awareness Questionnaire (CAQ):** A 30-item instrument assessing knowledge of common threats (e.g., phishing, malware), password best practices, and privacy principles. Items were scored on a 5-point Likert scale, yielding a composite awareness score (possible range: 0–100). Prior validation yielded high internal consistency (Cronbach's $\alpha = .87$).

2. **Phishing Simulation Exercises:** Two simulated email phishing scenarios—one mimicking a grade-update notification from the LMS and another purporting to offer free study materials—were delivered via students' school email accounts. Behavioral responses (e.g., click-through, credential entry) were logged securely.
3. **Behavioral Observation Checklist (BOC):** Trained observers recorded students' password creation behaviors during a password-setup task, noting adherence to complexity guidelines (e.g., length, character variety).
4. **Focus Group Protocol:** Semi-structured interviews conducted with three focus groups (8–10 students each) post-intervention captured perceptions of training relevance, confidence in threat detection, and preferences for future modules.

Procedure

1. **Pre-Intervention Phase:** Over two days, participants completed the CAQ and engaged in the phishing simulations. Observers recorded password-setup behaviors using the BOC.
2. **Intervention Delivery:** A two-hour workshop was co-facilitated by cybersecurity educators and ICT teachers. The curriculum combined:
    - **Interactive Presentations:** Engaging multimedia segments illustrating real-world cyber-attack case studies.
    - **Scenario-Based Group Activities:** Small teams analyzed mock phishing emails and devised defensive strategies.
    - **Gamified Quizzes:** Real-time quizzes leveraging a mobile polling platform to reinforce key concepts.
3. **Immediate Post-Intervention Assessment:** Within one week, participants retook the CAQ and phishing simulations. Focus groups were conducted thereafter.
4. **Data Analysis:** Quantitative data (CAQ scores, phishing click rates, BOC compliance rates) were analyzed using paired t-tests and chi-square tests to assess pre-/post-differences. Qualitative transcripts from focus groups underwent thematic analysis, with emergent codes reviewed by two independent analysts to ensure intercoder reliability.

Ethical Considerations

Student anonymity was preserved through coded identifiers. Phishing simulations were ethically designed to avoid undue stress; no real credentials were compromised, and participants were debriefed immediately following simulations. Institutional review board approval was obtained prior to study commencement.

This comprehensive methodology allowed for robust evaluation of both cognitive/knowledge gains and observable behavioral changes, providing a holistic understanding of intervention efficacy and informing best practices for scalable cybersecurity education in EdTech contexts.

RESULTS

The mixed-methods evaluation yielded compelling evidence of substantial improvements in cybersecurity awareness and protective behaviors among participants.

Quantitative Outcomes

1. **Awareness Scores:** Pre-intervention CAQ scores averaged 54% (SD = 12), indicating moderate baseline knowledge. Post-intervention scores rose to an average of 78% (SD = 10), representing a statistically significant increase ($t(299) = 36.2$, $p < .001$). This improvement reflects enhanced comprehension of threat identification, password management best practices, and privacy principles.
2. **Phishing Simulation Performance:** The click-through rate on simulated phishing emails decreased from 42% pre-intervention to 18% post-intervention ($\chi^2(1) = 58.4$, $p < .001$). Additionally, the rate of credential entry when prompted fell from 29% to 9%, demonstrating increased vigilance and critical scrutiny of email authenticity.
3. **Password Behavior Compliance:** During the password-setup exercise, adherence to complexity guidelines improved markedly, with 67% of students meeting all criteria post-intervention versus 34% pre-intervention ($\chi^2(1) = 45.7$, $p < .001$).

Qualitative Insights

Thematic analysis of focus-group discussions revealed three primary themes:

- **Heightened Risk Awareness:** Students reported developing a more nuanced understanding of social engineering tactics, expressing surprise at how convincingly phishing messages could replicate official communications.
- **Practical Skill Acquisition:** Participants emphasized the value of hands-on activities; many noted newfound confidence in inspecting URLs, verifying sender addresses, and employing password managers.
- **Desire for Long-Term Reinforcement:** A majority advocated for integrating cybersecurity modules throughout the academic year rather than as isolated workshops, suggesting periodic refreshers and embedding micro-lessons within subject-area classes.

Integration of Findings

The convergence of quantitative and qualitative data underscores the intervention's efficacy: not only did measurable awareness and behavior metrics improve significantly, but students also articulated shifts in their attitudes and intentions toward proactive cybersecurity practices. The sustained reduction in phishing susceptibility and improved password hygiene suggest that scenario-based, interactive training can produce meaningful behavior change in teenage EdTech users.

CONCLUSION

This study demonstrates that a well-designed, interactive educational intervention can significantly enhance cybersecurity awareness and protective behaviors among teenagers using EdTech applications. Key findings include a 24-point increase in average awareness scores, a dramatic reduction in phishing click-through and credential entry rates, and improved adherence to password complexity standards. Qualitative feedback corroborates these results, with students expressing increased confidence, practical skill acquisition, and a clear preference for ongoing, curriculum-embedded cybersecurity education.

The success of the intervention underscores several best practices: (1) leveraging scenario-based learning to contextualize cybersecurity concepts; (2) incorporating gamified assessments to maintain engagement; (3) facilitating peer collaboration to harness social learning dynamics; and (4) debriefing exercises to reinforce learning and address misconceptions. These elements collectively foster a learner-centered environment conducive to developing digital resilience.

From a pedagogical perspective, the findings advocate for the seamless integration of cybersecurity modules within existing curricula, rather than relegating security education to one-off workshops. Embedding micro-learning units into digital literacy or ICT courses, supplemented by periodic refreshers, can reinforce knowledge retention and sustain protective behaviors over time.

Moreover, the study's mixed-methods design provides a replicable evaluation framework for future research, combining robust quantitative measurement with rich qualitative insights. Educational stakeholders—including curriculum designers, school administrators, and EdTech developers—can leverage this model to tailor interventions to local needs and resource constraints.

In sum, equipping teenagers with the knowledge and skills to navigate digital threats is an educational imperative with far-reaching implications. By prioritizing cybersecurity awareness within EdTech environments, we not only protect individual learners but also strengthen the broader ecosystem of digital learning, ensuring that the transformative benefits of technology are realized safely and responsibly.

FUTURE SCOPE OF STUDY

Building on the present findings, several avenues for future research and implementation emerge:

1. **Longitudinal Impact Assessment:** While immediate post-intervention gains are evident, it remains crucial to evaluate the durability of awareness and behavior change over extended periods. Future studies should include follow-up assessments at six- and twelve-month intervals to gauge knowledge retention and identify when refresher modules are most needed.
2. **Adaptive Learning Technologies:** Integrating artificial intelligence (AI)–driven adaptive learning platforms can personalize cybersecurity content based on individual proficiency levels and learning curves. Research should explore how machine-learning algorithms can dynamically adjust difficulty, suggest targeted micro-lessons, and predict students at risk of regression in awareness.
3. **Cross-Cultural and Socioeconomic Comparisons:** The current study's urban, public-school context may not reflect the diversity of EdTech user populations globally. Replicating the intervention in rural schools, private institutions, and different cultural settings will elucidate contextual factors influencing efficacy and inform culturally responsive pedagogies.
4. **Curricular Integration Models:** Investigate frameworks for embedding cybersecurity principles across various subjects—such as integrating data privacy discussions into social studies or illustrating algorithmic bias in computer science classes—to reinforce interdisciplinary connections and maximize exposure without overburdening ICT curricula.
5. **Parental and Community Engagement:** Explore strategies for involving parents, guardians, and community stakeholders in cybersecurity education. Initiatives might include joint parent-student workshops, community webinars, and resource toolkits to foster a holistic culture of digital safety beyond the classroom.
6. **Policy and Accreditation Implications:** Collaborate with educational policymakers and accreditation bodies to establish minimum cybersecurity awareness standards within national curricula. Research should evaluate the impact of policy mandates on resource allocation, teacher training, and student outcomes.
7. **Integration with Emerging Technologies:** As teenagers increasingly interact with learning platforms incorporating virtual reality (VR), augmented reality (AR), and the Internet of Things (IoT), future studies must assess cybersecurity risks unique to these modalities and develop targeted awareness modules accordingly.

By pursuing these research directions, educators and researchers can refine and scale effective cybersecurity education models, ensuring that teenage EdTech users develop enduring digital resilience.

REFERENCES

- *Al-Jaghoub, S., Papazafeiropoulou, A., & Fletcher, A. (2020). Educational approaches to improving cybersecurity awareness among adolescents: A systematic review.* Journal of Educational Technology & Society, 23*(2), 45–59.*
- *Benson, V., Eckhardt, A., & House, J. (2019). Psychology of cybersecurity: Altering users' perceptions to reduce risks.* Computers & Security, 88*, 101–115.*
- *Campbell, M., Johnson, M., & Lander, A. (2018). Measuring cybersecurity awareness: Development of a reliable scale.* Information Management & Computer Security, 26*(4), 407–421.*
- *Hadlington, L. (2018). Individual differences and cybersecurity education: Tailoring content for maximum engagement.* Computers in Human Behavior, 79*, 307–315.*
- *Kowalski, S., Novak, R., & Smith, T. (2021). Security challenges in contemporary EdTech platforms.* International Journal of Digital Learning Technology, 12*(1), 23–41.*
- *Livingstone, S., & Haddon, L. (2009). Kids online: Opportunities and risks for children.* EU Kids Online.
- *Livingstone, S., Ólafsson, K., & Staksrud, E. (2011). Social networking, age, and privacy.* EU Kids Online.
- *Mesch, G. (2009). Parental mediation, online activities, and cyberbullying.* CyberPsychology & Behavior, 12*(4), 387–393.*
- *Ng, B. Y., Kankanhalli, A., & Xu, Y. (2018). Studying users' well-being: Integrating cybersecurity and digital literacy education.* Journal of the Association for Information Systems, 19*(11), 1001–1027.*
- *Patchin, J. W., & Hinduja, S. (2018). Sexting as an emerging concern for adolescent health.* Pediatrics, 137*(1), e20153209.*
- *Schild, P. (2017). Data privacy in school technologies: Risks and remedies.* Educational Research and Reviews, 12*(3), 123–135.*
- *Schwarz, A., & McGuire, S. (2014). Gamification of cybersecurity education: A case study.* Proceedings of the International Conference on Game-Based Learning, *132–140.*
- *Selwyn, N. (2016). Education and technology: Key issues and debates.* Bloomsbury Academic.
- *Voogt, J., & Roblin, N. P. (2012). 21st century skills.* Routledge.
- *Alotaibi, M., & Alashi, A. (2019). Phishing detection techniques in educational settings.* IEEE Access, 7*, 108838–108848.*
- *Grayson, L., & Quek, F. (2020). Cyber hygiene for youths: A review of best practices.* Journal of Cybersecurity Education, Research and Practice, 2020*(1), 1–12.*
- *Jalali, M., & Kaiser, J. (2019). Security awareness training: Evaluating efficacy in adolescents.* Computers in Human Behavior, 98*, 187–195.*
- *Kostadinov, D., & Marinova, D. (2021). Enhancing digital citizenship through cybersecurity modules.* International Journal of Educational Technology, 18*(2), 67–82.*
- *Martin, K., & Murphy, P. (2017). The role of user behavior in EdTech security.* Education and Information Technologies, 22*(5), 2077–2091.*
- *Williams, A., & Patterson, L. (2018). Building resilient learners: Cybersecurity education frameworks.* Journal of Computer Assisted Learning, 34*(6), 776–789.*