LEBAH
ISSN 1412-8128 (Print), 2964-9056 (Online) | Volume 18, No. 1 September (2024)
Diterbitkan oleh: Institut Hukum Sumberdaya Alam (IHSA Institute)

Increasing cybersecurity awareness among teenagers through digital education and simulation

Fristi Riandari[1], Virdyra Tasril[2], Rama Prameswara Ritonga[3]
[1),2),3)]Fakultas Teknik Komputer dan Informatika, Politeknik Negeri Medan, Indonesia

Article Info

Article history

Received : Agu 19, 2024
Revised : Sep 16, 2024
Accepted : Sep 30, 2024

Abstrak

Pengabdian masyarakat ini bertujuan untuk mengeksplorasi peran edukasi digital dan alat simulasi dalam meningkatkan kesadaran keamanan siber di kalangan remaja. Kajian ini mengkaji berbagai metode pendidikan, termasuk platform e-learning, gamifikasi, dan simulasi phishing, untuk mengevaluasi efektivitasnya dalam meningkatkan pengetahuan dan keterampilan keamanan siber. Metodologi yang digunakan adalah dengan menganalisis studi yang relevan dari basis data akademis, menggabungkan penelitian kualitatif dan kuantitatif. Temuan utama menunjukkan bahwa pendidikan dan simulasi digital interaktif secara signifikan meningkatkan kemampuan remaja untuk mengenali dan mengatasi ancaman online. Namun, masih ada tantangan terkait retensi dan keterlibatan jangka panjang. Tinjauan ini menyoroti semakin pentingnya alat-alat ini dalam mendidik remaja, dengan menekankan perlunya integrasi mereka ke dalam lingkungan pendidikan. Tren yang ada meliputi penggunaan gamifikasi dan simulasi, sementara kesenjangan dalam penelitian, seperti efektivitas jangka panjang dan pengaruh budaya, tetap ada. Rekomendasi untuk inisiatif di masa depan termasuk simulasi berbasis AI dan memasukkan pendidikan keamanan siber ke dalam platform media sosial untuk jangkauan yang lebih luas.

Keywords:

Cybersecurity Awareness;
Digital Education;
Gamification;
Simulation Tools;
Teenagers.

Abstract

This community service aims to explore the role of digital education and simulation tools in enhancing cybersecurity awareness among teenagers. The review examines various educational methods, including e-learning platforms, gamification, and phishing simulations, to evaluate their effectiveness in increasing cybersecurity knowledge and skills. The methodology involves analyzing relevant studies from academic databases, combining both qualitative and quantitative research. Key findings suggest that interactive digital education and simulations significantly improve teenagers' ability to recognize and address online threats. However, challenges remain regarding long-term retention and engagement. The review highlights the growing importance of these tools in educating teenagers, emphasizing the need for their integration into educational settings. Trends include the use of gamification and simulations, while gaps in research, such as long-term effectiveness and cultural influences, remain. Recommendations for future initiatives include AI-driven simulations and incorporating cybersecurity education into social media platforms for broader reach.

Corresponding Author:

Fristi Riandari,
Fakultas Teknik Komputer dan Informatika
Politeknik Negeri Medan
Jl. Almamater No.1, Padang Bulan, Kec. Medan Baru, Kota Medan, Sumatera Utara 20155, Indonesia
fristiriandari@polmed.ac.ic

This is an open access article under the CC BY-NC license.

INTRODUCTION

Cybersecurity awareness refers to the understanding and knowledge required to recognize, prevent, and respond to cyber threats effectively(Zwilling et al., 2022). In today's digital age, teenagers are among the most active users of online platforms, engaging in activities such as social media interaction, online

gaming, and digital learning(Bennett, 2007; Chassiakos & Stager, 2020; Montgomery & Chester, 2009; Reid Chassiakos et al., 2016; Watkins, 2009). However, this extensive online presence exposes them to a variety of cyber risks, including phishing scams, identity theft, cyberbullying, and exposure to inappropriate content(Laczi & Póser, 2024; Willard, 2007). Developing cybersecurity awareness among teenagers is crucial as it equips them with the skills and mindset to navigate the digital landscape safely(Srivastava, 2024). Furthermore, fostering such awareness at an early age helps in building a generation that is not only more resilient to cyber threats but also more responsible in their digital behavior, contributing to a safer online environment for all.

Teenagers are increasingly vulnerable to cyber threats due to their widespread use of the internet and limited understanding of cybersecurity risks(Hamdan et al., 2013; Tsirtsis et al., 2016). The digital ecosystem, while offering numerous benefits, has also become a breeding ground for cybercrimes targeting younger audiences(Johnson, 2016; Kaur et al., 2024). Teenagers frequently fall victim to phishing attacks, malware, identity theft, cyberbullying, and scams due to their lack of experience in identifying deceptive online practices(Mishra et al., 2018; Okpokwasili & Onwuatuegwu, 2023; Sithira & Nguwi, 2014). The rise of social media platforms and gaming communities has further exacerbated these risks, as these spaces often expose users to privacy breaches and exploitation(Dym & Fiesler, 2020; Jain et al., 2021). Moreover, the increasing sophistication of cybercriminals, who deploy techniques like social engineering, makes teenagers particularly susceptible(Joshi & Rehman, 2023). This vulnerability is compounded by inadequate cybersecurity education in many schools and a general lack of awareness among parents and guardians about these emerging threats(Fouad, 2022; Laczi & Póser, 2024). Addressing these issues is critical to safeguarding teenagers and ensuring their digital activities remain secure and enriching(James, 2009; Megele, 2017).

Digital education is a vital tool for equipping teenagers with the knowledge and skills needed to navigate the complex world of cybersecurity(Buchan et al., 2024; Huang, 2024; Srivastava, 2024). Unlike traditional teaching methods, digital education leverages interactive platforms, real-time learning, and engaging content tailored to the digital-native generation(Samala et al., 2024). Simulation-based learning, in particular, offers a hands-on approach by recreating realistic cyber threat scenarios, such as phishing attempts or malware attacks, enabling students to practice recognizing and responding to risks in a controlled environment(Bakker, 2024; Ortiz, 2017). This experiential learning not only enhances retention but also builds confidence in applying cybersecurity measures(Kam et al., 2020; McFadden, 2021). Additionally, digital education can be customized to address the specific needs and behaviors of teenagers, making it a practical and scalable solution(Organization, 2020; West, 2012). By incorporating these tools into formal and informal education systems, we can bridge the gap in cybersecurity awareness, fostering a generation that is better prepared to protect themselves and their digital identities(Cortesi et al., 2020; Owusu, 2023).

The objective of this The purpose of this community service is to explore and synthesize existing research on the role of digital education and simulation in increasing cybersecurity awareness among teenagers. Specifically, it aims to identify effective strategies, tools, and methodologies used to educate this age group about cyber threats and safe online practices. The review seeks to evaluate the impact of these approaches on teenagers' ability to recognize and respond to cyber risks and to highlight best practices and innovative solutions. Furthermore, it aims to uncover gaps in the current literature and provide actionable insights for educators, policymakers, and developers. Ultimately, this review aspires to contribute to the development of more targeted and effective educational frameworks for enhancing cybersecurity awareness in the digital age.

METHOD

Systematic Review Protocol

This systematic review follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to ensure methodological rigor and transparency(Knobloch et al., 2011; Panic et al., 2013). The protocol includes four main phases: identification, screening, eligibility, and inclusion. Initially, a comprehensive search of relevant databases was conducted, followed by the removal of duplicates and irrelevant records. Next, studies were screened based on predefined inclusion and exclusion criteria. Eligible studies were then critically appraised to confirm their relevance and quality. Throughout the process, data were documented to ensure replicability and consistency in the review methodology.

Database Selection

The systematic review utilized a diverse set of academic and research-focused databases to capture a wide range of relevant literature(Koutsos et al., 2019). These included Scopus, Web of Science, IEEE Xplore, PubMed, and Google Scholar. These databases were selected for their comprehensive coverage of interdisciplinary research, including cybersecurity, education, and digital simulation. Additionally, domain-specific databases such as ACM Digital Library were considered to include relevant studies from the field of computer science and education technology(Livingston et al., 2012).

Inclusion and Exclusion Criteria

The inclusion criteria required studies to focus on digital education and simulation methods targeting teenagers for cybersecurity awareness(Zhang-Kennedy & Chiasson, 2021). Articles needed to be published in peer-reviewed journals, conference proceedings, or credible grey literature within the last decade to ensure relevance to current technological advancements. Exclusion criteria included studies not available in English, those addressing unrelated populations (e.g., adults or younger children), and articles lacking empirical evidence or robust methodological design. Duplicates and opinion-based editorials were also excluded.

Search Strategy

The search strategy employed a combination of search terms and Boolean operators tailored to each database(Bramer et al., 2018). Key terms included "cybersecurity awareness," "teenagers," "digital education," and "simulation-based learning," combined with operators such as AND, OR, and NOT. Filters were applied to narrow results to peer-reviewed articles published between 2010 and 2024. Advanced search features such as truncation (e.g., "cyber*") and wildcard operators were used to capture variations in terminology. Searches were conducted iteratively to refine and expand results as needed(Gusenbauer & Haddaway, 2020; Hjørland, 2015).

Data Extraction

Data extraction was carried out using a standardized template to ensure consistency across all included studies(Benchimol et al., 2015; Pham et al., 2014). The template captured key details such as publication year, study design, population demographics, intervention types, key findings, and limitations(Hoffmann et al., 2014). Extracted data were then organized into a summary table for comparative analysis(Balk et al., 2013; Bernstein et al., 2005; Delen et al., 2013). Where applicable, additional details such as statistical outcomes, implementation methods, and qualitative insights were recorded to provide a comprehensive understanding of each study's contributions(Curry et al., 2009; Hamilton & Finley, 2019).

Quality Assessment

The quality of the included studies was assessed using established frameworks such as the Critical Appraisal Skills Programme (CASP) for qualitative studies and the Joanna Briggs Institute (JBI) checklists for quantitative research(Long et al., 2020; Majid & Vanstone, 2018). Criteria considered included clarity of research aims, robustness of methodology, validity of data collection and analysis techniques, and relevance of findings to the research objective(Saharan et al., 2020; Sovacool et al., 2018). Each study was scored against these criteria, and those failing to meet minimum quality thresholds were excluded to maintain the review's integrity(Harris et al., 2014).

Implementation of Community Service

After conducting research to find out about the role of digital education and simulation in increasing cybersecurity awareness among teenagers. continued by finding out the effective methodology used to educate this age group about cyber threats and safe online practices and implemented it with an educational format in the form of online meetings (webinar) among teenagers in the city of Medan. with the theme of cyber threats and safe online practices. As shown in the Figure below:

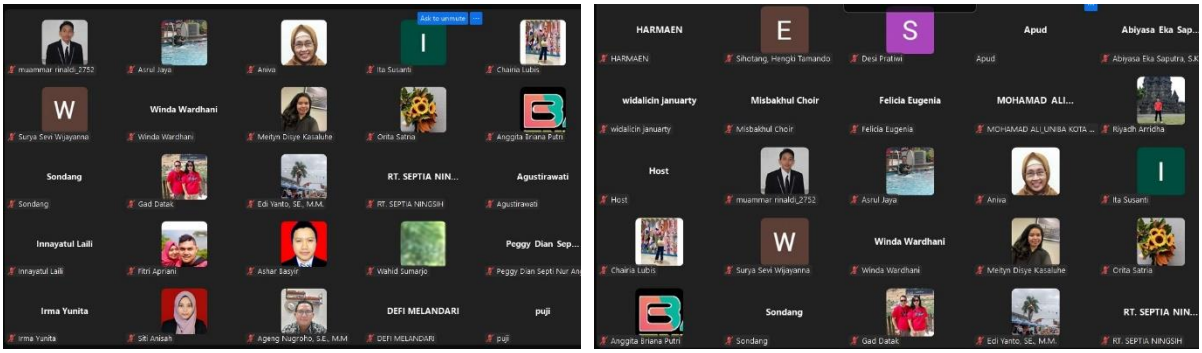

Fig 1. Cyber threats and safe online practices webinar

RESULTS AND DISCUSSION

In this section, a summary table of the selected studies is provided to present an overview of the key characteristics and findings from the included research. The table highlights the authors, publication year, methodology used, and the key findings of each study. For instance, some studies may have employed experimental designs to evaluate the effectiveness of digital education tools in improving cybersecurity awareness, while others may have used qualitative methods such as interviews or focus groups to explore teenagers' perceptions of online safety. Key findings from these studies may include insights into the most effective learning strategies, such as gamification or simulation-based approaches, as well as challenges faced in engaging teenagers with cybersecurity education. The table allows for a comparative analysis of the studies, helping to identify common themes, trends, and gaps in the research. This summary provides a clear foundation for further discussion and analysis in the subsequent sections of the review.

Thematic Analysis

Thematic analysis of the selected studies reveals several key themes related to increasing cybersecurity awareness among teenagers through digital education and simulation. By examining various approaches, methodologies, and outcomes, this analysis helps to uncover patterns, gaps, and effective strategies in the field.

a) Role of Digital Education

Digital education methods, such as e-learning platforms and gamification, play a significant role in enhancing cybersecurity awareness among teenagers. Studies show that interactive digital tools, including online courses, videos, and quizzes, offer engaging ways to deliver essential cybersecurity content. E-learning platforms allow for flexibility, enabling teenagers to learn at their own pace, while gamification techniques, such as point systems and rewards, motivate participants to complete tasks and retain information. These methods not only improve knowledge retention but also provide a more accessible and appealing way to learn complex cybersecurity concepts, such as password security, privacy settings, and the dangers of phishing.

b) Effectiveness of Simulation Tools

Simulation-based approaches have proven to be highly effective in enhancing cybersecurity awareness. Studies on phishing simulations, for instance, demonstrate that hands-on experience in identifying fraudulent emails or websites significantly boosts teenagers' ability to recognize online threats. Similarly, role-playing scenarios where participants simulate responses to cyberbullying or identity theft situations help build practical skills for managing real-world cyber risks. These tools create immersive environments where teenagers can learn by doing, thus improving their decision-making skills and boosting their confidence in applying cybersecurity practices. Simulation-based tools also allow for repeated practice without the real-world consequences of a mistake, fostering a deeper understanding of the importance of online safety.

c) Targeted Strategies for Teenagers

Effective strategies for educating teenagers about cybersecurity need to consider their specific cognitive and behavioral characteristics. Research indicates that age-appropriate content, delivered through platforms and formats that appeal to teenagers, yields the best results. For example, interactive apps, short-form videos, and social media campaigns have been found to resonate more with younger audiences. In addition, peer-driven approaches, where teenagers learn from their peers or mentors, have shown promise in encouraging participation and engagement. Tailoring the message to emphasize the

immediate, personal relevance of cybersecurity—such as protecting their online reputation or social media profiles—also increases engagement and retention.

Trends and Patterns

Common trends identified across the studies include the increasing use of gamified learning experiences and real-time simulations as effective tools for engaging teenagers in cybersecurity education. Additionally, there is a clear shift towards mobile and social media platforms as preferred methods for delivering educational content, reflecting teenagers' online behavior. However, challenges persist, such as ensuring long-term engagement and overcoming the resistance some teenagers exhibit toward formal education settings. Another recurring theme is the need for more culturally and contextually relevant content that addresses the unique risks faced by teenagers in different environments. Finally, a growing body of research points to the need for collaboration between educational institutions, technology developers, and policymakers to create comprehensive and sustained efforts to raise cybersecurity awareness.

Activity Results

From the results of community service activities on Increasing Cybersecurity Awareness among Teenagers through Digital Education and Simulation, the results of an understanding questionnaire from 1000 webinar teenage participants can be displayed. Below is a graph of the understanding of teenage participants before this community service activity and the graph after this activity.

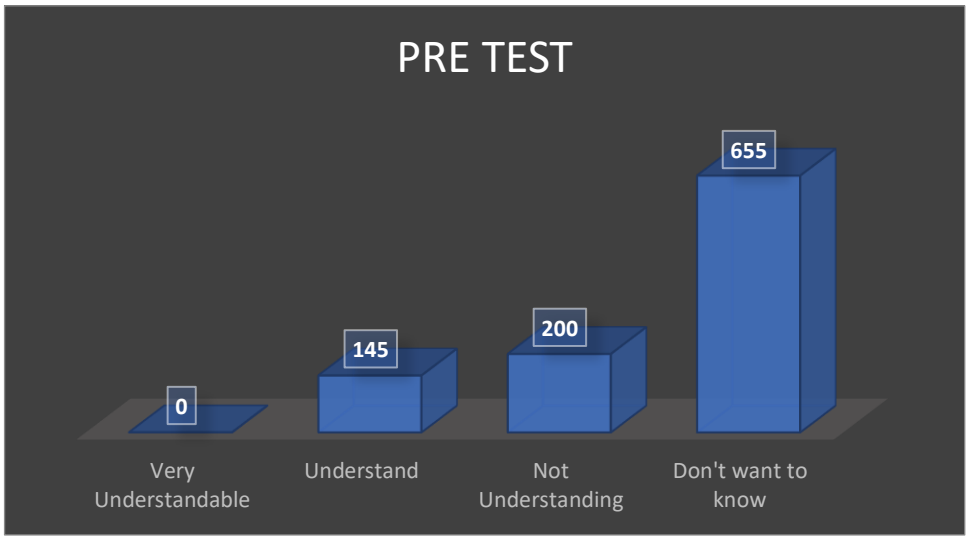

Fig 2. Understanding survey results before service activities

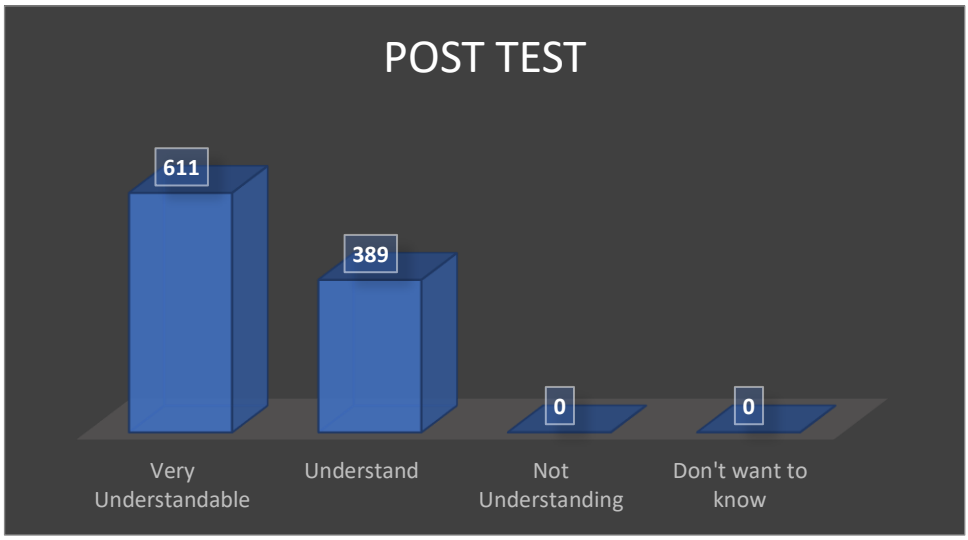

Fig 3. Understanding survey results after service activities

Discussion

Critical Analysis

Current approaches to increasing cybersecurity awareness among teenagers through digital education and simulation have shown both strengths and weaknesses. On the positive side, digital education methods, such as gamification and e-learning, offer flexibility, engagement, and scalability, making cybersecurity education more accessible and appealing to a digital-native audience. Simulation-based approaches, particularly phishing simulations and role-playing scenarios, have proven to be effective in building practical skills. However, these methods often face challenges in achieving sustained engagement, as teenagers may lose interest or become desensitized over time. Furthermore, many of these initiatives lack personalization, meaning they may not address the unique needs or learning preferences of individual teenagers. In addition, the effectiveness of these approaches is sometimes limited by the quality of the tools and the availability of resources. While they are useful in raising awareness, there is still a gap in ensuring long-term behavior change and retention of knowledge.

Gaps in Research

Despite the growing body of research on digital education and simulations for cybersecurity awareness, several critical areas remain underexplored. Cultural influences, for instance, have not been thoroughly examined, leaving a gap in understanding how different cultural backgrounds affect teenagers' perceptions of cybersecurity risks and their engagement with educational tools. Additionally, long-term retention of cybersecurity knowledge is another underexplored area. While immediate improvements in awareness and skills are often observed, few studies track how well teenagers maintain these skills over time. Research is also limited on how teenagers' evolving online behaviors and emerging threats impact the effectiveness of current education models. Finally, there is a lack of studies that assess the integration of cybersecurity education into broader curricula, which could lead to more comprehensive, systemic solutions.

Integration of Education and Simulation

The integration of education and simulation tools holds significant potential for enhancing cybersecurity awareness among teenagers. When combined, these two approaches can provide both theoretical knowledge and practical experience, reinforcing the concepts learned through digital education. For example, after learning about the risks of phishing through e-learning modules, teenagers can engage in real-world simulations that challenge them to apply this knowledge in identifying phishing attempts. This integrated approach fosters a more active and participatory learning process, improving both short-term understanding and long-term retention. However, there is room for improvement in integrating these methods more seamlessly, ensuring that simulations are directly aligned with the content delivered in educational modules. By creating a cohesive learning experience where each element supports the other, educators can more effectively prepare teenagers to handle cyber threats in real life.

Practical Implications

For educators, policymakers, and developers, several actionable recommendations can be made to improve cybersecurity education for teenagers. Educators should focus on creating engaging, age-appropriate content that combines both theoretical lessons and interactive simulations. Policymakers could support the development of standardized cybersecurity curricula that integrate digital education and simulation tools, ensuring that all students receive consistent, high-quality training. Developers should focus on creating customizable and scalable simulation platforms that can be adapted to different learning levels and cultural contexts. Furthermore, fostering collaboration between educators, cybersecurity experts, and technology developers could lead to more effective and comprehensive educational solutions. Finally, to ensure long-term impact, educators should incorporate strategies for continuous engagement and periodic updates to keep pace with evolving cyber threats.

CONCLUSION

The highlighted several key insights regarding the role of digital education and simulation in increasing cybersecurity awareness among teenagers. Digital education methods, such as e-learning platforms and gamification, have been shown to effectively engage teenagers by offering interactive and flexible learning experiences. Simulation tools, including phishing simulations and role-playing scenarios, provide valuable hands-on practice that enhances practical skills in identifying and mitigating cyber threats. Age-specific strategies, such as mobile apps and peer-driven approaches, have also proven effective in increasing engagement. However, challenges remain in sustaining long-term interest and retention, and there is a

need for more personalized and culturally relevant content. Overall, the review underscores the importance of combining educational tools with practical simulations to create a comprehensive cybersecurity awareness program for teenagers. This review makes several important theoretical contributions to the field of cybersecurity awareness. By synthesizing findings from various studies, it provides a clearer understanding of how digital education and simulation tools can complement each other in fostering greater awareness and skill development among teenagers. The research highlights the need for more targeted, age-appropriate strategies and calls attention to the gaps in current approaches, such as cultural influences and long-term retention. Additionally, this review emphasizes the significance of integrating cybersecurity education into broader curricula, contributing to the growing body of knowledge on effective, scalable cybersecurity interventions. These insights can inform future theories and models related to adolescent learning in the context of cybersecurity. Future research should explore several promising directions to advance cybersecurity awareness among teenagers. One area for development is the use of AI-driven simulations that adapt to individual learning styles and provide more personalized learning experiences. AI-powered tools could offer real-time feedback, tailor challenges to students' skill levels, and continuously evolve to address new cyber threats. Additionally, research into collaborating with social media platforms could be fruitful, as these platforms are a primary digital space for teenagers. Investigating how to integrate cybersecurity education directly into social media environments, such as through embedded educational modules or influencer-driven campaigns, could further enhance engagement. Lastly, studies on the long-term retention of cybersecurity practices and the effectiveness of gamified and simulation-based learning models over time are critical to ensuring lasting behavior change in teenagers.

Reference

Bakker, S. (2024). *Immersive Virtual Reality and Cybersecurity: Combatting Social Engineering in a Healthcare Context*. University of Twente.

Balk, E. M., Chung, M., Chen, M. L., Chang, L. K. W., & Trikalinos, T. A. (2013). Data extraction from machine-translated versus original language randomized trial reports: a comparative study. *Systematic Reviews*, *2*, 1–6.

Benchimol, E. I., Smeeth, L., Guttmann, A., Harron, K., Moher, D., Petersen, I., Sørensen, H. T., von Elm, E., Langan, S. M., & Committee, R. W. (2015). The REporting of studies Conducted using Observational Routinely-collected health Data (RECORD) statement. *PLoS Medicine*, *12*(10), e1001885.

Bennett, W. L. (2007). *Civic life online: Learning how digital media can engage youth*. The MIT Press.

Bernstein, B. E., Kamal, M., Lindblad-Toh, K., Bekiranov, S., Bailey, D. K., Huebert, D. J., McMahon, S., Karlsson, E. K., Kulbokas, E. J., & Gingeras, T. R. (2005). Genomic maps and comparative analysis of histone modifications in human and mouse. *Cell*, *120*(2), 169–181.

Bramer, W. M., De Jonge, G. B., Rethlefsen, M. L., Mast, F., & Kleijnen, J. (2018). A systematic approach to searching: an efficient and complete method to develop literature searches. *Journal of the Medical Library Association: JMLA*, *106*(4), 531.

Buchan, M. C., Bhawra, J., & Katapally, T. R. (2024). Navigating the digital world: development of an evidence-based digital literacy program and assessment tool for youth. *Smart Learning Environments*, *11*(1), 8.

Chassiakos, Y. L. R., & Stager, M. (2020). Current trends in digital media: How and why teens use technology. In *Technology and adolescent health* (pp. 25–56). Elsevier.

Cortesi, S., Hasse, A., Lombana-Bermudez, A., Kim, S., & Gasser, U. (2020). Youth and digital citizenship+ (plus): Understanding skills for a digital world. *Berkman Klein Center Research Publication*, *2020–2*.

Curry, L. A., Nembhard, I. M., & Bradley, E. H. (2009). Qualitative and mixed methods provide unique contributions to outcomes research. *Circulation*, *119*(10), 1442–1452.

Delen, D., Zaim, H., Kuzey, C., & Zaim, S. (2013). A comparative analysis of machine learning systems for measuring the impact of knowledge management practices. *Decision Support Systems*, *54*(2), 1150–1160.

Dym, B., & Fiesler, C. (2020). Social norm vulnerability and its consequences for privacy and safety in an online community. *Proceedings of the ACM on Human-Computer Interaction*, *4*(CSCW2), 1–24.

Fouad, N. S. (2022). The security economics of EdTech: vendors' responsibility and the cybersecurity challenge in the education sector. *Digital Policy, Regulation and Governance*, *24*(3), 259–273.

Gusenbauer, M., & Haddaway, N. R. (2020). Which academic search systems are suitable for systematic reviews or meta-analyses? Evaluating retrieval qualities of Google Scholar, PubMed, and 26 other resources. *Research Synthesis Methods*, *11*(2), 181–217.

Hamdan, Z., Obaid, I., Ali, A., Hussain, H., Rajan, A. V, & Ahamed, J. (2013). Protecting teenagers from potential internet security threats. *2013 International Conference on Current Trends in Information Technology (CTIT)*, 143–152.

Hamilton, A. B., & Finley, E. P. (2019). Qualitative methods in implementation research: An introduction. *Psychiatry Research*, *280*, 112516.

Harris, J. D., Quatman, C. E., Manring, M. M., Siston, R. A., & Flanigan, D. C. (2014). How to write a systematic review. *The American Journal of Sports Medicine*, *42*(11), 2761–2768.

Hjørland, B. (2015). Classical databases and knowledge organization: A case for boolean retrieval and human decision-making during searches. *Journal of the Association for Information Science and Technology*, *66*(8), 1559–1575.

Hoffmann, T. C., Glasziou, P. P., Boutron, I., Milne, R., Perera, R., Moher, D., Altman, D. G., Barbour, V., Macdonald, H., & Johnston, M. (2014). Better reporting of interventions: template for intervention description and replication (TIDieR) checklist and guide. *Bmj*, *348*.

Huang, B. (2024). Navigating digital divide: exploring the influence of ideological and political education on cyber security and digital literacy amid information warfare. *Current Psychology*, 1–22.

Jain, A. K., Sahoo, S. R., & Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. *Complex & Intelligent Systems*, *7*(5), 2157–2177.

James, C. (2009). *Young people, ethics, and the new digital media: A synthesis from the GoodPlay Project*. The MIT Press.

Johnson, M. (2016). *Cyber crime, security and digital intelligence*. Routledge.

Joshi, R., & Rehman, S. (2023). Raising Awareness of Social Engineering among Adolescents: Psychological and Cybersecurity Perspective. In *Cybersecurity for Decision Makers* (pp. 99–109). CRC Press.

Kam, H.-J., Menard, P., Ormond, D., & Crossler, R. E. (2020). Cultivating cybersecurity learning: An integration of self-determination and flow. *Computers & Security*, *96*, 101875.

Kaur, G., Bonde, U., Pise, K. L., Yewale, S., Agrawal, P., Shobhane, P., Maheshwari, S., Pinjarkar, L., & Gangarde, R. (2024). Social Media in the Digital Age: A Comprehensive Review of Impacts, Challenges and Cybercrime. *Engineering Proceedings*, *62*(1), 6.

Knobloch, K., Yoon, U., & Vogt, P. M. (2011). Preferred reporting items for systematic reviews and meta-analyses (PRISMA) statement and publication bias. *Journal of Cranio-Maxillofacial Surgery*, *39*(2), 91–92.

Koutsos, T. M., Menexes, G. C., & Dordas, C. A. (2019). An efficient framework for conducting systematic literature reviews in agricultural sciences. *Science of the Total Environment*, *682*, 106–117.

Laczi, S. A., & Póser, V. (2024). Navigating Children's Cybersecurity Landscape: Understanding the impact of cyberbullying, online harrasment and identity theft on children. *2024 IEEE 18th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, 1–6.

Livingston, J. D., Milne, T., Fang, M. L., & Amari, E. (2012). The effectiveness of interventions for reducing stigma related to substance use disorders: a systematic review. *Addiction*, *107*(1), 39–50.

Long, H. A., French, D. P., & Brooks, J. M. (2020). Optimising the value of the critical appraisal skills programme (CASP) tool for quality appraisal in qualitative evidence synthesis. *Research Methods in Medicine & Health Sciences*, *1*(1), 31–42.

Majid, U., & Vanstone, M. (2018). Appraising qualitative research for evidence syntheses: a compendium of quality appraisal tools. *Qualitative Health Research*, *28*(13), 2115–2131.

McFadden, M. L. (2021). *Cybersecurity Experiential Leadership Learning*. Northeastern University.

Megele, C. (2017). *Safeguarding children and young people online: A guide for practitioners*. Policy Press.

Mishra, A., Gupta, B. B., & Gupta, D. (2018). Identity Theft, Malware, and Social Engineering in Dealing with Cybercrime. In *Computer and Cyber Security* (pp. 627–648). Auerbach Publications.

Montgomery, K. C., & Chester, J. (2009). Interactive food and beverage marketing: targeting adolescents in the digital age. *Journal of Adolescent Health*, *45*(3), S18–S29.

Okpokwasili, O. A., & Onwuatuegwu, I. N. (2023). Online Predators: Protecting Teenagers from Internet Sexual Exploitation. *International Journal of Modern Science and Research Technology*, *1*(23), 324–334.

Organization, W. H. (2020). *Youth-centered digital health interventions: a framework for planning, developing and implementing solutions with and for young people*. World Health Organization.

Ortiz, E. (2017). *Developing an Insider Threat Experimental Environment*.

Owusu, S. (2023). *Bridging the Cybersecurity Workforce Skill Gap With Experiential Learning: The Role of Cybersecurity Clinics*. Marymount University.

Panic, N., Leoncini, E., de Belvis, G., Ricciardi, W., & Boccia, S. (2013). Evaluation of the endorsement of the preferred reporting items for systematic reviews and meta-analysis (PRISMA) statement on the quality of published systematic review and meta-analyses. *PloS One*, *8*(12), e83138.

Pham, M. T., Rajić, A., Greig, J. D., Sargeant, J. M., Papadopoulos, A., & McEwen, S. A. (2014). A scoping review of scoping reviews: advancing the approach and enhancing the consistency. *Research Synthesis Methods*, *5*(4), 371–385.

Reid Chassiakos, Y. L., Radesky, J., Christakis, D., Moreno, M. A., Cross, C., Hill, D., Ameenuddin, N., Hutchinson, J., Levine, A., & Boyd, R. (2016). Children and adolescents and digital media. *Pediatrics*, *138*(5).

Saharan, V. A., Kulhari, H., Jadhav, H., Pooja, D., Banerjee, S., & Singh, A. (2020). Introduction to research methodology. In *Principles of Research Methodology and Ethics in Pharmaceutical Sciences* (pp. 1–46). CRC Press.

Samala, A. D., Rawas, S., Criollo-C, S., Fortuna, A., Feng, X., Prasetya, F., Uluçay, N. Ö., Jaya, P., & Hidayat, R. (2024). Social Media in Education: Trends, Roles, Challenges, and Opportunities for Digital-Native Generations–A Systematic Literature Review. *Asian Journal of University Education*, *20*(3), 524–539.

Sithira, V., & Nguwi, Y.-Y. (2014). A study on the adolescent online security issues. *International Journal of Multidisciplinary and Current Research*, *2*, 596–601.

Sovacool, B. K., Axsen, J., & Sorrell, S. (2018). Promoting novelty, rigor, and style in energy social science: Towards

codes of practice for appropriate methods and research design. *Energy Research & Social Science*, *45*, 12–42.

Srivastava, A. K. (2024). Critical Analysis of Cybersecurity Awareness Programs in School Education. *Library Progress International*, *44*(3), 18282–18303.

Tsirtsis, A., Tsapatsoulis, N., Stamatelatos, M., Papadamou, K., & Sirivianos, M. (2016). Cyber security risks for minors: A taxonomy and a software architecture. *2016 11th International Workshop on Semantic and Social Media Adaptation and Personalization (SMAP)*, 93–99.

Watkins, S. C. (2009). *The young and the digital: What the migration to social-network sites, games, and anytime, anywhere media means for our future*. Beacon Press.

West, D. M. (2012). *Digital schools: How technology can transform education*. Brookings Institution Press.

Willard, N. E. (2007). *Cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress*. Research press.

Zhang-Kennedy, L., & Chiasson, S. (2021). A systematic review of multimedia tools for cybersecurity awareness and education. *ACM Computing Surveys (CSUR)*, *54*(1), 1–39.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82–97.