International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Learning Strategies for Promoting Cybersecurity Awareness among Students: A Brief Review

Kumari Sarita[1], Kashish[2], Pritpal Singh[3], Gurpreet Singh[4], Satinder Kaur[5]

[1, 2, 3]Department of Computer Science
[4, 5]Department of Computer Engineering & Technology
[1, 2, 3, 4, 5]Guru Nanak Dev University, Amritsar

Abstract

As the utilization of digital learning applications is increasing rapidly, cybersecurity has become an emerging concern all over the world. Since everything is going online, so, it becomes important to be aware of cybersecurity assaults. Various studies have been undertaken to determine the extent of cybersecurity awareness among students. During the contemporary pedagogical epoch of the COVID pandemic, diverse learning strategies and protocols have been developed to enlighten students about cybersecurity. The current work aims to gather and assemble assorted methods along with some approaches in a single distribution. An in-depth study of these learning strategies paves the way for further planning and creating new technologies by merging already existing techniques. Moreover, new IoT, as well as machine learning tools and techniques, can be further embedded in the above strategies.

Keywords: Cybersecurity Awareness, Learning Strategies, Students

1 Introduction

In the online teaching era, the web has become the major source to exchange information among students due to the COVID pandemic. The online exchange of digital information is sometimes compromised using cyberattacks [3]. A cyberattack is an illegal attempt to acquire unapproved access to a device, an environment, or a network. The reason for a cyberattack is to destroy, disable, control, or steal the data related to these frameworks [24]. As the students make use of online teaching technologies the most, there are a greater number of chances for them to get vulnerable to cyberattacks [6]. Consequently, India has the second position in the top five cyberattacked countries in the year 2020 as per the report of DSCI (Data Security Council of India) [25]. To reduce the risks of cyberattacks, it is necessary to provide awareness of cybersecurity among the students.

Cybersecurity is the safeguard to the privacy or security of the computer interfaces and systems [24]. In modern digital life, awareness and knowledge about cybersecurity attacks are endless, however, one must be trained to protect sensitive and confidential data [19]. Unfortunately, school or university students suffer from a lack of awareness concerning cybersecurity attacks and the means to rectify them. A lot of researchers have worked in this discipline to assess the awareness about cybersecurity among the students and found an unsatisfactory level of awareness about cybersecurity among them [1,3,6,16,19,23,24].

The current study aims to highlight the recent learning techniques and methodologies used by various

researchers for cybersecurity awareness. The remainder of the paper is structured as follows: Section 2 provides an overview of previous studies related to awareness of cybersecurity among university and school students. Section 3 depicts the methodology adopted during the study. Section 4 reviews some learning techniques and methodologies used in past studies. Further, Section 5 presents the answers to research questions framed in Section 3. In the end, Section 6 concludes the paper and provides some recommendations for further work to increase awareness regarding cybersecurity in the modern teaching era.

2 Literature Review

Cybersecurity is the ability to protect and defend the use of cyberspace from cyberattacks [17]. In a survey, seven lakh cybercrimes were disclosed all over India as of August 2020, however, a critical increment of about four lakh cybercrimes was observed afterward as compared to the previous year [21]. Although more than half of Indian youth don't have even a little idea about how to deal with cyberattacks [26]. To determine the level of awareness about cybersecurity among university or school students, a lot of researchers have worked in this discipline [3,6,7,16,19,20,22,24]. The literature review comes up with a glance at related studies of various methodologies and techniques to improve cybersecurity awareness.

Further, Ronald *et al.* [8] conducted a study to test the effectiveness of cybersecurity competitions by providing a virtual learning environment to students, and it was observed that the use of workshops and lectures can improve the effectiveness of cybersecurity competitions. Although Sreejith *et al.* [4] conducted a questionnaire-based survey through a gaming approach. The results showed that the students' participation was good and the approach was helpful, with good learning outcomes.

Jones *et al.* [15] conducted interviews with 44 cybersecurity professionals to identify the knowledge, skills, and abilities required to perform the job of cybersecurity. Furthermore, the researchers utilized a game-based learning methodology to increase the interest and awareness about cybersecurity which was found to be more enjoyable and interesting for male students than female students [14]. Abbas and Moallem [19] evaluated the cybersecurity awareness among the students in the public universities of California, and it was found that the students lacked the knowledge of basic principles of security.

Moreover, Gabra *et al.* [10] carried out a case study using a questionnaire-based methodology to identify the level of cybersecurity awareness among university students in Nigeria. The results indicated that the students lack the basic knowledge of cybersecurity, and it is recommended to conduct cybersecurity awareness programs by the university to improve the cybersecurity awareness level. Although Vykopal *et al.* [5] proposed a KYPO4INDUSTRY training facility to teach cybersecurity by providing a course syllabus. As per findings, this methodology was helpful for students to practically learn about threats, to develop an educational cybergame, and to improve their soft skills during various public presentations.

Lorenz and Kikkas [18] discussed pedagogical and ethical challenges to developing critical thinking in cybersecurity. The user evaluation method was used to conduct the study, which helped to provide new knowledge about cybersecurity among students. Furthermore, Carames and Lamas [9] proposed a practical use-case-based teaching methodology that provided an introduction to the basics of IoT cybersecurity for future developers.

Further, Pang *et al.* [27] conducted a survey on internet usage and cybersecurity awareness among the students of three age groups between 8 and 21 years. The results further show that the majority of the students lacked knowledge of cybersecurity tools for tablets and smartphones. Moreover, Ahmad *et al.* [2]

proposed a roadmap for cybersecurity education, which will be helpful for the universities to choose the best approach for their degrees.

The majority of the researchers have focused on the evaluation of the level of cybersecurity awareness and the course content of cybersecurity awareness programs; however, nobody effort to describe all these techniques and methodologies in a single distribution. The current paper aims to enlighten some previous methodologies and techniques designed by various researchers.

3 Methodology

Review methodology provides an overview of the review process, as in Figure 1. The authors used Google Scholar, Science Direct, ResearchGate, and Web of Science to collect and extract data with the help of meta keywords such as Cybersecurity awareness, among students, teaching era, and Learning Strategies for cybersecurity awareness. The research data is searched only for the years from 2015 to 2021. A total of 55 papers are retrieved: 15 from Google Scholar, 10 from Science Direct, 20 from Research Gate, and 10 from Web of Science. However, only 25 papers are selected for the current review: 8 from Google Scholar, 4 from Science Direct, 8 from Research Gate, and 5 from Web of Science. Furthermore, only English language articles are selected, and relevant information related to the current study is extracted from the search engines. Two categories of papers are found during the collection and extraction process. The first category of papers is related to the evaluation of cybersecurity awareness, whereas the second category of papers is concerned with the improvement of cybersecurity awareness among students. The total count of first category papers is 12, whereas the number of research papers belonging to the second category is 13. After extracting the specific papers, the following research questions are framed:

- **RQ1:** Which learning strategies for Cybersecurity awareness are found in the literature?
- **RQ2:** Which learning Strategy for Cybersecurity awareness is found most suitable as per the literature?
- **RQ3:** What is the status of cybersecurity awareness among students as per the literature?
- **RQ4:** What are the remedial plans to improve cybersecurity awareness among students?

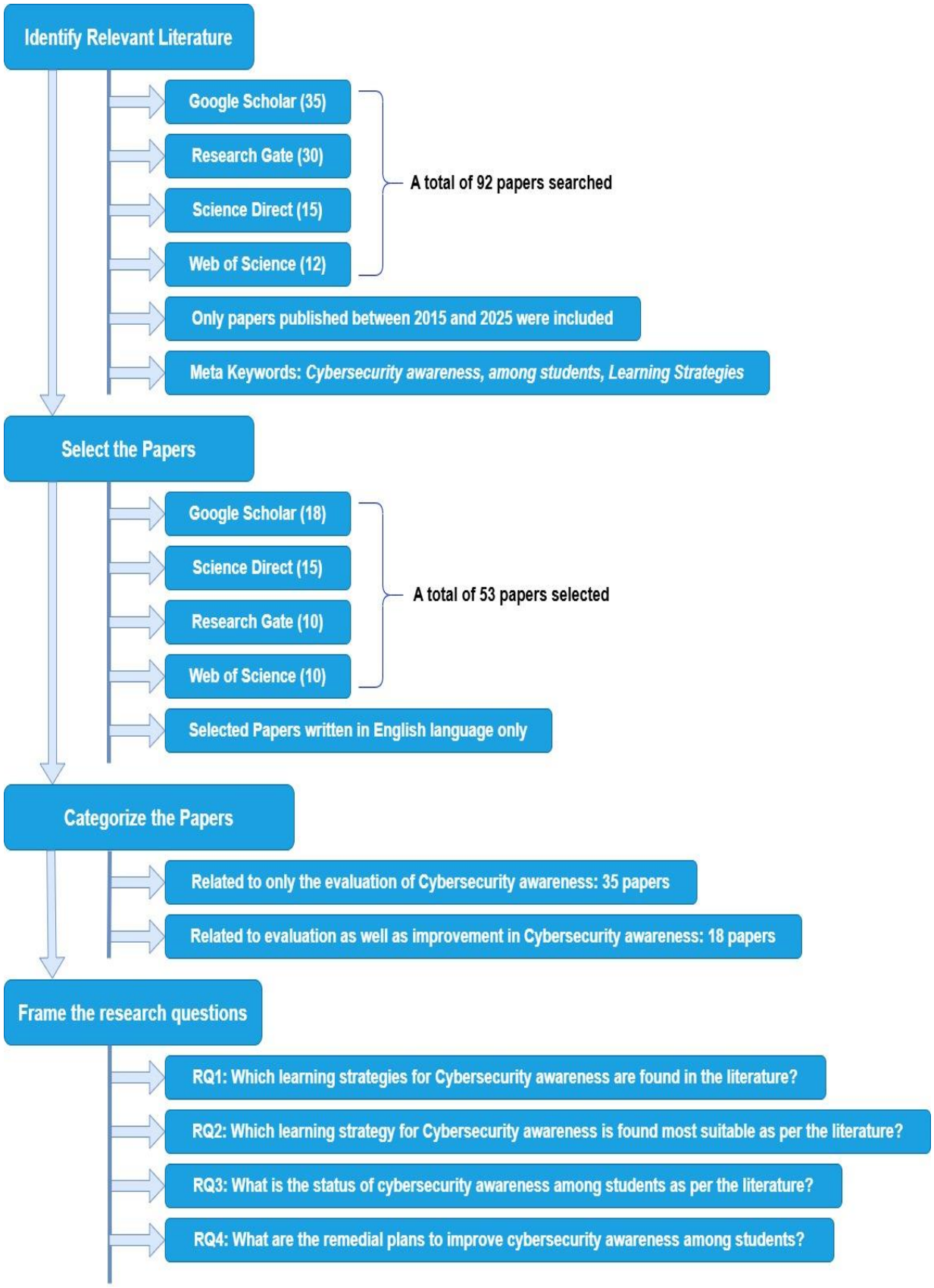

Figure 1: ***Review Methodology***

4 Recent Learning Strategies Used for Cybersecurity Awareness

There exist different learning strategies for the evaluation as well as improvement of cybersecurity awareness, as in Figure 2.

Figure 2: ***Learning Strategies for Cybersecurity Awareness***

4.1 Questionnaire-Based Survey

Questionnaire-based survey methodology is the cybersecurity awareness evaluation approach. This is a survey method used to collect information about the cybersecurity awareness level. Three types of modes are available for this kind of approach: open-ended, closed-ended, and mixed-mode. An open-ended mode consists of the detailed description of the answer to a specific question, whereas a closed-ended mode consists of multiple-choice questions. Although a mixed-mode comprises the combination of open-ended and closed-ended modes. A questionnaire-based survey may be conducted online as well as offline. This methodological approach can help to improve the level of cybersecurity awareness based on the answers by the respondents. Pang *et al.* [27] used a questionnaire-based survey approach to evaluate the level of awareness among students aged between18-21 years. The questionnaire was related to awareness about basic terms like firewall, privacy, tracker, browser, antivirus, phishing, security warning, installation and use of security software, security issues of tablets and mobile devices, as well as security breaches [27]. Recently, a questionnaire-based survey approach was implemented to evaluate the basic concept of cybersecurity trust, privacy, password-related issues, and cybersecurity awareness program [10,11].

4.2 Interviews with Cybersecurity Professionals

This methodological approach is the cybersecurity awareness improvement approach. This is the smart approach to finding solutions to various issues related to cybersecurity. Jones *et al.* made use of an interviewing approach [15]. This approach was based on cyber defense and helped determine what KSAs (knowledge, skills, and abilities) are required to resolve cybersecurity-related problems [15]. The researchers asked three types of questions during the interview: demographic, KSA, and open-ended questions [15]. The demographic questions were related to the analysis of computer network defense, its infrastructure support, incident response, vulnerability evaluation, and management [15]. The second category of questions was concerned with the importance and learning of KSA. The open-ended questions were asked about the usage of cyber-related tools [15].

4.3 Gamification

This methodology is used to evaluate as well as improve cybersecurity awareness. Game-based learning is also known as learning for fun [4]. To evaluate the cybersecurity awareness level among students, an innovative and excellent approach is called the gamification approach. This is a game-based learning methodology where the educational games are designed to learn and perform various cybersecurity tasks [5,13]. The Gamification approach allows learners to play the game by following a set of instructions and giving reviews about the game [5]. Through this learning method, the learner will be able to learn how to deal with cyberattacks. An interactive video game, Cyber Shield Game, has been developed to enhance employees' cybersecurity awareness through a scenario-based gamified experience. It includes four levels: Password Complexity, Social Engineering, Phishing Attack, and Physical Security—each targeting specific cybersecurity threats [34]. Similar gamified approaches have shown significant promise. For example, a four-level gaming approach was proposed to learn about cybersecurity [4]. The first level was the test of basic programming skills, the second level was related to web application security, the third level was concerned with application security, and the fourth level was associated with forensics and reverse engineering [4]. Furthermore, an innovative game-based learning methodology was implemented for cybersecurity education in the PNW Gen Cyber camp [14]. This methodology is comprised of four modules: social engineering and information security concept, secure online behavior game, cybersecurity defense tower game, and 2D Gen Cyber card game [14]. The performance of students in the game was measured by a five-point Likert scale in the range from 5 (strongly agree) to 1 (strongly disagree) [14]. This methodological approach was an excellent platform for knowledge enhancement in cybersecurity concepts, understanding the first principles of cybersecurity, increasing cybersecurity awareness, and inspiring them to build their careers in the field of cybersecurity [14].

4.4 Lectures and Presentations

Lectures and presentation methods are the cybersecurity awareness improvement approaches. These are the most commonly used methods to aware the students of the basic concepts of cybersecurity and to enhance their soft skills by making presentations. By using this approach, the students will be able to protect, identify, and solve the issues related to cybersecurity [12]. A hands-on learning methodology was employed for students to learn and implement the concepts of cybersecurity [8]. This methodology also offered students to practice network configuration and defense by providing a virtual network based on Virtual Machines [8]. In this approach, students presented interactive lectures and presentations based on

the previously learned concepts of cybersecurity for new students [8]. This learning approach encouraged the students to build their virtual machines with some kind of vulnerabilities and inspired them to identify and rectify such kinds of issues [8].

4.5 Workshops and Courses

This is the most effective approach for the evaluation and improvement of cybersecurity awareness. Several workshops can be conducted to train the students by following a course syllabus in the field of cybersecurity. This methodology provides a virtual learning environment to introduce, apply, and solve cybersecurity-related problems [2]. Vykopal *et al.* [5] proposed a training facility named KYPO4INDUSTRY to employ a testbed for hands-on ICS cybersecurity teaching. It was a novel university course to teach about ICS domain threats, to design an educational cyber game, and to enhance their soft skills [5]. Furthermore, Gupta *et al.* [12] introduced a course on AI-assisted Malware Analysis. This course aimed to introduce malware attack stages, to represent malware knowledge, to collect malware data, to identify a feature, to identify malware, to classify malware, and also to learn about the latest malware research topics and case studies [12]. Moreover, a roadmap was presented to provide cybersecurity education by introducing the basic concepts of cybersecurity, implementing these concepts in other fields, and using multiple approaches to solve cybersecurity problems [2]. This approach was helpful for the universities to choose the best approach for their degrees in the field of cybersecurity [2].

4.6 Simulation-based learning

Simulation-based learning provides a practical and immersive way to build cybersecurity awareness. Through the simulation of real-world threat scenarios, such as malware incursions or phishing emails, students can actively participate in recognizing and addressing security threats in a controlled setting [50,51]. This practical experience enhances comprehension, boosts memory, and enhances learners' self-assurance when implementing cybersecurity procedures in real-world circumstances [52]. To investigate the efficacy of this strategy, pilot research was carried out with Master's students from various academic backgrounds and with differing degrees of cybersecurity expertise [53]. To introduce participants to the platform, the study used an agent-based simulation tool called CyberAIMs in conjunction with a real-world cyber case scenario. In this, students took a pre- and post-test to evaluate how the simulation affected their way of thinking. The study showed that simulation-based learning significantly enhanced students' understanding of critical factors in cybersecurity decision-making and fostered the development of higher-order cognitive skills, including systems thinking and adversarial reasoning [52]. In order to broaden the breadth of simulation-based learning, Surdjono et al. [53] developed a cybersecurity awareness program for accounting and finance students that uses mobile simulations. The initiative used the 4D methodology (Define, Design, Develop, Disseminate) to build interactive simulations that taught cyber hygiene principles through mobile devices. The study, which included 68 participants and instruments including behavioral questionnaires and awareness tests, showed a significant improvement in cybersecurity practices and awareness. This study demonstrates how mobile platforms may facilitate simulation-based education by integrating simulation features into mobile learning environments. This maintains the immersive aspect of simulation while providing accessibility, flexibility, and contextual relevance.

5 Results and Analysis

This section aims to provide the answers to the research questions framed in section 3. These research questions are answered based on the results of the data collected from the existing literature and presented in Table 1.

Table 1: ***Analysis of existing literature***

RQ-ID	Research Question	Outcomes	Papers
RQ1	Which learning strategies fo Cybersecurity awarenes are found in the literature?	To answer this research question, a total o 53 papers were selected in the period fro 2015 to 2025. The papers are then analyzed to find the learnin methods and techniques for cybersecurit awareness among students. Durin analysis, six learning strategies are foun to evaluate as well as to improv cybersecurity awareness among students These are Questionnaire-Based Survey Interviews with Industry Experts Gamification Approach, Lectures an Presentations, Workshops, Courses, an Simulation-based Learning.	[2], [4], [5], [8] [10], [11], [12], [13], [14], [15], [27], [28], [29], [30], [31], [32], [33] [34], [35], [36] [37], [38], [39] [40]
RQ2	Which learning Strategy for Cybersecurity awareness i found most suitable as per the literature?	To answer this question, the results o selected studies are analyzed. As per th analysis, the Questionnaire-Based Surve Methodology is found to be more suitabl only for the evaluation of cybersecurit awareness among students. Although th majority of researchers utilized th Gamification approach, hence, this i found as the most suitable learnin strategy for the evaluation as well as th improvement of cybersecurity awarenes among students.	[4], [5], [13], [14], [28], [29], [30], [33], [34], [35] [36]
RQ3	What is the status of cybersecurity awarenes among students as per th literature?	During the analysis of related studies, it is found that the level of cybersecurit awareness among students is very poo and no or very less awareness program for cybersecurity are conducted b universities and organizations to rais awareness the students abou cybersecurity.	[6], [19], [23], [16], [26], [27], [11], [22], [7], [20], [41], [42], [43] [44]

RQ4	What are the remedial plans t improve cybersecurit awareness among students?	A lot of remedial suggestions are foun during the review of past studies awareness programs by each universit and organization should be develope time to time, improvement in the trainin content and certification courses, desig and development of methods for creatin better as well as more interesting cybe games, and more effective hands-o practice in the field of cybersecurit through training. Moreover, a nev learning strategy can be created b embedding new IoT as well as machin learning tools and techniques in all th above strategies.	[27], [11], [5], [8], [9], [45], [46] [47], [48], [49]

6 Conclusion

In the digital scenario, cybersecurity has become a major concern as it is safeguarding the security and privacy of the data and the computer system itself. It has become necessary to be aware of cyberattacks and also of how to prevent sensitive information from these cyber threats. As per the prior studies reviewed, the cybersecurity awareness among university students is far and there is also a lack of cybersecurity awareness improvement programs conducted by the university organizations. The current study aims to review different techniques used by past studies to improve cybersecurity awareness among students. The gaming approach is found to be most suitable among all other learning strategies. It is proposed that new techniques and methodologies can be further planned and created by merging already existing techniques. Moreover, new IoT, as well as machine learning tools and techniques, can be embedded in the above strategies.

References

[1] Abd Rahim, N. H., Hamid, S., Kiah, M. L. M., Shamshirband, S., and Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes*.

[2] Ahmad, N., Laplante, P., Defranco, J., and Kassab, M. H. (2021). A cybersecurity-educated community. *IEEE Transactions on Emerging Topics in Computing*.

[3] Ahmed, N., Kulsum, U., Azad, I. B., Momtaz, A. Z., Haque, M. E., and Rahman, M. S. (2017). Cybersecurity awareness survey: An analysis from Bangladesh perspective. In *2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)*, pages 788–791. IEEE.

[4] Boopathi, K., Sreejith, S., and Bithin, A. (2015). Learning cyber security through gamification. *Indian Journal of Science and Technology*, 8(7):642–649.

[5] Č eleda, P., Vykopal, J., Švábenskỳ, V., and Slavíček, K. (2020). Kypo4industry: A testbed for teaching cybersecurity of industrial control systems. In *Proceedings of the 51st, ACM Technical Symposium on Computer Science Education* pages 1026–1032.

[6] Chandarman, R. and Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *The African Journal of Information and Communication*, 20:133– 155.

[7] Chasanah, B. R. and Candiwan, C. (2020). Analysis of college students' cybersecurity awareness in Indonesia. *SISFORMA*, 7(2):49–57.

[8] Cheung, R. S., Cohen, J. P., Lo, H. Z., Elia, F., and Carrillo-Marquez, V. (2012). Effectiveness of cybersecurity competitions. In *Proceedings of the International Conference on Security and Management (SAM)*, page 1. The Steering Committee of The World Congress in Computer Science, Computer.

[9] Fernández-Caramés, T. M. and Fraga-Lamas, P. (2020). Teaching and learning iot cybersecurity and vulnerability assessment with Shodan through practical use cases. *Sensors*, 20(11):3048.

[10] Gabra, A. A., Sirat, M. B., Hajar, S., and Dauda, I. B. (2020). Cyber security awareness among university students: A case study. *Journal of Critical Reviews*, 7:16.

[11] Garba, A. A., Siraj, M. M., Othman, S. H., and Musa, M. (2020). A study on cybersecurity awareness among students in your state university, Nigeria: A quantitative approach. *International Journal on Emerging Technologies*, 11(5):41–49.

[12] Gupta, M., Mittal, S., and Abdelsalam, M. (2020). Ai assisted malware analysis: A course for next-generation cybersecurity workforce. *arXiv preprint arXiv:2009.11101*.

[13] Jian, N. J. and Kamsin, I. F. B. (2021). Cybersecurity awareness among the young in Malaysia by gamification. In *3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021)*, pages 487–494. Atlantis Press.

[14] Jin, G., Tu, M., Kim, T.-H., Heffron, J., and White, J. (2018). Game-based cybersecurity training for high school students. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*, pages 68–73.

[15] Jones, K. S., Namin, A. S., and Armstrong, M. E. (2018). The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school: Results from interviews with cybersecurity professionals. *ACM Transactions on Computing Education (TOCE)*, 18(3):1– 12.

[16] Khalid, F., Daud, M. Y., Rahman, M. J. A., and Nasir, M. K. M. (2018). An investigation of university students' awareness of cyber security. *International Journal of Engineering & Technology*, 7(4.21):11–14.

[17] Kissel, R. (2013). Nistir 7298: Glossary of key information security terms, revision 2. *United States Department of Commerce: National Institute of Standards and Technology*.

[18] Lorenz, B. and Kikkas, K. (2020). Pedagogical challenges and ethical considerations in developing critical thinking in cybersecurity. In *2020 IEEE 20th International Conference on Advanced Learning Technologies (ICALT)*, pages 262–263. IEEE.

[19] Moallem, A. (2019). *Cybersecurity Awareness Among Students and Faculty*. CRC Press.

[20] Onyema, E., Edeh, C., Gregory, U., Edmond, V., Charles, A., and Richard-Nnabu, N. Cybersecurity awareness among undergraduate students in enugu Nigeria.

[21] Report, C. (2020). Cybercrime report: https://www.statista.com/.

[22] Senthilkumar, K. and Easwaramoorthy, S. (2017). A survey on cyber security awareness among college students in Tamil Nadu. In *IOP Conference Series: Materials Science and Engineering*, volume 263, page 042043. IOP Publishing.

[23] Slusky, L. and Partow-Navid, P. (2012). Students' information security practices and awareness. *Journal of Information Privacy and Security*, 8(4):3–26.

[24] Sridevi, K. (2020). Cyber security awareness among in-service secondary school teachers of Karnataka. *Indian Journal of Educational Technology*, 2(2):82.

[25] Subexsecure (2020). Cybersecurity report: https://www.subexsecure.com/.

[26] Subramaniam, S. R. (2017). Cyber security awareness among Malaysian pre-university students. *Proceeding of the 6th Global Summit on Education* pages 1–14.

[27] Tirumala, S. S., Sarrafzadeh, A., and Pang, P. (2016). A survey on internet usage and cyber-security awareness in students. In *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, pages 223–228. IEEE.

[28] Baraković, S., & Baraković Husić, J. (2023). Cyber hygiene knowledge, awareness, and behavioral practices of university students. Information Security Journal: A Global Perspective, 32(5), 347-370.

[29] Guo, H., & Tınmaz, H. (2023). A survey on college students' cybersecurity awareness and education from the perspective of China. Journal for the Education of Gifted Young Scientists, 11(3), 351-367.

[30] Kaleeshwari, S., & Jegadeeshwaran, M. (2024) Quantitative Assessment of the Cybersecurity and Cybercrime Awareness among Postgraduate Commerce Students in the Coimbatore District, India.

[31] Behzadi, B. (2024). Examining the efficacy of cybersecurity education at Swedish universities: A qualitative inquiry through interviews.

[32] Growth, A. T. (2025). Cybersecurity Awareness in Higher Education. Bridging Technology and Development for Sustainable Innovation and Geopolitical Dynamics, 197.

[33] Matovu, R., Nwokeji, J. C., Holmes, T., & Rahman, T. (2022, October). Teaching and learning cybersecurity awareness with gamification in smaller universities and colleges. In 2022 IEEE frontiers in education conference (FIE) (pp. 1-9). IEEE.

[34] Pramod, D. (2024). Gamification in cybersecurity education; a state of the art review and research agenda. Journal of Applied Research in Higher Education.

[35] Abu-Amara, F., Hosani, R. A., Tamimi, H. A., & Hamdi, B. A. (2024). Spreading cybersecurity awareness via gamification: zero-day game. International Journal of Information Technology, 16(5), 2945-2953.

[36] Amjad, K., Ishaq, K., Nawaz, N. A., Rosdi, F., Dogar, A. B., & Khan, F. A. (2025). Unlocking Cybersecurity: A Game-Changing Framework for Training and Awareness—A Systematic Review. Human Behavior and Emerging Technologies, 2025(1), 9982666.

[37] Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. Information, 12(10), 417.

[38] Subhani, A., Khan, I. A., & Ahmad, U. (2023). Importance of conducting cyber security awareness sessions among undergraduate students. Journal of Advanced Research in Social Sciences and Humanities, 8(2), 59-68.

[39] Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. Information, 12(10), 417.

[40] Junghans, C., Quirchmayr, G., Schaberreiter, T., Kandlhofer, M., Bieber, R., Andriessen, J., & Pardijs, M. (2024). Enhancing Cybersecurity Awareness and Education. In Proceedings of the Central and Eastern European eDem and eGov Days 2024 (pp. 240-246).

[41] Ahamed, B., Polas, M. R. H., Kabir, A. I., Sohel-Uz-Zaman, A. S. M., Fahad, A. A., Chowdhury, S., & Rani Dey, M. (2024). Empowering students for cybersecurity awareness management in the emerging digital era: the role of cybersecurity attitude in the 4.0 industrial revolution era. Sage Open, 14(1), 21582440241228920.

[42] Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. International Journal of Information and Education Technology, 10(5), 378-382.

[43] Alqahtani, M. A. (2022). Factors affecting cybersecurity awareness among university students. Applied Sciences, 12(5), 2589.

[44] Kumbhakar, M. M., & Kumar, N. (2025). Cyber Security Awareness Among Higher Education Students.

[45] Arishi, A. A., Kamarudin, N. H., Bakar, K. A. A., Shukur, Z. B., & Hasan, M. K. (2024). Cybersecurity Awareness in Schools: A Systematic Review of Practices, Challenges, and Target Audiences. integration, 15(12).

[46] Kallonas, C., Piki, A., & Stavrou, E. (2024, May). Empowering professionals: a generative AI approach to personalized cybersecurity learning. In 2024 IEEE global engineering education conference (EDUCON) (pp. 1-10). IEEE.

[47] AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K. K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. Computers & Security, 119, 102754.

[48] Arishi, A. A., Kamarudin, N. H., Bakar, K. A. A., Shukur, Z. B., & Hasan, M. K. (2024). Cybersecurity Awareness in Schools: A Systematic Review of Practices, Challenges, and Target Audiences. integration, 15(12).

[49] Wang, T., Zhou, N., & Chen, Z. (2025). CyberMentor: AI Powered Learning Tool Platform to Address Diverse Student Needs in Cybersecurity Education. arXiv preprint arXiv:2501.09709.

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

[51] Ortiz, E. (2017). Developing an Insider Threat Experimental Environment.

[52] 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.

[53] Surdjono, H. D., Fadli, R., Sari, R. C., Eliza, F., Yassin, A., Kulanthaivel, G., ... & Purnomo, S. (2025). Effectiveness of Cybersecurity Awareness Program Based on Mobile Learning to Improve Cyber Hygiene. International Journal of Information and Education Technology, 15(2).