International Journal of Recent Advances in Multidisciplinary Topics
Volume 5, Issue 4, April 2024
https://www.ijramt.com | ISSN (Online): 2582-7839

Review of Learning Strategies for Cybersecurity Awareness among Students in Online Teaching Era

Kumari Sarita[1*], Kirandeep Kaur[2], Parminder Kaur[3], Satinder Kaur[4]
[1]Research Scholar, Department of Computer Science, Guru Nanak Dev University, Amritsar, India
[2]Research Scholar, Department of Computer Engineering and Technology, Guru Nanak Dev University, Amritsar, India
[3]Professor, Department of Computer Science, Guru Nanak Dev University, Amritsar, India
[4]Assistant Professor, Department of Computer Engineering and Technology, Guru Nanak Dev University, Amritsar, India

***Abstract*: As the usage of online educational applications is growing rapidly day by day, cyber security has become a global widespread issue. Due to the covid pandemic, everything is going on the web so it becomes important to know about cyber security assaults. A lot of research has been carried out for the determination of awareness of cybersecurity among school university students. Various learning strategies and procedures are developed to enlighten the students to be aware of cyber security in the modern teaching era during the covid pandemic. This paper aims to gather and highlight these techniques and methodologies in a solitary distribution. An in-depth study of these learning strategies paves the way for further planning and creation of new technologies by merging already existing techniques. Moreover, new Internet of Things (IoT), as well as machine learning tools and techniques can be embedded in the above strategies.**

***Keywords*: cyberattacks, cybercrimes, cybersecurity awareness, learning strategies, online teaching, 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 preliminary 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 got the second position in the top five cyberattacked countries in the year 2020 as per the report of Data Security Council of India (DSCI) [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 awareness [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 overlook 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 the awareness regarding cybersecurity in the modern teaching era.

2. Literature Review

Cybersecurity is the ability to protect and defend the use of cyberspace from cyber-attacks [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 bit 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

*Corresponding author: saritacs.rsh@gndu.ac.in

learning outcomes.

Jones et al. [15] conducted interviews with 44 cybersecurity professionals to identify the knowledge, skills, and ability 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 in 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 in the basic knowledge of cybersecurity and 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 years and 21 years. The results further show that the majority of the students lacked the 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, no effort was made to describe all these techniques and methodologies in a solitary distribution. The current paper aims to enlighten some previous methodologies and techniques designed by various researchers.

3. Methodology

Review methodology provides an overlook 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, 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 papers 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 papers 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 papers are related to the evaluation of cybersecurity awareness whereas the second category of paper 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 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?

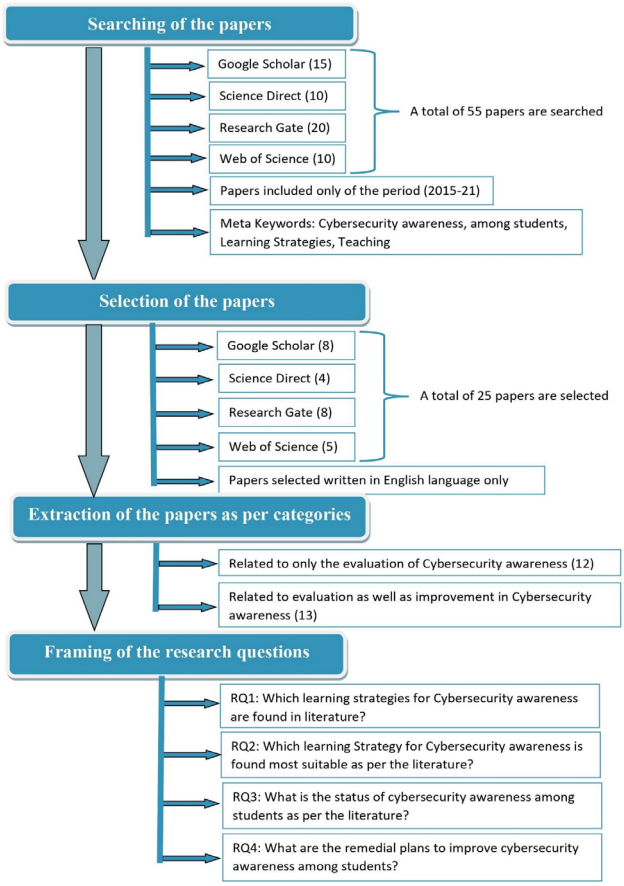

Fig. 1. Review methodology

4. Recent Learning Strategies Used for Cybersecurity Awareness

There exist various learning strategies for the evaluation as well as improvement of cybersecurity awareness.

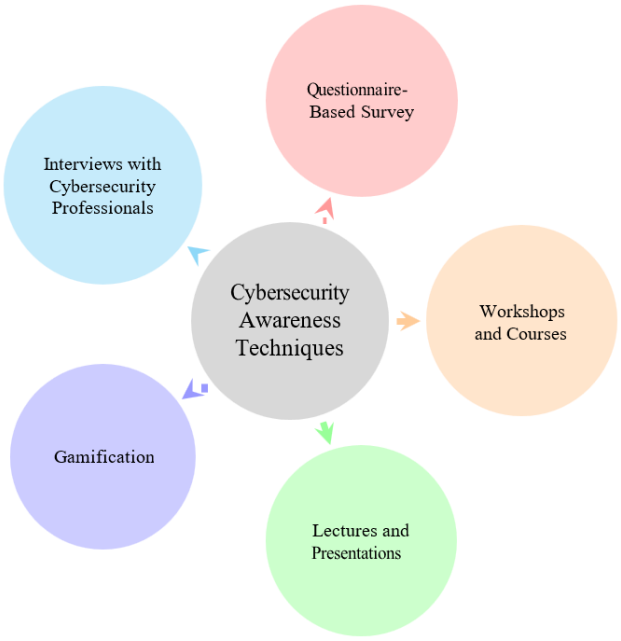

Fig. 1. Learning strategies for cybersecurity awareness

A. 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 con- ducted 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 the students of age between18-21 years. The questionnaire was related with awareness about the 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 on security bleaches sources [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].

B. Interviews with Cybersecurity Professionals

This methodological approach is the cybersecurity awareness improvement approach. This is the smart approach to finding the solutions to various issues related to cybersecurity. Jones et al. made use of interviewing approach [15]. This approach was based on cyber defense and helped determine what KSAs (knowledge, skills, and ability) 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 questions were concerned with the importance and learning of KSA. The open-ended questions were asked about the usage of cyber-related tools [15].

C. 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 some set of instructions and giving reviews about the game [5]. Through this learning method, the learner will be able to learn about how to deal with cyberattacks. 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 last 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].

D. Lectures and Presentations

Lectures and presentations 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 inspire them to identify and rectify such kinds of issues [8].

Table 1
Analysis of existing literature

RQ-ID	Research Question	Outcomes	Papers
RQ1	Which learning strategies for Cybersecurity awareness are found in literature?	To answer this research question, a total of 25 papers are selected in the period from 2015 to 2021. The papers are then analyzed to find the learning methods and techniques for cybersecurity awareness among students. During analysis, five learning strategies are found to evaluate as well as to improve cybersecurity awareness among students. These are Questionnaire-Based Survey, Interviews with Industry Experts, Gamification Approach, Lectures and Presentations, Workshops and Courses.	[27], [10], 11], [15], [4], [5], 13], 14], 12], [8], [2]
RQ2	Which learning Strategy for Cybersecurity awarenessis found most suitable as per the literature?	To answer this question, the results of selected studies are analyzed. As per theanalysis, Questionnaire-Based Survey Methodology is found more suitable only for the evaluation of cybersecurity awareness among students. Although, the majority of researchers utilized the Gamification approach, hence, this is found as the most suitable learning strategy for the evaluation as well as the improvement for cybersecurity awareness among students.	[4], [5], [13], [14]
RQ3	What is the status of cybersecurity awarenessamong students as per the literature?	During the analysis of related studies, it is found that the level of cybersecurityawareness among students is very poor and no or very less awareness programs for cybersecurity are conducted by universities and organizations to aware the students about cybersecurity.	[6], [19], [23], [16], 26], 27], [11], [22], [7], [20]
RQ4	What are the remedial plans to improve cybersecurity awareness among students?	A lot of remedial suggestions are found during the review of past studies: awareness programs by each university and organization should be developed time to time, improvement in the training content and certification courses, design and development of methods for creating better as well as more interesting cyber games, and more effective hands-on practice in the field of cybersecurity through training. Moreover,a new learning strategy can be created by embedding new IoT as well as machine learning tools and techniques in all the above strategies.	[27], [11], [5], [8], [9]

E. 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 some 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 way 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].

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.

6. Conclusion

Cybersecurity has become the major issue in the digital cyber world as it is safeguarding the security and privacy of the data and computer system itself. It is necessary to beware of cyberattacks and also about how to prevent sensitive information from these cyber threats. As per the studies reviewed, the cybersecurity awareness among the university students is at 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 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. A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes,* 2015.

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

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

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

[5] Čeleda, P., Vykopal, J., Švábenskỳ, V., and Slavíček, K. Kypo4industry: A testbed for teaching cybersecurity of industrial control systems. In *Proceedings of the 51st ACM TechnicalSymposium on Computer Science Education*, pp. 1026–1032, 2020.

[6] Chandarman, R. and Van Niekerk, B. Students' cybersecurity, awareness at a private tertiary educational institution. *The African Journal of Information and Communication*, 20:133–155, 2018.

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

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

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

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

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

[12] Gupta, M., Mittal, S., and Abdelsalam, M. (2020). Ai assisted malware analysis: A course fornext generation cybersecurity workforce. *arXiv preprint arXiv:2009.*11101, 2020.

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

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

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

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

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

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

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

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

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

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

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

[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*, pp. 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)*, pp. 223–228. IEEE.