Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 3 Issue 2 (2023)

Cybersecurity Awareness in Digital Classrooms: An Emerging Pedagogical Priority

Dr. Kamlesh Dhull
Assistant Professor, Vaish College of Education Rohtak

Abstract

New learning forms have come about because of the new technologies that have entered the learning landscape. The advent of digital technologies has transformed the education landscape, converting familiar classrooms into vibrant setting environments where digital technology is a key part of teaching and learning. The use of online learning platforms, cloud-based educational tools, virtual classrooms, and collaborative applications have greatly improved the accessibility, flexibility, and student engagement. This digital shift has also facilitated users to be targeted by cyber security issues like phishing, data breach, identity theft, malware infection and unauthorized access and cyber bullying. In an era of electronic learning, the need to raise cybersecurity awareness has become a key pedagogical requirement to create a safe and secure learning setting.

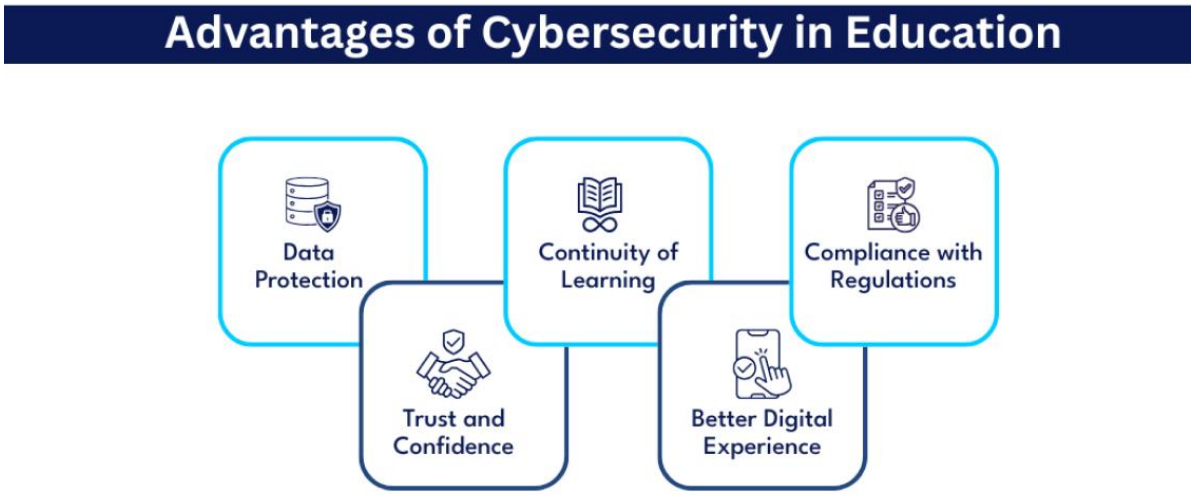
This paper discusses the importance of Cybersecurity Awareness in the digital classroom and the part that teachers, students and institutions can play in making this digital classroom safer. The paper brings to the fore the growing threats to the internet education system and stresses the need to make education a safe space for discussions on cyber security. It contains key aspects of cyber security literacy such as the security of passwords, privacy of personal information, safe use of the internet, digital citizenship and information security and responsible online behaviour.

Existing cybersecurity education barriers are also discussed, such as the lack of digital literacy, training programs, knowledge and awareness programs and evolving cyber threats. Using the best available literature and current educational practices, the study recommends areas for supporting the development of cybersecurity awareness by integrating awareness into the curriculum, teacher training, creating policies, running awareness campaigns, and establishing technology-based security measures. The findings show that in addition to the traditional ICT skills, the competence to address cybersecurity should be included in the digital skills toolkit. By informing our learners and school community about cyber security, they and our schools remain safe from potential threats and are empowered to engage safely and responsibly in a highly connected digital world. The study concludes that the embedding of cybersecurity into the educational setting is essential in creating a resilient and secure digital learning environment in the 21st Century.

Keywords: Cybersecurity Awareness, Digital Classrooms, Cyber Safety, Information Security, Digital Learning, Online Education, Data Privacy, Cyber Threats, Digital Citizenship, ICT in Education, E-Learning Security, Cyber Hygiene, Educational Technology, Safe Internet Practices, Digital Literacy.

Introduction

Learning environments are becoming more dynamic than classroom classrooms with the use of Information and Communication Technology (ICT) in the teaching and learning process at an astonishingly fast pace. The use of online learning platforms, cloud-based educational resources, virtual classrooms, learning management systems (LMS), and mobile apps has greatly improved the accessibility, flexibility, and effectiveness of the teaching and learning process. Technology was an important part of education during the COVID-19 pandemic, accelerating the process of digitalization of learning.



Source: *https://www.academikamerica.com/blog/digital-learning-and-its-risks-the-role-of-cybersecurity-in-edtech*

The advantages of digital classrooms to education are numerous, but along with these benefits, there are numerous cybersecurity risks associated with a digital classroom environment that affect students, educators, and educational institutions. But cyber incidents such as phishing, malware attack, ransomware attack, identity theft, unauthorized access, data breach, cyberbullying and privacy violations have become commonplace in educational contexts. There is a concern for privacy and the security of data as a result of the huge volume of data gathered and stored online, personal, academic and behavioural.

Cyber Security Awareness - Knowledge, skills, attitudes and practices which will enable a person to recognize, avoid, and respond to cyber security threats. Raising awareness about cybersecurity is a new challenge for schools, and not only from a technical point of view, but also from a pedagogical one. Students and teachers do not always use digital tools appropriately, and do not understand good online safety habits, safe password habits, data privacy, digital ethics, and measures to mitigate cyber risk. This lack of knowledge leaves schools vulnerable to cyber incidents that may have an impact on learning experiences and on sensitive information.

With the continuous development of the education field, the digitalization of education has heightened the awareness of educators and students on cybersecurity, and the necessity of integrating cybersecurity into the teaching and learning process has grown. Educators are key

players in shaping responsible digital citizens by providing students with skills to safely and ethically use digital environments. Furthermore, the value of cybersecurity education in the twenty first century is gaining in recognition by the education administration and policy makers.

In this context, the current study will delve into the cybersecurity awareness situation in digital classrooms, as a new educational priority. The study explores the significance of Cyber Security Literacy in education, the substantial threat schools encounter in their digital learning spaces, and the measures for developing a Cyber Security awareness amongst student and teachers. Recognizing these concerns, schools can create a safer and more secure digital learning environment that prepares learners and educators for successful learning and teaching in the digital era.

Background of the study

With the tremendous development of Information and Communication Technology (ICT) in the field of education, digital classrooms are now implemented in schools, colleges and universities all over. Online learning solutions, such as cloud-based education resources, virtual classrooms, learning management systems (LMS), mobile learning apps, and other tools have revolutionized education by providing increased access, flexibility, and effectiveness. With the onset of COVID-19 and the rapid shift towards digital learning, the use of technology led learning environments has further increased and digital classrooms are today part of the learning environments.

All the opportunities brought by digital transformation are complemented by cybersecurity challenges for teaching and learning. Internet connected devices and digital applications increasingly become an important source of information and knowledge for pupils, teachers and educational institutions to access, share and purchase in relation to the school. As technology becomes more of a necessity, school stakeholders have faced a number of cyber threats, such as phishing attacks, malware infections, ransomware attacks, identity theft, data breaches, cyberbullying, and unauthorized access to sensitive information. With all these personal and academic data, educational institutions are emerging as prime targets for cybercrime.

Cybersecurity awareness is defined as knowledge, attitudes and actions that enable individuals to identify, avoid and appropriately respond to cyber risks. Cybersecurity awareness is extremely important in digital classrooms not only for safeguarding institutional data, but for establishing a safe and secure learning environment. Students can be subject to cyber attacks and privacy breaches while utilizing online services without understanding of cyber security threats. Similarly, teachers may not be properly trained in cyber security practices, affecting the security of cyber learning systems.

The preparedness for cybersecurity is especially important in the context of the use of new technologies in education, such as artificial intelligence, cloud computing, Internet of Things (IoT) devices, and collaborative online tools. Cybersecurity is increasingly a pedagogical challenge that impacts not only on how teachers teach and teach effectively, but how students learn, how to keep them safe online and how they behave with technology.

Cybersecurity awareness needs to be considered a relatively new pedagogical priority and cyber security education needs to be integrated to teaching/learning. Encouraging responsible use of the internet, building digital resilience and creating safe learning environments

requires that the student and the teacher knows how to be cyber secure. Digital literacy and cyber security skills are featured prominently in national educational policies and frameworks worldwide, reflecting their importance as key skills for the 21st century.

In this regard, the present research investigates the awareness and concerns of cybersecurity in digital classrooms and its emerging importance as a teaching and learning priority. It aims to gain insights into the problems, opportunities, and pedagogical approaches for raising awareness about cybersecurity among students and teachers to help build safer and more resilient digital learning communities.

Justification

Education has recently undergone a paradigm shift as digital technologies have increasingly found their way into the classroom, changing the face of education into a highly connected digital learning space. The adoption of online learning systems, cloud based learning resources, mobile learning applications, virtual classrooms and learning management systems have vastly improved teaching and learning. This digital revolution, however, has also introduced several risks to educational institutions, teachers, and students in the cybersecurity sector, such as phishing attacks, data breaches, identity theft, malware infections, cyberbullying, and breaches of sensitive information.

Digital classrooms are often the setting for students to share personal and academic information as well as institutional data with digital platforms, many of which they may not know how to use safely and securely. The security of digital resources and safe online learning experiences are also a challenge for teachers and educational administrators. Many stakeholders in the education sector are exposed to cyber risks due to limited awareness on cybersecurity, even when digital technologies are increasingly becoming part of everyday life.

Cybersecurity education has become even more important as remote and hybrid education has become the norm, with digital devices and internet-based communication playing a vital role in the learning process. There is a growing awareness of the need for cybersecurity as a not only a technical but a pedagogical issue, which can be addressed systematically in the educational process. Creating a student population with cyber security awareness can help build the qualities of responsible digital citizenship, safe online practices and effective risk management skills, which are critical in today's digital world.

Furthermore, national policies in education and international education programs are focused on digital literacy and the responsible use of technology. However, few studies have examined the characteristics of cybersecurity knowledge in digital classrooms, as well as how the knowledge translates into the educational effectiveness, safety, and resilience of a school. This presents a large gap in the existing literature that needs to be addressed by research.

Thus, this study is justified because it aims to analyze the level of cybersecurity awareness in digital classrooms, identify the existing challenges and propose ways for the inclusion of cybersecurity education in pedagogical practices. The study results will be used in educational policy making, curriculum development, teacher training and institutional cyber-security. Finally, the research will help develop safer, more secure and digitally responsible learning environments that can respond to the challenges of cybersecurity in the twenty first century.

Objectives of the Study

1. To explore the cybersecurity awareness of students and educators in digital classroom setting.
2. To discover the most significant threats and risks faced in online learning and teaching in the context of cybersecurity.
3. To demonstrate the impact of Cybersecurity Education on Safe Digital Learning.
4. To assess the preparedness of educational institutions to tackle cyber security issues in virtual classrooms.
5. To evaluate current cyber security policies, guidelines and training programs for educational institutions.

Literature Review

Education is quickly digitalizing and moving the traditional classroom into a technology-enabled learning environment. While digital classrooms provide enhanced accessibility, collaboration, and flexibility, they also expose students and educators to various cybersecurity threats such as phishing, malware attacks, identity theft, data breaches, and cyberbullying. Hence, the awareness creation on cybersecurity has become a key pedagogical issue in modern education.

Tversky and Kahneman (1974) emphasized that people make decisions using rules of thumb and heuristics and that cognitive biases can make them more vulnerable to cyber threats. Their work serves as a theoretical framework of the vulnerability of human beings in digital environments.

Aldawood and Skinner (2019) did a literature review of cybersecurity awareness and social engineering training programs and concluded that human factors are one of the weakest links in cybersecurity frameworks. It is important that they promote awareness education and not training programmes on a one-off basis, the authors said.

The systematic review of literature on cybersecurity education, which was carried out by the authors of the papers Švábenský, Vykopal and Čeleda (2019), revealed that cybersecurity education is gradually becoming a vital part of educational programmes. They observed that there is an increasing need to incorporate a technical as well as human-centric approach of cyber security into learning environments.

Alqahtani and Kavakli-Thorne (2020) found that AR-based cybersecurity learning activities increased the engagement and knowledge of the cyber risks among the learners. Their results indicated that students' cybersecurity awareness can be improved by using interactive learning approaches.

The purpose of a systematic review of the literature conducted by Khando et al. (2021) was to examine the relationship between information security awareness and security behaviors of users, with the aim of identifying positive effects of information security awareness building efforts. The research highlighted the need for structured campaigns about cybersecurity awareness programmes to lower cybersecurity risks for students and staff in educational institutions.

Quayyum, Cruzes and Jaccheri (2021) explored cybersecurity awareness programmes for children and found that cybersecurity education should be age appropriate to ensure children

are taught to behave safely online from an early age. Their research brought to the forefront the need to include cybersecurity awareness in curriculum.

In their study, Alsulami et al. (2021) examined the awareness level of social engineering threats in educational institutions, and found that even though students were exposed to digital technologies on a regular basis, they did not know much about the social engineering threats. The authors called for specific cyber awareness campaigns in the educational environment.

In the era of data-driven digital economy, Awareness had been redefined by Akter et al. (2022) by incorporating both behavioral competencies and risk perception. The report highlighted cybersecurity awareness is now an important aspect of digital literacy.

Fauzi et al. (2022) evaluated the effectiveness of different types of cybersecurity awareness training and concluded that interactive training styles and simulation-based training styles are more effective in enhancing cybersecurity behaviour compared to traditional lecture-based training.

The recent research on smart learning environments by Hwang et al. (2020) and other studies highlighted the growing importance of cybersecurity awareness of both teachers and students in order to ensure safe digital learning experiences.

Dimitriadou and Lanitis (2023) reviewed the concept of smart classrooms and the new educational technologies, noting that one of the major problems affecting the use of technologies in educational spaces is cybersecurity and data privacy. The authors emphasized the need for cybersecurity awareness in digital pedagogy.

In a systematic review of cybersecurity education in the K-12 sector, Ayeyemi (2023) discovered that cybersecurity is becoming a part of the school curriculum around the globe. The review highlighted the need to educate young learners at an early age about cyber safety so that they can become digital citizens.

Kraus et al. (2023) assessed the effectiveness of a cybersecurity awareness course at the university level and found that students had increased knowledge, attitudes, and security practices after taking the course. The research showed that a structured cybersecurity education program was effective in fostering learners' secure digital practices.

Al-Hamar (2023) highlighted the different modern approaches in Cybersecurity training, noting that while passive learning was effective, hands-on cybersecurity activities, simulation exercises and experiential learning yielded better learning outcomes. Among the key findings of the study was the increasing importance of "active learning" in cybersecurity education.

Sodikin and Hikmawan (2023) investigated the impact of gamification on the learning of cybersecurity, and they determined that the use of game-based learning had a significant effect on enhancing the cybersecurity knowledge retention of students. The results of their research come with the recommendation to implement innovative pedagogies in cybersecurity awareness education.

Shakela and Gamundani (2023) analyzed the cybersecurity awareness platforms and found that today's awareness efforts are largely focused on digital, interactive and user-centred strategies. They recognized that there was a need for adaptive awareness platforms that could respond to a changing cyber threat landscape in the education context.

Alnajim et al. (2023) have undertaken a comprehensive study on cyber security educational and training methods, and discovered that VR technologies, AR, and immersive learning techniques have great potential to improve cyber security awareness and skill building.

Malele (2023) analyzed the cybersecurity problems in online learning that relies on cloud technologies and found that the use of cloud technologies in education is on the rise, requiring educators and learners to be more aware of the cybersecurity risks. This study highlighted the role of cyber security literacy in online learning environments.

Mou et al. (2023) conducted a review of human cybersecurity behavior studies and identified a number of significant factors that affect safe online behavior: behavioral intention, risk perception, and cybersecurity awareness. The study highlighted the need for a focus on behavioural considerations in cybersecurity education.

Material and Methodology

Research Design:

In this study, the research design was a descriptive and analytical research.The descriptive and analytical research was used in this study to analyze the level of cybersecurity awareness in the digital classroom and its increasing importance as a pedagogical priority. The study focused on the knowledge, attitudes and practices of students and teachers on cybersecurity in technology-enabled learning environment. The mixed-method approach was adopted to gain a quantitative and qualitative insight into readiness for cyber security education in educational settings. The study covered the current trends and developments of digital education until 2023, such as the growing number of online learning platforms, cloud-based educational tools and virtual classrooms.

Data Collection Methods:

In the study both primary and secondary data sources were used. The collection of primary data was done using the students' and teachers'/education administrators' regularly used digital learning platforms, based on structured questionnaire. The questionnaire included questions on password protection, online privacy, awareness of phishing, cyber hygiene and attitudes towards cyber risks in education. Additionally, teachers were informally interviewed, and discussed to understand the challenges and best practices related to cybersecurity in digital classrooms on a qualitative scale. The secondary data gathered included peer reviewed journal articles, government reports, policy documents, conference proceedings, publications in the field of educational technology, cyber security frameworks and reports from international institutions such as UNESCO, OECD, and cyber security agencies since 2023. These sources allowed an overall picture of the trends in cybersecurity awareness and cybersecurity educational responses to be gained.

Inclusion and Exclusion Criteria:

This study engaged stakeholders who actively engage in the digital learning environment, such as students at the school level, college level, teachers, and academic leaders who are involved with online education platforms by 2023. Relevant articles from research journals, reports and policy documents were read, in English language and directly pertinent to cybersecurity awareness, digital education, cyber safety practices and technology enhanced learning. The research papers which were not directly related to the Cybersecurity Awareness in educational environment were not included in the study. Publications which cannot be

substantiated and evidences by empirical research and duplicate research works are not included to ensure the relevance and quality of the research.

Ethical Considerations:

Ethical standards were followed throughout the process of data collection and analysis in the research. No pressure or bias was placed upon any student in the primary school to participate in the survey and informed consent was sought from all students in the primary schools before the data were obtained. Participants were assured that their personal information and identity would be kept confidential and for educational purposes. The study does not reveal any sensitive personal or institutional data. Secondary sources are referenced and cited appropriately with regard to academic integrity and to ensure there is no plagiarism. This research tried to keep a focus on the objectivity, transparency, and respect of the privacy of participants in the study, as well as examined the practices of cybersecurity awareness in digital classrooms up to the year 2023.

Results and Discussion

Table 1: Demographic Profile of Respondents (N = 250)

Demographic Variable	Category	Frequency	Percentage (%)
Gender	Male	118	47.2
	Female	132	52.8
Educational Level	Undergraduate	95	38.0
	Postgraduate	85	34.0
	Faculty Members	70	28.0
Digital Classroom Usage	Less than 1 year	42	16.8
	1–3 years	106	42.4
	More than 3 years	102	40.8

Interpretation

According to the demographic data, there were slightly more females (52.8%) than males (47.2%). The majority had more than one year of experience in digital classrooms, and thus had some experience of exposure to digital learning environments and cybersecurity related problems.

Table 2: Level of Cybersecurity Awareness Among Respondents

Awareness Level	Frequency	Percentage (%)
High	72	28.8

Awareness Level	Frequency	Percentage (%)
Moderate	118	47.2
Low	60	24.0
Total	250	100

Interpretation

Few respondents (28.8%) showed high cyber security awareness, and nearly half (47.2%) showed moderate cyber security awareness. The results suggest that there is a big demand for Cyber Security education programs in Digital Learning environments.

Table 3: Awareness of Common Cybersecurity Threats

Cybersecurity Threat	Aware (%)	Not Aware (%)
Phishing Attacks	82.4	17.6
Malware	76.8	23.2
Identity Theft	69.2	30.8
Ransomware	58.4	41.6
Data Breaches	74.0	26.0

Interpretation

The most widely known threat was phishing (82.4%) and the second most widely known threat was malware (76.8%). Educational institutions have less awareness of ransomware (58.4%), indicating that they must pay more attention to the new cyber risks.

Table 4: Cybersecurity Practices Followed by Respondents

Practice	Always (%)	Sometimes (%)	Never (%)
Use Strong Passwords	62.0	31.6	6.4
Enable Two-Factor Authentication	44.8	35.2	20.0
Update Software Regularly	55.2	33.6	11.2
Verify Unknown Links	71.6	22.4	6.0
Use Secure Networks	66.8	24.4	8.8

Interpretation

The majority of respondents scanned unknown links before clicking (71.6%) and used secure networks (66.8%). However, there was a disparity between cyber security practices and awareness as only 44.8% reported using two factor authentication always.

Table 5: Perceived Importance of Cybersecurity Education in Digital Classrooms

Response	Frequency	Percentage (%)
Strongly Agree	108	43.2
Agree	92	36.8
Neutral	32	12.8
Disagree	12	4.8
Strongly Disagree	6	2.4

Interpretation

80% of the respondents agreed or strongly agreed the digital classroom pedagogy should include cybersecurity education. This underscores the increasing importance of cyber security in today's education.

Table 6: Challenges Faced in Maintaining Cybersecurity in Digital Classrooms

Challenge	Mean Score	Rank
Lack of Cybersecurity Training	4.31	1
Limited Awareness of Emerging Threats	4.18	2
Weak Password Practices	3.95	3
Inadequate Institutional Policies	3.87	4
Use of Unsecured Devices	3.72	5

(5-point Likert Scale: 1 = Strongly Disagree, 5 = Strongly Agree)

Interpretation

Limited awareness of emerging threats (Mean = 4.18) and lack of cybersecurity training (Mean = 4.31) were the two most important challenges. The outcomes indicate a need for teacher and student cybersecurity education formal programs.

Discussion

The results reveal that the respondents possess moderate level of knowledge about cybersecurity concepts but they have knowledge gap and practice gap. The lower awareness of ransomware and advanced threats suggest that there's a need for more comprehensive

cybersecurity education while the higher awareness of phishing suggests that phishing isn't a hidden threat, but readily observable in an educational setting.

The results also indicate that respondents understand the importance of cybersecurity, but lack a consistent practice of following security best practices, such as using two-factor authentication. This lack of knowledge and behaviour aligns with previous studies showing that changing from awareness to safe online behaviour is challenging.

Another significant finding of the study is that the lack of training constitutes the main obstacle for digital classrooms to be prepared in the field of computer security. With the increase in the use of digital learning platforms in the field of education, cybersecurity awareness should be integrated into curriculum planning, teacher training, and orientation programmes for students in recent years.

In general, the results confirm that cybersecurity awareness is not just a technical problem anymore, but a key pedagogical issue. Awareness workshops, simulated phishing, modules on cyber security in the academic curriculum and policy frameworks to foster safe learning environments for institutions should be put in place.

Limitations of the study

The present study entitled "Cybersecurity Awareness in Digital Classrooms: An Emerging Pedagogical Priority" has certain limitations that need to be taken into consideration when interpreting the findings of the present study. Firstly, the findings of this research are not generalizable as the geographic location of the study and the sample size does not cover the various educational institutions, teachers and learners of the several regions. Second, the data used in the research is self-reported data gathered from questionnaires and interviews with some respondents who may suffer from perceptional, memory or social desirability bias. Thirdly, threats and technologies are constantly changing, meaning that awareness, security and education might also evolve over time and may have long-term implications on the applicability of results. Fourth, educational institutions may have different digital infrastructures and Internet connectivity, as well as technology resources and other elements that influence awareness of and readiness for cybersecurity in all learning environments. Also, the study is not focused on technical assessment of the cyber security skills or weaknesses of the systems, but more on an awareness and perceptions study. Lastly, the scope of the data collection and analysis could have been constrained by time, resources and access to participants. However, the results of this study offer important insights for the increasing significance of cybersecurity education and the need for embedding cybersecurity awareness into digital teaching and learning.

Future Scope

The emergence of digital technologies, online learning platforms, artificial intelligence, cloud and IoT devices in education has made cybersecurity awareness a key concern in digital classrooms. Further studies are needed to develop in-depth cybersecurity programs for students at various educational stages, ranging from primary schools to universities and colleges. Research can also explore how well gamified learning, virtual simulations and AI-powered training can improve students' understanding of cybersecurity and good online practice.

Research can be conducted to explore how teachers, school administration, and parents can contribute to a cyber-safe learning environment. Cross-regional, cross-institutional and cross-country analysis can offer lessons about good practice in cyber security education and policy. Furthermore, new trends like ransomware attacks, phishing and identity theft, cyberbullying, deepfake technologies and data privacy issues in the education environment could also be explored in future studies.

The rapid development of educational technologies and the use of smart classrooms, learning management systems, mobile learning applications, and cloud-based educational platforms brings to the forefront the issues related to their potential impact on cyber security. Longitudinal studies can assess the long-term effectiveness of cybersecurity awareness initiatives on students' e-literacy, online safety habits, and responsible online behavior. In addition, future academic research in the field of cybersecurity awareness in national education policies and teacher training is a substantial arena.

Furthermore, future research could create predictive models and evaluation systems to gauge students' and teachers' cybersecurity preparedness. The field of education, information technology and psychology and cybersecurity could be merged to support the creation of resilient digital-learning environments that will ensure safe, secure and sustainable experiences in the digital age.

Conclusion

Digital technologies have developed quickly and are an integral part of classroom learning and teaching with greater access, flexibility and personalisation of learning. At the same time, the transition to the digital environment has increased the likelihood of cyber incidents such as data breaches, phishing, malwares, identity theft, and unauthorized access to the learning management system. The era of using digital tools has increased educators' and students' need to be cybersecurity-aware, making cybersecurity more of a pedagogical priority than a technical one.

It also highlights the need for responsible digital citizenship and for the safe use of education technologies, supported by effective cybersecurity education. Raising student, teacher and educational administration cyber risk awareness is a significant step towards reducing cyber risks and enhancing the security culture within education institutions. Creating safe digital learning environments is essential, which starts with fostering a cybersecurity culture, incorporating cybersecurity principles into classrooms, regularly training on cybersecurity issues, transitioning to safe online practices and implementing cybersecurity policies in the institution.

It is also important to have collaboration and synergy between the different actors—ranging from policy makers and education institutions, to technology providers and cyber security experts—in order to face the new challenges of cyber threats and to support sustainable digital education. Since technology is always changing and becoming a powerful influence in the learning and teaching process, it should be incorporated into the educational curriculum planning and pedagogy with a focus on cybersecurity awareness. This way, schools can create a secure, safe and forward-looking online classroom environment that promotes academic development and online safety.

References

1. Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., & Shamshirband, S. (2022). Cybersecurity awareness in educational institutions: Challenges and strategies for digital learning environments. *Education and Information Technologies, 27*(6), 8157–8178. https://doi.org/10.1007/s10639-022-10947-3
2. Alsmadi, I., & Zarour, M. (2020). Cybersecurity awareness among students in higher education institutions. *International Journal of Information and Education Technology, 10*(8), 581–586. https://doi.org/10.18178/ijiet.2020.10.8.1430
3. Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley.
4. Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society*, 118–131.
5. Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*. Prentice-Hall.
6. Choucri, N., Madnick, S., Ferwerda, J., & Vercelli, A. (2018). Cybersecurity education and awareness in digital societies. *Information Systems Frontiers, 20*(4), 789–802. https://doi.org/10.1007/s10796-017-9754-2
7. Chugh, R., Grose, R., & Macht, S. (2020). Social media usage and cyber safety awareness among students. *Education and Information Technologies, 25*(2), 1389–1406. https://doi.org/10.1007/s10639-019-10016-5
8. Dey S. M. (2021). Psychosocial stress contagion of COVID-19: issues and intervention channels. Ensemble SP-1, 44–53. https://doi.org/10.37948/ensemble
9. Dey, S. M. Women & children trafficking in Bangladesh: A historical significance & current challenges
10. Dey, Sourav (2012). "Discursive Self in Consumption: Body, Fluidity, and Femininity". Global Media Journal, Indian Edition 3 (1), pp. 1-12.
11. European Union Agency for Cybersecurity (ENISA). (2021). *Cybersecurity education initiatives and best practices*. ENISA Publications.
12. Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security, 31*(8), 983–988. https://doi.org/10.1016/j.cose.2012.08.004
13. Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346
14. International Telecommunication Union. (2020). *Child online protection guidelines*. ITU Publications.
15. Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005
16. Joinson, A. N., Reips, U. D., Buchanan, T., & Paine Schofield, C. B. (2010). Privacy, trust, and self-disclosure online. *Human–Computer Interaction, 25*(1), 1–24. https://doi.org/10.1080/07370020903586662
17. Kaspersky. (2022). *Cybersecurity and digital learning: Protecting students in connected classrooms*. Kaspersky Research Reports.

18. Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*(4), 289–296. https://doi.org/10.1016/j.cose.2006.02.008
19. Livingstone, S., Davidson, J., Bryce, J., Batool, S., Haughton, C., & Nandi, A. (2017). *Children's online activities, risks and safety*. London School of Economics and Political Science.
20. N. BN, D. E. Geetha and R. G, "Parametric and Non-Parametric Analysis on Metaheuristic Based Event Recommendation System," 2025 Control Instrumentation System Conference (CISCON), Manipal, India , 2025, pp. 1-10, doi: 10.1109/CISCON66933.2025.11337415.
21. N. BN, S. B. Murthy and S. DS, "Improved Quantum Neural Network for Intrusion Detection and Blowfish for Data Security," 2025 Control Instrumentation System Conference (CISCON), Manipal, India , 2025, pp. 1-9, doi: 10.1109/CISCON66933.2025.11337273.
22. NIST. (2020). *National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework*. National Institute of Standards and Technology.
23. Nithya BN, Hemanth Uppala,.(2026). Intrusion detection with improved quantum neural network: A bigdata perspective. Future Generation Computer Systems, Vol-175. DOI: https://doi.org/10.1016/j.future.2025.108102
24. OECD. (2021). *Digital education outlook 2021: Pushing the frontiers with AI, blockchain and robotics*. OECD Publishing.
25. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003
26. Pusey, P., & Sadera, W. A. (2011). Cyberethics, cybersafety and cybersecurity: Preservice teacher knowledge and preparedness. *Journal of Digital Learning in Teacher Education, 28*(2), 82–85.
27. Richardson, J., North, M., & Smith, C. (2021). Cybersecurity awareness and online learning: Implications for educational institutions. *Journal of Information Technology Education: Research, 20*, 301–320.
28. Riek, M., Bohme, R., & Moore, T. (2016). Measuring the influence of cyber security awareness campaigns. *Proceedings of the Workshop on the Economics of Information Security*, 1–15.
29. SANS Institute. (2021). *Security awareness planning kit*. SANS Security Awareness Publications.
30. UNESCO. (2023). *Guidance for generative AI in education and research*. UNESCO Publishing.
31. Von Solms, B., & Van Niekerk, J. (2013). From information security to cybersecurity. *Computers & Security, 38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004
32. Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security* (7th ed.). Cengage Learning.
33. Williams, P. A. H., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in digital learning environments. *Educational Technology & Society, 18*(3), 220–233.
34. Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs, 43*(3), 389–418. https://doi.org/10.1111/j.1745-6606.2009.01146.x

35. Zaeem, R. N., & Barber, K. S. (2020). The effect of cybersecurity awareness on digital privacy and security behavior. *IEEE Security & Privacy, 18*(3), 46–54. https://doi.org/10.1109/MSEC.2020.2975600
36. Zeng, E., Mare, S., & Roesner, F. (2017). End user security and privacy concerns in educational technology systems. *Proceedings on Privacy Enhancing Technologies, 2017*(4), 72–91. https://doi.org/10.1515/popets-2017-0040