INNOVATIVE RESEARCH ORGANISATION
International Journal of Advance Research in Education, Technology & Management
(Scholarly Peer Review Publishing System)

Cyber Security Awareness among students: Challenges and Strategies for a Secure Digital Learning Environment

Sandeep Kumar

Assistant Professor and Head, Department of Defence and Strategic Studies

Sri Guru Tegh Bahadur Khalsa College, Sri Anandpur Sahib, Punjab, India

INTRODUCTION

The digital transformation of education has transformed the ways in which students study, communicate, access information, submit assignments, take examinations and interact with professors and institutions. The COVID-19 pandemic has hastened this transformation, but the trend to digital education has persisted post-pandemic. Educational methods are slowly being merged with online learning platforms, cellphones, cloud-based applications, learning management systems, digital libraries, virtual classrooms, educational films, online assessments, artificial intelligence technologies and social media. The growth of digital education offers enormous prospects. Students are able to take use of distance education resources, take part in virtual classes, collaborate with peers, connect with experts and use multimedia materials to better learning results. India's National Education Policy (NEP) 2020 acknowledges the need for technology in education and promotes digital learning, digital infrastructure, teacher capability, and technology-enabled educational ecosystems. In this sense, the Ministry of Education has encouraged initiatives connected to digital education such as the National Digital Education Architecture and the National Educational Technology Forum.

But digital schooling also brings new threats with its advantages. Students can be exposed to phishing, malware, identity theft, cyberbullying, disinformation, privacy breaches, online scams, account takeovers, and dangerous content, just to name a few, through the same devices and platforms that enable learning. Schools also hold large amounts of sensitive information, such as students' names, addresses, academic records, ID information, examination results, financial information and sometimes health-related or biometric information. This has made educational institutions a prime target for cybercriminals. That means cyber security is not simply an IT concern anymore. It is a matter of education, social, economic, ethical and national security issues. "The cyber-resilient citizen must be nurtured from the early days of education. Students who understand the fundamentals of cyber hygiene, privacy protection, responsible online activity, secure authentication, disinformation detection and incident reporting are better placed to protect themselves and help build a safer digital society. And this difficulty is much more significant because technology skill and cyber security competency are not the same. A student may be quite proficient in using smartphones, social media, online gaming, artificial intelligence or educational apps but have little understanding of phishing, password attacks, privacy threats, harmful links, social engineering or data exploitation. Cyber security awareness needs to be done through intentional education and continual reinforcement. UNICEF and UNESCO guidance on internet safety in school, due out in 2026, underscores a growing need to protect kids, teachers and parents in an environment increasingly shaped by artificial intelligence and developing digital technology. The warning highlights hazards related with digital learning applications, privacy, cyberbullying, inappropriate material, harmful contact and abuse of personal data.

Similarly, the Indian Computer Emergency Response Team (CERT-In), which works under the Ministry of Electronics and Information Technology, has developed awareness content for children and young users to learn about safe internet usage. Its Cyber Smart Kids Suraksha Guide guides kids to use the internet safely and securely.The present study consequently emphasizes on cyber security awareness among students and explores how educational institutions might develop a safe digital learning environment trough education, policy, technology and behavioral change.

INNOVATIVE RESEARCH ORGANISATION
International Journal of Advance Research in Education, Technology & Management
(Scholarly Peer Review Publishing System)

PROBLEM DESCRIPTION

The paradox of the increasing digitization of education is that it has created a dilemma: Students have access to information and communication technology as never before, yet their capacity to utilize these devices securely may not improve at the same speed. There are a couple of reasons behind this. Firstly, many students feel that cyber security is simply a technical subject for computer professionals. Secondly, the cyber safety education is generally done through periodic awareness campaigns rather than methodically included in the curriculum. Thirdly, teachers themselves may need to be trained further on new cyber hazards. Fourth, students are likely to utilize several internet services, which make them rely on passwords, mobile applications, cloud platforms, social media accounts, and third-party services. Fifth, the rapid growth of generative AI, deepfakes, synthetic media, and sophisticated phishing techniques has made the digital space harder to navigate safely. The latest National Guidelines on Children's Online Safety in India highlight serious gaps in basic online literacy training on cyber safety, training of teachers on ICT and institutional policies. According to UNICEF India's recommendation for 2026, a mere percentage of schools have official cyber-safety programs and highlights the need for stronger policy implementation and capacity-building for teachers. And it's not only a technology problem. It is a failing of comprehensive cyber awareness and responsible conduct, institutional preparedness and resilience.

OBJECTIVES OF THE STUDY

The major purpose of this study is to investigate the significance of cyber security awareness among the students.

- Identify key cyber hazards faced by students in digital learning environments.
- To explore the behavioral and technological issues affecting vulnerable students.
- To find out the role of teachers, parents, educational institutions and government organizations in enhancing cyber awareness
- To analyze the importance of cyber security education in emerging digital education system of India. To offer measures for a safe and cyber robust digital learning environment;

A pragmatic approach for integration of cybersecurity awareness in educational institutions. Research Questions This research attempts to answer the following research questions:

RQ1: What are the major cyber security dangers in digital learning environments for students?

RQ2: Why is familiarity with technology not necessarily the same as understanding of cyber security?

RQ3: How can teachers and educational institutions build cyber-resilient students?

RQ4: How to integrate cyber security awareness into mainstream education?

RQ5: What institutional and policy initiatives may be implemented for a safer digital learning environment?

METHODS

The study is qualitative and exploratory in character and is based mostly on secondary data. It does not purport to set forth the results of a survey of primary schoolchildren. Instead, it brings together relevant scholarly research, government regulations, institutional recommendations, international guidelines and cyber security awareness tools.

The main sources reviewed are publications and policy documents of the Government of India, Ministry of Education, CERT-In, University Grants Commission (UGC), UNICEF, UNESCO, and International Telecommunication Union (ITU). In addition, relevant academic literature surrounding cyber security awareness, internet literacy, online safety, and educational technology has been reviewed. The UGC has a Handbook on Basics of Cyber Hygiene for Higher

INNOVATIVE RESEARCH ORGANISATION
International Journal of Advance Research in Education, Technology & Management
(Scholarly Peer Review Publishing System)

Education Institutions and a Syllabus of Cyber Security Course at Undergraduate and Post Graduate level, which indicates how cyber security has progressively infiltrated the higher-education policy and curriculum arena.

The research is organized into four analytical stages:

• Identification of threats to pupils in the internet environment

. • Recognizing behavioral and institutional vulnerabilities. Current educational and policy responses: A review.

• Develop a multi-layered cyber awareness framework. Findings are presented under the domains of technology, behavior, institution and education and policy by employing thematic analysis.

An additional shortcoming of the methodology is that cyber awareness is not measured by a primary survey or controlled experiment. Therefore, the results should be understood as an analytical and conceptual contribution and not as statistically generalizable evidence on a specific community of students. Conceptualization of Cyber Security Awareness Conceptualization of cyber security awareness is the knowledge of an individual about digital risks and ability to act correctly to prevent, detect and respond to cyber incident. Cyber security awareness for kids should address at least five dimensions: Knowledge: kids should know about the most frequent online hazards, including phishing, malware, ransomware, identity theft, social engineering, cyberbullying, bogus websites, fraudulent messages, and compromised accounts. Knowledge about Behavior needs to be transferred into safe behavior. Students should use strong, unique passwords, utilize multi-factor authentication, update their software, use secure networks, employ privacy controls and be careful what they post. Risk Recognition: Students should be able to recognize suspicious websites, unusual login requests, fake accounts, altered photographs, phony scholarship or career offers and misinformation. Awareness also entails understanding what to do when an incident arises. Response Capability: Students should know how to safeguard an account, preserve evidence, report an occurrence, warn teachers or parents and seek appropriate institutional or governmental aid. Ethical Digital Citizenship Cyber security should also encompass responsible online behavior. Students need to understand the social, intellectual, legal and ethical consequences of their actions in the digital world. So cyber awareness is more than just not acquiring viruses. It's a broader culture of safe, ethical, responsible and resilient digital behavior. Top Cyber Security concerns Facing Students Phishing and Social Engineering Phishing is one of the biggest concerns, because it exploits human behavior and not just technological vulnerabilities. Students may get fake messages that look like they are from educational institutions, banks, scholarship authorities, examination boards, universities, friends or social networking platforms. Attackers may try to create a sense of urgency by telling students that an account will be blocked, a scholarship will expire, an examination form is incomplete or an important document has to be downloaded. If the student clicked on a fraudulent link or entered credentials, the attacker may take over the account. Attackers exploit trust, curiosity, terror, authority and urgency, making social engineering very effective on the younger users. Weak and reused passwords Many students have lots of accounts. Password recycling is a major vulnerability. If a service is compromised, attackers may try the same username-password combination on other services. So, students should learn about: Unique passwords for important accounts. Use password managers, if applicable. Multi-factor authentication Lack of any simple personal information. If you believe your account has been hacked, reset your passwords immediately. Malware & Malicious Apps Students frequently download programs, games, software, papers, browser extensions and media files. Unknown apps can carry malware or spyware. The risk is higher when pupils switch off security safeguards, download pirated software or get programs from unapproved sources. **CERT-IN's CURRENT AWARENESS ADVISORY ADVOCATES SAFE DIGITAL BEHAVIORS AND PROVIDES SPECIALIZED RESOURCES FOR YOUNG USERS.** Cyberbullying & Online Harassment Cyberbullying can happen on social media, messaging applications, gaming platforms, discussion forums and educational groups. It may be threats, humiliations, impersonation, exclusion, dissemination of private information, edited photos or abusive communications. Cyber bullying is distinct from traditional bullying since it can occur outside of school or college hours and it can reach a large audience. Hence, it has the ability to influence the

INNOVATIVE RESEARCH ORGANISATION
International Journal of Advance Research in Education, Technology & Management
(Scholarly Peer Review Publishing System)

academic involvement, social ties and security of students. International child-online-protection frameworks recognize cyberbullying, harmful contact, inappropriate content and other kinds of online harm as important concerns requiring educational and institutional solutions. Data Protection & Privacy Digital schooling produces a great deal of data. Learning systems can collect names, attendance, assessment data, behavioral data, device data and other meta data. Students can also willingly disclose much more personal data through social media. Pictures, places, schools, phone numbers, email addresses and family members can be used in social engineering exploits. Hence, privacy education needs to be integrated into online literacy education. Disinformation and Misinformation Students are increasingly getting their information online and on social media. False information, deliberately produced, may be used to shape beliefs, make financial gains, cause social tensions, or ruin reputations. It is now possible for generative artificial intelligence to make convincing text, graphics, audio and video, complicating the situation. Therefore, pupils require both cyber security and media-literacy abilities. Artificial Intelligence Threats Artificial intelligence can help education, but it can also enable more sophisticated cyberattacks. Attackers may leverage artificial intelligence to craft convincing phishing messages, synthetic identities, automate social engineering or generate distorted media. The growing importance of AI-related cyber security threats was underlined by CERT-In's issuance of a recommendation for AI-assisted vulnerability exploitation for 2026. Students need to learn that sophisticated content is not always real content.

Table 1: Major Threats and Preventive Measures

Cyber Threat	Student Vulnerability	Potential Consequence	Preventive Strategy
Phishing	Clicking unknown links	Credential theft	Verify sender and URL
Weak passwords	Reusing passwords	Account compromise	Strong, unique passwords
Malware	Unsafe downloads	Device/data loss	Updated security software
Cyberbullying	Excessive social-media exposure	Psychological and social harm	Privacy controls and reporting
Identity theft	Sharing personal information	Fraudulent activity	Data minimisation
Fake websites	Trusting visual appearance	Financial/credential loss	Verify official websites
Misinformation	Poor source evaluation	Wrong decisions	Digital/media literacy
AI-generated deception	Trusting synthetic content	Fraud/manipulation	Verification and critical thinking
Public Wi-Fi risks	Unsafe connections	Data interception	Secure networks/VPN where appropriate
Data breaches	Weak institutional security	Exposure of student records	Institutional cyber controls

Why Being Tech-Savvy Isn't the Same as Being Cyber-Aware

The idea that all young people are 'digital natives' and thus cyber-safe is a common one, but it is problematic. Online literacy is frequently defined as the ability to operate gadgets and programs. But cyber security knowledge needs risk assessment and ethical actions

INNOVATIVE RESEARCH ORGANISATION
International Journal of Advance Research in Education, Technology & Management
(Scholarly Peer Review Publishing System)

. For example, a student may be very proficient in using Instagram, Youtube, internet games, cloud storage and AI applications, but still

: • Reusing the same password on different accounts;

• Clicking on links without verifying the sender;

• Publicly sharing personal information;

• Receiving contacts from unknown people;

• Downloading applications from untrusted sources;

• Not turning on multi-factor authentication;

• Trusting AI-generated information without checking it;

• Ignoring software updates, or

• Cyber incidents not reported

The difference between digital fluency and digital safety is therefore of critical importance. Education must transition from teaching students how to use technology to educating students how to use technology ethically and safely.

Cyber security and the Indian education system: India's educational revolution is increasingly relying on digital infrastructure. NEP 2020 emphasizes the value of technology enabled education along with difficulties including digital gap, teacher preparedness, limitations of infrastructure and the need for digital skills. It additionally emphasizes the need for cybersecurity as part of educational achievement. The UGC offers publication tools such as a cyber hygiene guidebook for higher education institutions and a cyber security course syllabus for undergraduate and post-graduate education. These changes indicate that cyber security needs to be tackled at multiple levels: School Level: Basic cyber hygiene, online safety, privacy, cyberbullying, misinformation and responsible use of social media. Higher Secondary Level: Advanced Concepts of Cyber Security, Ethical use of technology, Digital Identity, AI Safety, Cyber Crime Awareness, Principles of Incident Response. Undergraduate Level: Cyber hygiene, information security, privacy, cyber law, ethical hacking ideas, digital forensics knowledge and discipline-specific cyber dangers. Teacher Training Cyber safety, kid protection online, privacy, incident reporting, classroom technology management, appropriate use of AI How Teachers Can Contribute in Cyber Security Awareness

Teachers have an important role to play in building cyber-resilient children. They are frequently the first adults in schools to observe behavioral changes, suspicious activities online, cyberbullying or misuse of digital media. ,Good cyber hygiene , Social engineering and phishing attacks.

Teacher training should therefore include:

• Manage logins and passwords.

• Privacy of data

• Cyberbullying and internet harassment.

• safely using educational applications

• Deep fakes and falsehoods created by AI.

• Online citizenship.

• Incident reporting. Protection of children on-line.

INNOVATIVE RESEARCH ORGANISATION
International Journal of Advance Research in Education, Technology & Management
(Scholarly Peer Review Publishing System)

For example, the ITU's child-online-protection training emphasizes the role of educators and academic and non-academic personnel in making online educational environments safer. We shouldn't expect teachers to be cyber security engineers. They are responsible for raising awareness, modeling appropriate behavior, recognizing hazards, advising students and triggering institutional reaction mechanisms when necessary.

Role of Educational Institutions: Educational institutions need to be proactive in creating an institutional culture of cyber security rather than sporadic awareness campaigns. A comprehensive institutional approach should include: Cyber Security Policy: Every organization should have a clear policy on permissible use of technology, password strength, data security, social media conduct, incident reporting, and consequences of misuse.

Regular Awareness Programs: Cyber awareness should not be a once a year event, but it should be imparted throughout the year. Practical Training: Students are better able to learn about cyber safety when they practice identifying phony phishing communications, checking URLs, creating strong passwords, updating privacy settings and reporting suspicious behavior. Incident Reporting Mechanism: Provide an easy, confidential means for students to report cyberbullying, account compromise, fraud, harassment or suspicious activities. Technical Protection: Institutions should have systems that are up-to-date, secure Wi-Fi networks, access control, backups, authentication systems, endpoint security and enough monitoring.

Data Governance: Institutions should not gather data that is not essential and should ensure student information is handled securely and accessible appropriately. Parents and Families' Role: Cyber security education cannot end at the classroom door. Students utilize digital devices at home, in public and on the move. Parents need to create an environment where pupils feel safe to disclose faults. If kids fear punishment, they might hide things like clicking on a harmful website, chatting to someone they don't know, or experiencing cyberbullying.

Parents should promote:

• Open communication.

• Privacy-minded behavior.

• Device security is good.

• Be responsible on social media. Browsing the web.

• Report suspicious activity.

• Good and balanced digital habits.

UNICEF's online-safety resources emphasize the need of guiding children to interact with digital spaces securely and preserving open lines of contact with trusted adults.

Digital Citizenship and Cyber Security Awareness: Cyber security should be considered as an aspect of digital citizenship. Digital citizenship means responsible engagement in the digital society. This includes respecting people, privacy, ethics in communication, critical evaluation of information, comprehending intellectual property, responsible use of AI and safe use of the internet. Hence, a cyber-savvy learner must understand that: Connectivity is a privilege, Responsibility while connected is a requirement. Educational institutions should teach students to consume digital information, to critically analyze, ethically use, protect and responsibly generate digital information. Cyber Security Awareness Framework for Students This study presents SAFE-D Education Framework

S – Secure: Students are trained on secure passwords, multi-factor authentication, device protection, software update, and secure networks.

A - examine: Students learn to examine links, messages, websites, apps, online identities and sources of information before trusting them.

INNOVATIVE RESEARCH ORGANISATION
International Journal of Advance Research in Education, Technology & Management
(Scholarly Peer Review Publishing System)

F – Filter: Students learn how to filter out misinformation, dangerous content, suspicious requests, unnecessary data acquisition and unsafe online interactions. E - Escalation: Students are trained to escalate cyber incidents to instructors, parents, institutional authorities, service providers or relevant mechanism in the government.

D – Defend: Students build durable habits of privacy protection, good digital citizenship, cyber resilience and ethical technology use

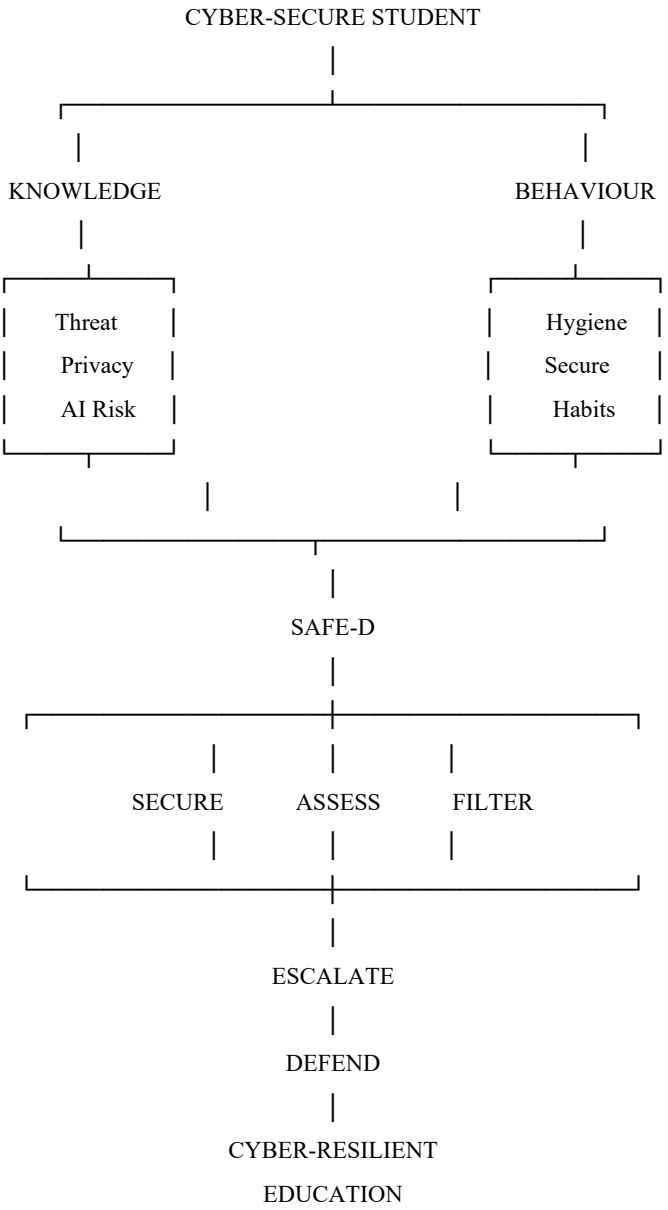

Figure 1

INNOVATIVE RESEARCH ORGANISATION
International Journal of Advance Research in Education, Technology & Management
(Scholarly Peer Review Publishing System)

CYBER-RESILIENT EDUCATION: The model highlights that cybersecurity awareness is a continuous process rather than a one-time lesson. Results and Discussion The analysis gives several important results.

Finding 1: Cyber Awareness is an Educational Imperative With the proliferation of digital learning, cyber security can no longer be detached from education. Students cannot get the full benefit of digital technology unless they can do so safely.

Finding 2: Human conduct remains a major vulnerability: even smart .Assents an essential layer of Defense.

Finding 3: Cyber Literacy is Part of Online Literacy Online literacy has typically been characterized as the capacity to access and use information technology . We also need to expand this notion to current schooling, encompassing privacy, authentication, misinformation, cyber ethics, AI literacy, and incident response.

Finding 4: Teachers are force multipliers: By teaching a single teacher, you can effect dozens or hundreds of children. In this sense, teacher training must be considered as a strategic investment in cyber resilience.

Finding 5: Cybersecurity must be continuous: Rapidly evolving cyber dangers. Not enough one off seminar. Regular awareness campaigns, practical exercises, revised policies and periodic reviews are needed in institutions.

Finding 6: The threat landscape is developing with AI: Generative AI is emerging and boosting the sophistication of phishing, impersonation, misinformation and synthetic media. Therefore, AI literacy should be part of cyber awareness campaigns.

7. **Student awareness alone cannot defend educational institutions;** institutional preparedness is vital. Network security, data governance, access control, backup systems, incident response and institutional rules are just as vital.

Table 2: Recommended Institutional Cyber Awareness Programme

Component	Frequency	Target Group	Expected Outcome
Cyber orientation	Beginning of academic year	New students	Basic awareness
Cyber hygiene workshop	Every semester	Students	Safer online habits
Teacher training	Twice yearly	Faculty/staff	Improved guidance
Phishing simulation	Periodically	Students/staff	Threat recognition
Cyberbullying awareness	Every semester	Students	Safer online interaction
AI safety session	Annually	Students/teachers	Critical AI use
Password/MFA campaign	Every semester	All users	Better account security
Incident-response drill	Annually	Institution	Faster response
Parent awareness session	Annually	Parents	Home-school cooperation
Cyber security audit	Periodically	Institution	Reduced vulnerabilities

INNOVATIVE RESEARCH ORGANISATION
International Journal of Advance Research in Education, Technology & Management
(Scholarly Peer Review Publishing System)

How to Build a Secure Digital Learning Environment

Cyber Security in Curriculum Cyber security does not have to be introduced as a separate subject in all the levels of education. Its basic ideas can be implemented in the curricula of computer science, social sciences, citizenship education, as well as life skills and vocational education.

Use Experiential Learning Students should be involved in actual tasks and simulations, not memorizing definitions.

Examples include:

• Identifying phishing emails.

• Testing of suspicious URLs.

• Creation of a strong password.

• Updating privacy settings.

• Deepfake detection.

• Practice on incident reporting.

• Evaluating Internet sources

Establish Student Cyber Clubs: Schools and universities may establish Cyber Security Clubs for students to participate in awareness campaigns, quizzes, poster contests, cyber drills, talks on ethical technology and peer education. EncouragePeer-to-Peer Learning: Students frequently learn best from peers. Cyber ambassadors, student cyber volunteers, can help to spread safe habits across classrooms. Build Teacher Capacity Regular faculty development programs should cover new hazards and appropriate use of digital instructional resources. Develop Cyber Incident Response Procedures: Institutions should clearly outline:

• who to contact;

• what information needs to be preserved;

• how to secure accounts;

• how to isolate infected systems;

• when to notify parents; and

• when an incident should be reported to appropriate authorities.

AI Literacy: Students need to know how to fact-check information created by AI, identify hallucinations, identify manipulation of media, protect personal data while using AI tools, and adhere to academic-integrity norms.

Policy ramifications: These results have ramifications for education policies in India. First, digital education policy should routinely include cyber security knowledge. The NEP 2020 lays a broad basis for technology enabled education, but secure digital engagement demands concurrent attention to security, privacy and resilience. Second, institutions of higher education need to be able to leverage current UGC cyber-hygiene and cyber-security resources. Third, national agencies such as CERT-In can keep developing age-appropriate cyber awareness material for schools. CERT-In has already had awareness leaflets and particular resources for young users. Fourth, coordination between education institutions, technological businesses, government agencies, parents and civil society organizations is crucial. Cyber security is not the responsibility of a single stakeholder.

INNOVATIVE RESEARCH ORGANISATION
International Journal of Advance Research in Education, Technology & Management
(Scholarly Peer Review Publishing System)

Finally, education on cyber security should be considered as part of the national cyber resilience. Today's students will be tomorrow's professionals, administrators, entrepreneurs, researchers, warriors, teachers and policy makers; and we want them to be successful. Their online behavior will define India's bigger digital security landscape

Recommendations and Findings Based on the analysis, the following recommendations are made:

- Introduce age appropriate cyber security instruction from school level.
- Mainstream cyber hygiene in online literacy programs.
- Carry out compulsory cyber awareness orientation for incoming pupils.
- Provide frequent cyber security training for teachers and administrators
- Create cyber security clubs and student cyber ambassadors.
- Conduct fake phishing and cyber-safety exercises.
- Turn on multi-factor authentication for institutional accounts.
- Establish institutional level cyber incident reporting processes.
- Improve privacy and data protection procedures in educational institutions.
- Cyber education needs to include AI literacy and deep fake awareness.
- Raising awareness on cyberbullying and internet harassment.
- Get kids to check work before they hand it in.
- Encourage linkages between educational institutions and cyber security authorities.
- Review institutional cyber security policy from time to time.
- Involve parents in cyber safety awareness initiatives.
- Regularly review student cyber security awareness.
- Develop multi-lingual cyber awareness material to increase accessibility.
- Develop inclusive gender and socio-economic sensitive cyber safety initiatives

CONCLUSION

The digital transformation of education has provided unparalleled potential for learning, collaboration, innovation and access to knowledge. At the same time, it has produced a complicated digital world where children are exposed to phishing, cyberbullying, identity theft, privacy breaches, malware, misinformation, social engineering and emerging AI-enabled risks. Thus, awareness of cybersecurity needs to be incorporated into contemporary schooling. It is not enough to say that because young people are tech-savvy, they are automatically safe online. Digital competency must be supported with cyber competence. Creating a safe digital learning environment is everyone's job. Students must develop safe and ethical habits, teachers must become competent cyber-safety mentors, parents must provide supportive guidance, institutions must establish strong policies and technical safeguards, and government and technology organizations must provide appropriate resources and support. India has already built major foundations with NEP 2020, UGC resources, CERT-In awareness activities and its digital education efforts. The next stage should be to shift the way cyber security education is being taught from an ad hoc awareness effort to a continual institutional culture. The proposed SAFE-D framework – Secure, Assess, Filter, Escalate and Defend offers a practical conceptual method to achieve this goal. The key point is that cyber security has to be part of our educational conduct in our daily lives. The end goal should not be only to produce pupils who can use digital technologies. The goal should be to

develop cyber-aware, responsible, ethical, resilient, and digitally enabled citizens. Education is not just the acquisition of knowledge; it is one of the most potent tools of constructing a secure digital future in our increasingly linked world

REFERENCES

1. 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, 1–15.
2. CERT-In. (2025). Cyber Smart Kids Suraksha Guide. Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology, Government of India.
3. CERT-In. (2026a). Blueprint for reducing exposure and defending against AI-assisted vulnerabilities exploitation in digital infrastructure. Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology, Government of India.
4. CERT-In. (2026b). Awareness booklets. Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology, Government of India.
5. International Telecommunication Union. (2009). Child online protection. ITU.
6. International Telecommunication Union. (n.d.). Child online protection training for social workers, academic and non-academic staff. ITU.
7. Ministry of Education, Government of India. (2020). National Education Policy 2020. Government of India.
8. Ministry of Education, Government of India. (2025). National Education Policy 2020 initiatives. Government of India.
9. UNICEF India. (2023). Online safety for children and adolescents. UNICEF.
10. UNICEF India & UNESCO Regional Office for South Asia. (2026). Children's online safety in education: Implications for students, teachers and parents and education functionaries in the age of AI and frontier digital technologies. UNICEF India.
11. University Grants Commission. (2022). Handbook on basics of cyber hygiene for higher education institutions. UGC.
12. University Grants Commission. (n.d.). Syllabus of cyber security course at undergraduate and post graduate level. UGC.
13. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102.
14. Whitman, M. E., & Mattord, H. J. (2021). Principles of information security (7th ed.). Cengage.
15. World Economic Forum. (2025). Global cybersecurity outlook 2025. World Economic Forum.