*Research Article*

# A Study of Cyber Safety Awareness among Students and Educational Initiatives

*Harshita Panjani[1] & Alka Mudgal[2]*

*[1]Ph.D. Scholar, Amity Institute of Education, AUUP, Noida*

*Email-harshita.panjani@s.amity.edu*

*[2]Head of Institute, Amity Institute of Education, AUUP, Noida*

**Abstract**

*In the digital era, cyber safety education in schools has become paramount in ensuring the ethical use of technology and responsible digital citizenship among students. Technological integration in education demands a safe online environment for students. Moreover, after the COVID-19 pandemic, an exponential increase in the use of the internet in India can be observed, as a hybrid model of teaching-learning has been implemented since then. With an increase in the usage of the internet and technological advancements in the field of education, the risk of cybercrime and online threats has also increased. Thus, cyber safety awareness is crucial as students are exposed to a variety of online risks. This research delves into various aspects of cyber safety education in schools, its significance in making students robust and responsible netizens, and the role of educators in fostering a safe online environment. A survey was conducted to assess cyber safety awareness among middle and secondary-level students of two age groups (12-15 years and 15-18 years). The result of the survey revealed that the majority of students were not well aware of safe internet use and digital practices. Cyber safety awareness was low among middle-grade students of the age group (12-15) in comparison to secondary-level students of the age group (15-18). The study emphasises incorporating structured cyber safety education in school curricula and building teacher capacity through continuous professional development, leading to the development of responsible, informed, and digitally resilient citizens.*

**Keywords:** Cyber Safety Education, Cyber Crime, NEP2020, Continuous Professional Development of Teachers

## Introduction

Cyber safety, also known as online safety or internet safety, refers to the practice of protecting oneself and others from various online threats and dangers while using the internet and digital technologies. It encompasses a range of measures and behaviours aimed at ensuring a secure and responsible online experience. It is necessary to ensure that online resources are used safely with utmost care and in a responsible manner. It is concerned with keeping the information safe online and handling it responsibly. It also involves being respectful towards others online and using netiquette. Cyber safety and security is also concerned with implementing and adopting strategies, to protect devices from attacks. The data should be protected from being misused through unauthorised access. (Cyber Safety Security guidelines, NCERT)

Information security is one of the biggest challenges in the present day. Cybercrime is the first thing that comes to mind when we think about

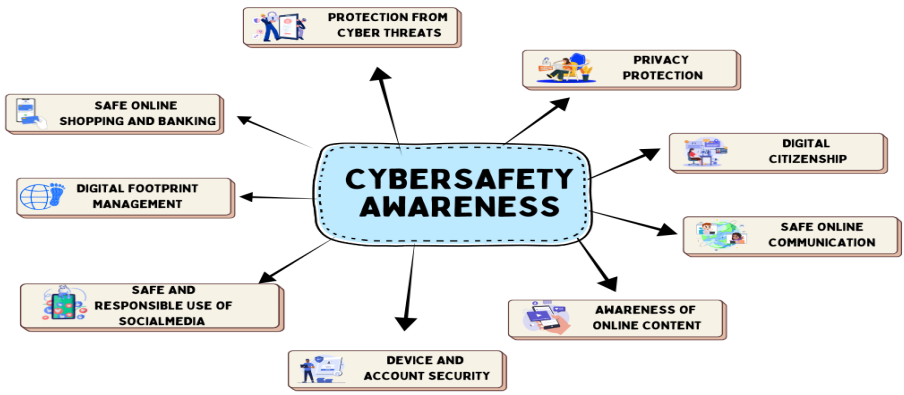
cyber security, and they are growing significantly every day. (R. Nihita, 2014). Cyber safety is essential in the digital age to protect from cyber threats like cyberbullying, stalking, trolling, malware, phishing, identity theft, etc.

The internet has made life of an individual easier, but there are some negative concerns that can also be easily observed. Fraudulent activities including hacking, phishing attacks, cyber trolling, cyber bullying and, child pornography have increased with an impact as a consequence of lack of awareness regarding cyber-safety among internet users. They are becoming easy victims of these fraudulent actions. (L. Prathamesh, 2021)

## Need for Cyber Safety Education in Schools

The risk of cyberattacks has increased due to the recent trend towards e-learning and a significant increase in online communications. Cybercriminals are currently taking advantage of these opportunities to steal sensitive information, deceive educational organisations, or use ransomware schemes. It is the responsibility of each individual to protect themselves online. (NCERT Training module, July 2023)

Education on cybersecurity is also necessary to ensure responsible use of technology. Teenagers use their devices to socialise online and spend a lot of time on computers. This gadget addiction consumes teenagers' valuable time, and eventually, it becomes impossible to avoid becoming addicted to online games. This may lead to health issues for youngsters. Users may not always be aware that they are being attacked, and these threats and attacks might take many different forms. Therefore, immediate action is required in this concern to ensure the safety of young children while using the resources online (Rahman et al., 2020). Since all protective elements are crucial in preventing cybersecurity threats, cyber safety education is also essential for addressing these issues. Education about cybersecurity is required to protect internet users against both current and emerging cyber threats.




National Education Policy (2020) envisions leveraging technology in education. In order to provide a safe and effective atmosphere for learning, it also places a strong emphasis on children's safety and security, especially cyber safety and security. NEP 2020 states that "Children and adolescents enrolled in schools must not be forgotten in this whole process. Their safety and rights should be prioritised and given due consideration. (Para 8.11, NEP 2020)

## Review of Literature

The increasing digitalisation in learning, especially after the COVID-19 pandemic, has significantly changed students' engagement with virtual space, raising concerns regarding cyber safety. The heightened use of the internet results in a greater risk of exposure to threats such as cyberbullying, phishing, identity theft, and privacy infringement (Rahman et al., 2020). Therefore, cyber safety education is recognised as an essential part of the school curriculum to promote responsible digital citizenship and protect students from cyberattacks.

Cyber safety refers to the attitudes and awareness required to protect users from cyber threats like malware, social engineering, and malicious content online (NCERT, 2023). Reddy and Reddy (2013) found that the occurrences and sophistication of cyber threats have increased as digital tools are used more intensively, calling for early and organised intervention. The research highlighted awareness of students regarding online behaviours, legal aspects, and the adoption of protective mechanisms and measures. Muniandy, Muniandy, and Samsudin (2017) conducted research on cybersecurity behaviours among Malaysian higher education students and found restricted awareness and insecure online behaviour, especially involving sharing passwords, unverified downloads, and social media privacy. This indicates a global tendency of lack of cyber hygiene that starts early and continues through adulthood unless addressed. Chawla, Kapoor, and Chawla (2023) undertook a regional study across Delhi/NCR schools and colleges that the majority of youth are not well aware of ethical and safe digital practices. Their research indicates that students who are frequent internet users are not well-informed regarding threats such as phishing, spoofing, and the legal aspects of online misbehaviour. The authors emphasize the necessity of well-organised school-based interventions and more incorporation of cyber ethics into digital literacy initiatives, particularly in the developing world. Yashwant (2021) further points out that education on cyber safety has to start at school and stresses the inclusion of subjects, including cyber hygiene, safe device usage, and netiquette in the regular curriculum. Additionally, the National Education Policy (NEP) 2020 emphasises child safety and digital security in schools (MoE, 2020). The policy also insists that students be taught 21st century skills, which include digital responsibility.

Moreover, programs such as the CyberPeace Foundation and the Cyber Safety Guidelines of the CBSE encourage cyber clubs, student-led awareness campaigns, and professional capacity-building for teachers (CBSE, 2023). These programs not only aim to educate students but also equip teachers with the right skills to support learners in navigating cyberspace safely.

## Objectives of the study

- To identify the major aspects and the need for Cyber Safety Education in schools.
- To assess students' knowledge, attitudes, and behaviours related to online safety and responsible digital citizenship.
- To compare the Cyber safety awareness among middle-grade (age group 12-15 years) and secondary-level (age group 15-18 years) students
- To identify best practices and recommendations for the effective implementation of cyber safety education programs in schools

## Methodology

This research employed a descriptive survey design to assess students' levels

of cyber safety awareness at the middle and secondary levels. The design was used because it enables the gathering of quantitative and qualitative data from a specified population to uncover prevalent awareness, practice, and knowledge regarding cyber safety matters. The sample consisted of 222 students from two private, CBSE-affiliated schools in the Delhi-NCR region. Out of these, 40 students were in the 12–15 years age group (middle grade), and 182 were in the 15–18 years age group (secondary grade). The schools do not have a formal cyber safety curriculum, but include cyber safety as a subject matter within the Computer Science subject at both grade levels. Students were randomly sampled using a simple random sampling method to prevent bias and ensure equitable representation from the two age groups and schools. For data collection, written consent was first secured from school principals and class teachers. They were informed about the purpose, scope, and ethical aspects of research.

**Data Collection**

Information was gathered by utilising a validated and structured questionnaire, formulated especially for this research. The questionnaire was comprised of two parts, part I consisted of 6 general cyber safety awareness questions and part II consisted of 18 items: 15 multiple-choice questions (MCQs) targeting core concepts of cyber safety and safe internet use, practices, including password protection, cyberbullying, malware, phishing, identity theft, and managing privacy, and 3 open-ended questions that are designed to elicit students' overall perception of cyber-attacks, such as identity theft, phishing, spoofing, and their knowledge of IT Act or cyber law-based safeguards. The questionnaire was distributed in physical mode (pen-and-paper) at regular school hours, in the presence of the investigator and school-appointed invigilators. Pre-content validation had previously been conducted by expert review by teachers and ICT experts to ascertain the validity, clarity, and age-appropriateness of the items.

**Scoring Procedure**

Every accurate answer in the MCQ section was worth one mark, with a maximum possible score of 15. Student awareness levels were graded based on total scores using the following scoring rubric:

- High awareness: Score ≥ 12
- Medium awareness: Score ≥ 8 and < 12
- Low awareness: Score ≥ 0 and < 8

General awareness-based questions were analysed to determine the percentage of students who selected the correct responses. Quantitative information collected through the MCQs was handled using descriptive statistics (mean, standard deviation, frequency, and percentage) and inferential statistics (independent t-test) to contrast awareness levels between age groups. The open-ended answers were examined qualitatively to determine frequent themes, misconceptions, and awareness gaps.

**Data Analysis**

Analysis was carried out using descriptive as well as inferential statistics to assess the level of cyber safety awareness among students.

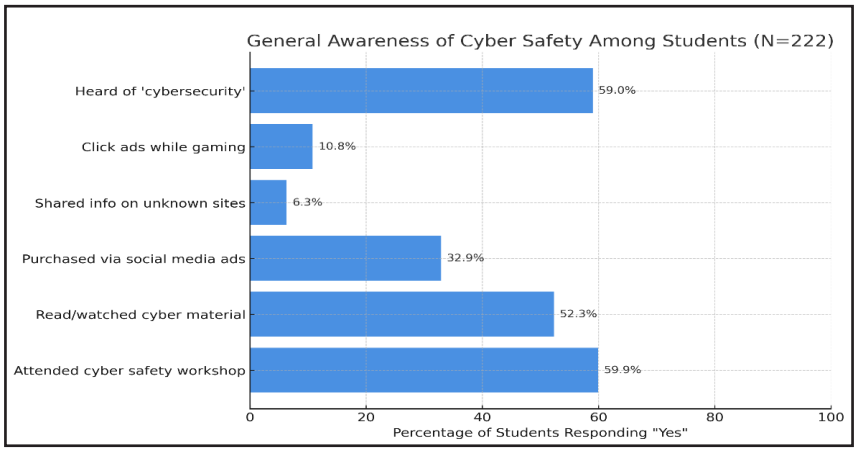
**Analysis of General Awareness (Part I)**

The responses of this part were analysed using percentage distribution to reflect upon the baseline familiarity and behaviour of the students related to cyber safety practices.

**Table-1: General awareness of students on cyber safety**

| S. No. | General Awareness Question | Yes (%) | No (%) |
|---|---|---|---|
| 1. | Have you ever heard the term "cybersecurity"? | 59.00% | 41.00% |
| 2. | Do you click on advertisement links while playing online games? | 10.80% | 89.20% |
| 3. | Have you ever shared personal information on unknown websites or links? | 6.30% | 93.70% |
| 4. | Have you purchased products after clicking ads on social media platforms (e.g., Instagram)? | 32.90% | 67.10% |
| 5. | Have you ever read or watched any material related to cybersecurity? | 52.30% | 47.70% |
| 6. | Have you ever attended a programme or workshop on cyber safety? | 59.90% | 40.10% |

**Figure-1: General awareness of students on cyber safety**



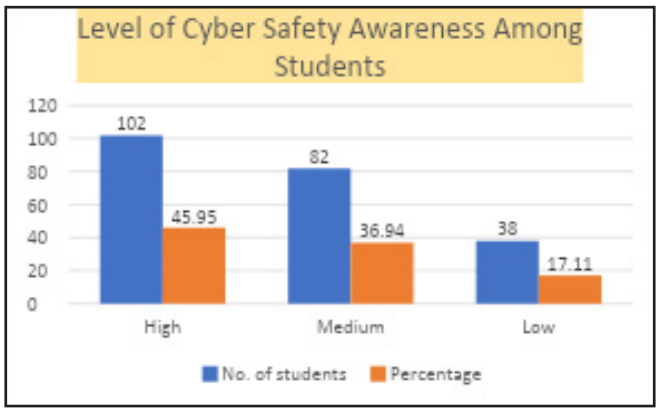

## Awareness level based on MCQ scores (Part II)

This part of the questionnaire consisted of 15 MCQs to assess the knowledge and awareness of students about core cyber safety concepts. The values of mean and standard deviation were calculated as (9.857 and 3.236) for age group (12-15) years and (13.75 and 1.699) for age group (15-18) years). Based on the maximum score, mean, and standard deviation, the level of cyber safety awareness among students was categorised as "High" (for score>=12), "Medium" (for score>=8 and <12), and "Low" (for score>=0 and <8).

**Table-2: Awareness level of Students on Cyber Safety**

| | Level of Awareness of Cyber Safety | | | |
|---|---|---|---|---|
| | High | Medium | Low | Total |
| No. of students | 102 (45.95%) | 82 (36.94%) | 38 (17.11%) | 222 |

**Figure-2: Level of Awareness of Students on Cyber Safety**



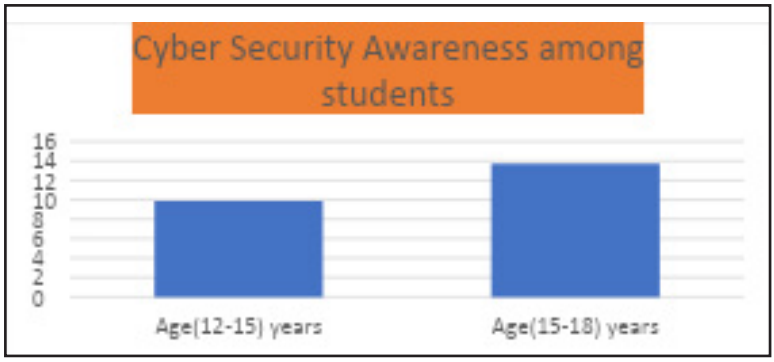

## Comparison of awareness across age-groups

An independent samples t-test was conducted between two age groups: 12–15 years (n = 40) and 15–18 years (n = 182) to determine the difference in the awareness level by age.

**Table-3: t-value for the difference in awareness of students about Cyber Safety -Group wise**

| Age Group | Mean Score | SD | T-stats |
|---|---|---|---|
| Age (12-15) years | 9.85714 | 3.236 | 6.914(Significant) |
| Age (15-18) years | 13.75 | 1.699 | |

**Figure-3: Mean score of Students on Cyber Safety**




## Findings and Discussions

### Findings

To measure basic knowledge and behaviours concerning cyber safety, six yes/no questions were given to students. Examining the results of the questions showed different awareness levels:

A significant number of students (131 of 222, 59.0%) had heard the word “cybersecurity” and so were moderately exposed to the

term. Only 24 students (10.8%) had clicked on advertisement links while gaming online, so this risk-taking behaviour appeared to be relatively rare. Yet, 14 students (6.3%) had posted personal details such as phone numbers or email addresses on unfamiliar websites, demonstrating a possible susceptibility to phishing or identity theft.

In addition, 73 students (32.9%) confirmed that they had purchased goods under ads viewed on social media such as Facebook or Instagram, which shows exposure to online commercialisation influence and scamming. Positively, 116 students (52.3%) reported having followed content pertaining to cybersecurity, including articles, videos, or material disseminated in school. A good number, 133 students (59.9%) of the students indicated that they had attended a cyber safety programme or workshop, which demonstrates initiatives by the schools or outside agencies to disseminate awareness, although not as an organised component of the curriculum.

The study indicates that the majority of students reflected general awareness of cyber crime and cyber safety measures. 45.95% (102/222) of students reflected a 'High' level of awareness for cyber-crime, online threats, and cyber safety measures. 36.94% (82/222) students have a 'Medium' level of awareness and only 17.11% (38/222) students were found to have a 'Low' level of awareness as presented in Table 2 and Figure 2. These results indicate, the majority of students reflected high level of cyber safety awareness, while a significant number of students were found to be within the medium or low category of awareness.

The mean scores of students aged (12-15) years were (Mean = 9.86, SD = 3.24) and for (15-18) years were (Mean = 13.75, SD = 1.70) respectively. This indicates that students at the secondary level are well aware of Cyber safety as compared to middle-grade students. To analyse the significance of the difference in awareness among students based on their age groups independent T-Test was employed and the result is presented in Table 3. The t-ratio computed as 6.914, is significant at both .01 level and .05 levels of significance. This reveals that there exists a significant difference between the awareness among the students falling in both the groups.

The answers provided by the students for open-ended questions reflected that the students were well aware of hacking, cyberbullying, and spoofing but the majority of students were not able to provide appropriate answers concerning online threats such as phishing, malware, spyware, etc. Very few students showed familiarity with legal provisions of cyber law and IT ACT 2000.

## Discussions

The findings of this research indicate the existing level of cyber safety awareness among secondary school students and highlight the critical areas that are in need

of educational intervention. The information shows that while the majority of students know the term cybersecurity, their experiential knowledge and behavioural use of online resources and online practices vary. While students reported that they had exposure to cyber safety content, awareness sessions, and workshops, this did not necessarily equate to conceptual understanding or informed and responsible online behaviour. This aligns with Chawla, Kapoor, and Chawla's (2023–24) concerns that even more digitally engaged students tend to have little knowledge of advanced cyber threats and ethical technology use. This disconnect can be attributed to the fact that there is not enough integration of cyber safety education within the formal curriculum, with such content being limited to a handful of lessons in the computer science subject.

One of the main findings of the study was the noticeable disparity in levels of awareness between middle and secondary level students. The secondary level exhibited greater consciousness of online threats and more secure behaviour online, which implies that maturity and exposure to technology can enhance digital competence. However, this raises concerns regarding the vulnerability of younger teens using digital platforms, potentially without the skills they need to do so securely. These results align with those of Yashwant (2021) and Rahman et al. (2020), who highlight the significance of age-specific cyber safety education from an early adolescent stage.

Further, the analysis based on responses of open-ended questions indicates a lack of knowledge regarding cyber laws and the function of legal protection, including the IT Act, among the majority of students. While some students could define common cyber threats, such as cyberbullying or identity theft, few reflected on legal protection mechanisms in mind. This supports Muniandy et al. (2017) and NCERT (2023) suggestions, which prioritise the inclusion of legal literacy in digital studies to enable students not only to protect themselves but also to identify their rights and responsibilities on the internet.

Another significant implication derived from the study is the necessity for teachers' roles to be enhanced in integrating cyber safety education. Although external workshops and awareness programs organised in school are beneficial, their one-off nature fails to have long-term consequences unless anchored by ongoing school-based education and teacher facilitation. Both the CBSE Cyber Safety Guidelines (2023) and the National Education Policy 2020 emphasise teacher training and student participation through systematic digital citizenship programs, although in the schools studied, cyber safety was not introduced as an independent curriculum, highlighting the need for educational initiatives in this regard.

Thus, the current study on cyber-safety awareness among students cannot rely on limited exposure through subject-specific learning,

a few workshops, or short-term interventions. It requires a holistic, curriculum-integrated, and age-appropriate strategy with the backing of skilled teachers who can lead the students to become responsible and knowledgeable digital citizens.

## Recommendations and Provisions for Enhancing Cyber Safety in Schools

In the current digital era, it is crucial to make students aware of information security and the development of digital skills required to securely browse the internet. Particularly young children need to be guided to use the internet safely and to safeguard themselves. Our country is rapidly developing its cyber infrastructure; thus, we must teach the populace and the next generation how to use it responsibly. Issues related to cyber safety, cyber security, and ethical use of technology must be included in the educational process from a young age. Technological elements, operational aspects, awareness, training, and education are all important components of cybersecurity (Yashwant, 2021). Some initiatives at the administrative and institutional levels to integrate Cyber Safety Education include:

### Establishment of I4C (Indian Cyber Crime Coordination Centre)

I4C was established by the Government of India under the Ministry of Home Affairs. This centre aims to offer an all-encompassing, well-coordinated framework for successfully combating cybercrimes.

### Formation of Cyber Crime cells within the Police departments in various states

Most states in India have their cybercrime cells or units within their respective police departments. These units are tasked with investigating cybercrimes within their jurisdiction. The Delhi Police Unit operates an association called CyPAD (Cyber Prevention Awareness Detection) that deals with all cybercrime cases, including cyberattacks, hacking, cracking, Phishing, snooping, spoofing, child pornography and crime against women. The CyPAD also develops standardised awareness modules to spread cyber safety awareness. This special Cell also organises awareness programmes for teachers and students of schools across Delhi and provides material associated to safety measures including videos, digital presentations, handouts on FAQ, online safety rules etc.

### Initiatives of CyberPeace Foundation

The objective of the Indian nonprofit CyberPeace Foundation is to increase resilience in cybersecurity against cyberattacks and cybercrimes. CyberPeace is working in collaboration with the UN, several state and federal governments, and global educational institutions. This organisation is a member of UN Global Compact Network India and is registered with NITI Aayog.

### Formation of Cyber Clubs in Schools

To counteract cyber risks and raise awareness, education is essential. Due to the younger generation's increased susceptibility to cybercrime, students in schools must receive adequate education about cyber hygiene and potential threats. CBSE has also provided guidelines for ensuring cyber safety in schools and issued a circular dated: 25.03.2023 for "Formation of Cyber Clubs in schools for developing an ecosystem to prevent cybercrime." With joint endeavours among educational institutions, educators, and learners, these Cyber Clubs can make a substantial impact towards cultivating more secure cyberspace and alleviating cyber hazards within our community.

## Teachers' Empowerment and Professional Development

Encouraging educators and students to become more aware of cyber concerns is an initiative that educational institutions and administration could take to prevent these groups from emerging cybersecurity dangers (Muniandy et al., 2017).

Teachers must spread cybersecurity awareness to encourage responsible online behaviour. The training and Continuous Professional Development of teachers on cyber safety can apprise them with the required knowledge and capacity building for guiding and supporting students. Teachers can instruct students about checking the validation of online communication sources, methods, and mediums; secure data-sharing methods; being careful about communication and sharing of information while playing online on gaming sites, and carefully sharing information on social media platforms, social networks, and even on e-learning platforms (NCERT Training module, July 2023).

Some of the sources of training and professional development of in-service teachers on cyber safety include:

- Workshops, seminars, training sessions organised by the government and online courses, and resource materials specifically designed to help teachers integrate cyber safety education into their curriculum.
- Conferences, seminars, or workshops focused on technology integration, digital citizenship, or cyber safety.
- E-learning modules and training programmes available on technology platforms that include DIKSHA, SWAYAM, Coursera, edX, Udemy, etc.
- Capacity Building Programmes are organised by CBSE, and online training programmes are offered through the CBSE Training portal regularly throughout the academic session.

## Conclusion

Cyber safety awareness is essential for an interconnected world, as students are exposed to a variety of online risks. With an increase in the usage of the internet and technological advancements in the field of education, the risk of cybercrime and online threats has also increased. This study indicates the urgent need for the structured implementation of cyber safety education in schools. The results of the study highlight that general cyber safety awareness exists among students, but significant gaps remain in students' understanding of online threats, safe browsing, and legal protection, specifically among middle-grade students. The answers provided by the students for open-ended Questions reflected that the students were well aware of hacking, cyberbullying, and spoofing, but the majority of students were not able to provide appropriate answers concerning online threats such as phishing, malware, spyware, and provisions of cyber law and IT ACT 2000. The knowledge about these online threats can be provided by organising cyber safety programmes in collaboration with national organisations like NCERT, Cyberpeace, Cypad (Cyber Crime Cell), etc., and by starting cyber safety clubs in schools for active participation of students in Cyber safety programmes. Various provisions are also required to integrate cyber safety into the school curriculum and to encourage teachers' participation in training and certification programmes in cyber safety to empower them to provide essential support for the development of students as responsible and knowledgeable digital citizens.

## References


CBSE. (2023). Cyber safety manual for schools. Central Board of Secondary Education. https://cbseacademic.nic.in/web_material/Manuals/Cyber_Safety_Manual.pdf

Chawla, V., Kapoor, A., & Chawla, R. (2024). Cybersecurity awareness amongst youth – A survey in Delhi/NCR. *Computer Science Journal,* 9(2).https://doi.org/10.17010/ijcs/2023/v8/i2/172777

Ministry of Education. (2020). National Education Policy 2020. *Government of India*. https://www.education.gov.in/sites/upload_files/mhrd/files/NEP_Final_English_0.pdf

Muniandy, L., Muniandy, B., & Samsudin, Z. (2017). Cybersecurity behaviour among higher education students in Malaysia. *Journal of Information Assurance & Cybersecurity,* 2017, 1–13. https://doi.org/10.5171/2017.800299

NCERT. (2023). Cyber safety and security guidelines for schools. Central Institute of Educational Technology. https://ciet.nic.in/upload/Cyber_safety_for_schools_new.pdf

Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). *The importance of cybersecurity education in school*. *International Journal of Information and Education Technology*, 10(5), 378–382. https://doi.org/10.18178/ijiet.2020.10.5.1393

Reddy, G. N., & Reddy, G. J. U. (2013). Study of cloud computing in healthcare industry. *International Journal of Scientific & Engineering Research,* 4(9), 68–71. https://www.ijser.org/onlineResearchPaperViewer.aspx?Study-of-Cloud-Computing-in-Health-Care-Industry.pdf

Yashwant, L. P. (2021). Need of cyber security education in school. *International Journal of Innovative Research in Technology,* 8(2), 199–203. https://www.ijirt.org/master/publishedpaper/IJIRT152027_PAPER.pdf