Axinova International Journal
Volume 1 | Issue 1 | May 2026
Available online at: https://axinovajournal.com/

Cyber Safety Awareness among School and College Students

Aditya Veer Singh[1], Vivek Kumar Madhesiya[2]

[1]Principal, Juris Law College, BKT Lucknow.

[1]Email: avsingh.adv@gmail.com

[2]Assistant Professor, Juris College of Law, Gomati Nagar, Lucknow

[2]Email: vivekmadhesiya9889@gmail.com

Received: 01 April 2026 | **Accepted:** 11 April 2026 | **Published:** 18 May 2026

Abstract

Cyber safety, the practice of protecting people and systems from digital harm, is a growing concern for school and college students worldwide. Frequent exposure to technology at an early age tempts students to engage in online activities before they acquire the knowledge and skills necessary to protect themselves. Consequently, cyber threats evolve, diversify, and infiltrate educational institutions, affecting productivity and posing social and reputational risks. Educational authorities, policymakers, and parents recognize the need to improve students' understanding of cyber safety. Schools cannot effectively address this issue, as cyber safety topics have been marginalized in the curriculum and instructional time is limited. Cyber safety awareness among school and college students, therefore, warrants urgent and systematic attention (Al-Tajer & Adeyemi Ikuesan, 2022).

Keywords: *Cyber safety, digital protection, students, online activities, cyber threats, educational institutions, cyber safety awareness, curriculum, digital literacy, cybersecurity education.*

1. Introduction

Cyber safety is a set of measures that needs to be taken while using the internet. Computer safety includes measures taken with regards to information systems and data present in them. While using computers, students transmit and receive data through various channels present in computers. Cyber safety is especially important for school children. Cyber safety concerns remain unreported causing adverse effects at individual and national levels. Thus, an enormous need at levels of school as well as further studies arises to teach students about cyber safety (Al-Tajer & Adeyemi Ikuesan, 2022).

In schools, students prepare themselves for the future challenges of society. They build their careers based on what they learn at school. Even students of further studies have limited body of knowledge. Cyber safety constitutes major portion in the present digital world that needs to be taught at school to avoid adverse effects. Cyber safety helps individuals in roaming the internet without causing any harm. A well-formed structure at school enables students to use it in their day-to-day activities (Goran, 2017).

2. The Digital Landscape in Educational Settings

Schools use a variety of communication platforms, social media, email services, and digital tools for teaching and learning. Students use a wide range of different devices including personal laptops, tablets, mobile phones, and school-provided facilities. They are connected to the Internet using the mobile network and Wi-Fi, inside and outside the school. They also access the Internet through their families' and friends' networks and mobile hotspots.

School education is generally managed as a set of well-coordinated systems. Teachers supervise students in school and help them in their learning process. Governments and school boards formulate rules regarding how students should be expected to behave while using electronic devices and digital platforms for education. The school authorities manage the cyber security rules and regulations that students should comply with so that they remain cyber safe while engaged in their learning process. Students, parents, teachers, and school authorities are responsible for ensuring that students grow up

safely, learning how to protect themselves from cyber risks. Cyber safety is a major topic being discussed across the globe as more and more people are subjected to risks due to online activities.

3. Core Cyber Safety Risks for Students

A comprehensive view of online cyber risks reveals distinctive danger types and groups of probable students. Four main cyber safety threats accompany the school and college student community, experiencing adolescence swings and associated development elements. Fictional portrayals represent life, prompting misguided thoughts in diverse online settings. Cyberbullying and online harassment are natural juvenile behaviours, and numerous studies and examples prove that when these virtual cruelties happen on a social level, students ignore them. Similarly, adolescents fear using social networks and chatting with strangers, but they practice it.

The three main cyber safety risks facing students provide sufficient evidence in the literature. Recent Indian studies have also explored the prevalence of cyber safety threats among Asian students. Regulation guidelines discussed suggestions specific for Indian students. The National Skills Development Council–Indian Cyber Crime Coordination Centre document "Cyber Safe Young India: Youth Guide on Cyber Safety" identifies crime categories and help-seeking behaviours of school-going students and the broader student population. Analysis of these resources reveals the landscape of cyber safety issues besetting students. Cyber security incidents such as malware infections, phishing, cheating, and spam and hoax threats indicate the challenges not only of the younger generation but also of the country at large.

3.1. Online Harassment and Bullying

During their online travels, children encounter not only friends and useful information but also bullies, namely those who harass or hurt others. Harassment can take several forms: making hurtful jokes, posting embarrassing photos, spreading rumors, or even creating fake profiles that mock or impersonate someone. Some say nasty things and threated to make sure they can hurt the child's online reputation. Others are less subtle: they pretend to be friends but steal personal information about the child or their family to use against children later or to cyberbully them.

Many girls feel harassed by boys sending sexual messages and touching them online in cyber-slapping, elbowing, or sucking; and 44% of girls and 25% of boys say they have been pushed, yelled at, threatened, deceived, or gossiped about on the Internet. Girls sometimes suffer more than boys from unwanted sexual overtures or from being called "sluts" or "whores" across networks. Many angered mothers are outraged when they discover that others – even some of their daughters' friends but especially boys – have created fake websites that hijack the names of their children, exposing their daughters to possible unemployment because of damage to their reputation. Yet it is not only boys who create harmful Web pages.

There are websites that enable people to create fake profiles that can ruin someone's life. A mother asked her daughter to tell the site to take URL for the profile down, but the site refused, claiming it wasn't responsible for the information. When a rumor was spread on Facebook that Megan was a prostitute, Megan's mother and the detective in charge of the case urged Megan's friends to forward the news to others saying: "Don't believe everything you hear." When her mother insisted that Megan stop using Facebook because th epeople on it are cruel, Megan would reply: "But they are my friends."

3.2. Privacy and Data Protection

Cyber safety measures proposed during education are aligned with routine teaching and core subjects, explicitly addressing privacy and data protection. Schools distribute personal information among students, parents, and academic peers, requiring learners to assess consent and its meaning. Institutional data exposure occurs through admission processes and study online platforms while students also share personal details in plays, role reversals, or presentations—sometimes without optional disclosure mechanisms. Constant connectivity encourages attentiveness to work-in-progress. Parents and guardians invite fellow parents or workers into homes or resort to instant messaging that lacks privacy assurance, all illustrating personal, collegial, and institutional data circulation.

3.3. Malware, Phishing, and Scams

The malware, phishing scams, and other online threats are incidents from the cyber world that can be replicated within a controlled environment. Schools are generally equipped with the arsenal to summon and warn students in such a safe virtual space. Although there are issues of gaining access to such simulations to warn the students, it remains the area

of play and alert at the institution level. External agencies like Cyber Safe Women Foundation have devised a game to warn children about cyber-attacks and cyber safety.

Exploiting people's ignorance or limitations has always been a business strategy in our day-to-day transactions, leading to ruinous outcomes. With the advent of technology, that has only become easier and more lucrative. The use of technology to deceive people into divulging confidential information (or personal information) or any other valuable asset for the advantage of the perpetrator has always existed but it has now taken a form that can be achieved from any corner of the world. With few bits of information acquired by dubious means or by social engineering the entire social life of an individual can be destroyed by the use of social networking sites.

3.4. Social Media and Public Behavior

A distinctive feature of contemporary cyberspace is the emergence of social media, now firmly woven into the fabric of everyday life and work. Social media tools have rapidly captivated users, forming preoccupations, patterns of social interaction, and means of expression through multimedia, including text, images, sounds, and motion video. The proliferation of smartphones means that these services are just a click away, making it relatively easy to share information with peers in seconds. However, the positive impact on social interaction also brings risks and concerns. One privileged area for further analysis is the potential dangers to the reputation and digital identity of users, i.e., the traces left in social networks and produced through online content sharing.

Privacy is one of the main concerns online users keep in mind when sharing personal information on the web, but even beyond the formal privacy issues, we are often reluctant to consider the consequences of our online actions or, at least, of the information shared in social media. In particular, we are often unaware of the links between past actions and future online behavior: the behavior of peers can have a strong influence upon our own choices, and the effects of the information that is available online may take a considerable time to materialize. Young people's digital footprints are almost fully transparent, and the risk of exposure to the "permanent record concept" — the belief that what is made available online can be read by anyone at any time — is somewhat unrealistic. It is virtually impossible to predict what will become important later on or what will be requested by recruiters or admissions officers when considering new job opportunities or college applications.

4. Theoretical Frameworks for Cyber Safety Education

Cyber safety education can be reframed within three theoretical constructs—the Knowledge-Attitude-Practice (KAP) model, Protection Motivation Theory (PMT), and Media Literacy. This combination highlights the current cyber safety knowledge of students and enables the identification of suitable priorities for educational interventions. The KAP model divides learning into three progressive phases, while PMT emphasizes the need to raise awareness of hazards, understanding of risk and consequence, and self-efficacy to motivate protective measures. The prime objective of any cyber safety awareness campaign should first be to define what is meant by "cyber safety"—the general precautionary measures necessary to ensure user protection from the associated dangers arising from technological advances. Initiatives promoting media literacy are essential to enable critical comprehension of messages transmitted through various media, thereby aiding the development of appropriate skills for safe and acceptable conduct in both online and offline environments. Media literacy development is crucial when curricula fail to address the implications of the recent dramatic advances in technology that directly encompass students' everyday lives (Al-Tajer & Adeyemi Ikuesan, 2022).

4.1. Knowledge-Attitude-Practice Model

The Knowledge-Attitude-Practice (KAP) model—originally applied to health education—has been adapted to interpret progress in cyber safety awareness among students and to design complementary educational interventions. The Knowledge dimension reflects understanding of how to conduct oneself safely online, of the risks associated with social networking and other internet activities, and of the technical and regulatory measures available to protect against those risks. The Attitude dimension encompasses subjective beliefs regarding cyber safety, including perceived hazard severity and vulnerability, and perceived efficacy of protective measures. The Practice dimension encompasses students' activities related to cyber safety, including protective measures (e.g., password management) and risk-taking behaviors (e.g., unwarranted

disclosure of personal information). Materials designed for secondary-school and college students have sought to increase coverage across all three dimensions (Al-Tajer & Adeyemi Ikuesan, 2022).

Two additional frameworks from health education—and associated curricular recommendations—are also relevant. Protective Motivation Theory helps design educational content by mapping risk perception (severity and vulnerability) and motivation (response efficacy and self-efficacy) to intended behavior (protective action). Media Literacy Theory positions exposure to mass and social media as a cyber safety risk and encourages educational materials that enable informed selection and critical evaluation of media content.

4.2. Risk Perception and Protective Motivation

The possibility of cyber threats depends on individual perceptions of online risk. Knowledge of possible online threats affects an individual's willingness to take protective actions. However, online risk perception is argued to stimulate protective motivation to gain or enhance safety on the internet. A protective motivation framework was developed in the study. The following factors are considered as stimuli of protective motivation, such as the threat of risk of privacy on internet communications, online risks not existing, the ease of fostering a good digital reputation, and the high reputation of a good university. Three consequences of protective motivation include intention to change device in properly way to avoid loss of important files, intention to back-up files regularly in-a-regular-time to avoid loss of important files, and intention to install enough antivirus software in-a-regular-time to avoid loss of important files (Teimouri et al., 2018).

The prevailing concern regarding the risk of online safety depends on the cyber-attack and associated problems in trend of daily life. The education scenario believes, a student must be secured from the online hazards while dealing with Internet, gadgets, social media sites, professional websites, and other sources. A student motivated regarding the hazards of Internet or Cybersecurity prepares himself/herself against any misuse of information and gets engaged in safe Internet practice. Cyber safety awareness is very crucial in order to deal with online issues and to lead a peaceful Internet generation today. Enhancement of Cybersecurity safety awareness is the need of the hour so that a student can be safe from the online threats. Cyber safety awareness must evolve in order to proliferate oneself through various issues easily; consequently, effective parameters of online safety are discussed and established in order to be secured from internet threats while dealing with cyber safety. Educational institutions play a vital role in the life-cycle development of any student today and cyber safety awareness within the institution can only help the student tackle the online safety parameters with ease and space while at the same time escalating the development of the student graph in the digital era (Jelovčan et al., 2021).

4.3. Media Literacy as a Protective Factor

Cyber safety education can empower students to navigate the internet safely and responsibly, and media literacy may be an effective mechanism to equip them with such knowledge (Venkata Prasad, 2011). The full range of definitions for media literacy is beyond this study's scope, yet it generally involves understanding the role of media in society and developing critical thinking skills to evaluate media content (Teimouri et al., 2018). Being proficient in different types of media and their influence helps students adopt reflective attitudes, make informed choices, and avoid harmful information. Cyber safety can become an integral part of such media literacy training in educational institutions.

5. Pedagogical Approaches to Cyber Safety

Cyber safety education addresses an urgent need for awareness, training, and protective strategies among students. The digital world can expose the young to threats that jeopardize their well-being, academic performance, and future opportunities. Educational institutions remain the most suitable settings for cyber safety training, as students—especially in secondary and higher education—depend increasingly on technology for their studies and socialization. Moreover, students are usually more receptive to learning during school hours than in the home environment, where parental engagement and guidance often gradually diminish (Al-Tajer & Adeyemi Ikuesan, 2022). The developmental stage of teenagers and young adults predisposes them to exposure to inappropriate content and cybercrimes, yet only limited awareness-raising initiatives targeting this cohort have been undertaken.

The urgency of this situation is compounded by growing reliance on technology since the COVID-19 lockdowns. More student-centered learning approaches necessitate extensive use of computers, tablets, mobile phones, and the internet (particularly social media)—devices and services that enhance educational delivery yet also create greater exposure to the

risks associated with the digital landscape. Consequently, the new normal for the students of today is indeed more digital than ever before, but they have scant knowledge of online safety issues. Further compounding the risks incumbents of the digital landscape encounter—and the potential repercussions of unsafe practices—is the limited redress available to victims of cybercrime, whether through the formal legal framework or internal institutional mechanisms. Such offenses are oftentimes difficult to track, leading to extended durations of victimhood with few apparent remedial alternatives.

Cyber-safety education can be significantly enhanced by the adoption of appropriate pedagogical approaches. Cyber safety may be integrated within existing subjects or offered as an independent subject of instruction at primary, secondary, or tertiary levels. In any case, imparting knowledge, changing perceptions, and modifying behavior remains essential. Multi-faceted approaches encompassing wide-ranging instructional methods—tutorial and experiential activities, hands-on involvement, explicit descriptions, structured discourse, digital channels, multimedia materials, demonstrations, and more—further complement the practice of protecting students within educational institutions.

5.1. Curriculum Integration and Learning Outcomes

Cyber safety education encompasses digital or virtual safety topics, risk exposure to material that causes distress or pain, and protection methods. Cyber safety is supported by digital citizenship, which promotes responsible and safe use of information technology. Cyber safety education is essential for students in schools and colleges, where concerns about cyber harassment, illicit data gathering, and other cyber hazards are prevalent. Cyber disposition refers to an individual's attitude, behaviour, and understanding about cyber space. The cyber disposition of a student has two components: knowledge, which refers to the understanding of situation or environment indicators and motivation, which refers to an individual's propensity to act upon a situation. Cyber disposition and cyber safety education should contribute to an improved cyber safety understanding and alignment with policies worldwide.

Curriculum integration involves the embedding of learning across the curriculum to assist student learning. Integration facilitates cross-disciplinary connections that are important for deeper learning. Learning outcomes are articulated statements of what students are expected to know and be able to do as a result of a learning experience. The purpose of defining learning outcomes is to assist teachers in planning and delivering unit or lesson content, and to support students in assessing their own understanding and progress. Cyber Safety Awareness occupies a prominent place in the same practice, with opportunities for students to engage with online and mobile technology regularly built into a school or college unit. Expected learning outcomes align with the Australian Curriculum and the National Principles for Child Safe Organisations, with links explicitly indicated. The Cyber Safety Awareness content aligns with the General Capabilities of the Australian Curriculum: Digital Literacy and Critical and Creative Thinking, which have been identified as strong areas of need for student development in the local context (Putnam, 2019).

5.2. Instructional Methods and Activities

Digital technologies, including the Internet, social media, smartphones, and tablets, are now indispensable tools for teaching and learning in schools and college campuses (Al-Tajer & Adeyemi Ikuesan, 2022). Cyber safety policies and practices should be established and adhered to in conjunction with digital technology use, as, without them, misunderstandings, abuse, harassment, bullying, and cyber-attacks have the potential to occur. Schools and educational institutions need to take responsibility for ensuring student cyber safety.

5.3. Assessment and Feedback Mechanisms

Assessment strategies drive program design and implementation, from defining target outcomes to selecting activities, durations, and materials (Al-Tajer & Adeyemi Ikuesan, 2022). Assessment practices help identify and communicate prevention needs and improvements, shaping and communicating educational approaches—from formative and situational needs, to long-term objectives. They produce data on intrinsic motivation and a desire for change, helping to justify programming and setting a baseline for measuring progress.

Feedback from stakeholders—including students, educators, administrators, and parents—facilitates programme refinement. Preliminary surveys capture existing knowledge, attitudes, and practices, establishing a baseline for subsequent evaluation. Evaluation instruments assess comprehension and motivation following individual lessons or activities; targeted student surveys gauge immediate appreciation or interest. Post-programme questionnaires revisit initial metrics and

determine protective actions taken since. Analysis of results guides content revisions and delivery adjustments, enhancing rights-based learning.

6. Policy, Governance, and School Roles

Education systems must help to raise awareness of cyber safety for young students who are just beginning to explore the World Wide Web. Schools have an important role to play in developing student knowledge about the potential risks and consequences of unsafe online behaviours and in fostering a safe and secure cyber learning environment. Institutions should support the implementation and ongoing development of cyber safety educational programs by enforcing relevant policies and providing students with guidance and resources on cyber safety.

Institutions need to develop cyber safety policies that outline the school's position on the appropriate use of technology and electronic devices, and the cyber safety requirements for all stakeholders. Such policies should comply with government guidelines and encompass other relevant school policies regarding technology use, bullying, harassment, discrimination, student well-being, and rights and responsibilities. Policy creation for cyber safety is of the utmost importance given the rapid rate of technological growth and development in all sectors, and to reflect the voice of the school community, policies should include input from students, educators, parents, and administration.

The school administration is responsible for communicating and implementing cyber safety policy across the school community and for adjusting policy in response to emerging technologies and any changes in the school's educational mission. Schools play a central part in policy formation by promoting awareness of cyber safety and outlining the individual rights and responsibilities of all stakeholders in the cyber environment. Each of the technology stakeholders has a distinct role to play, including the student, educator, parent, and administrator, which should all be clearly outlined in communications and relevant documents.

Incidents that violate cyber safety policies should be reported to the school's pastor, cyber safety mentor, or program coordinator, or any appropriate member of the school's administration. Cyber safety incidents are defined as a breach or infraction of cyber safety policy, and one or more tools may be available to report and disclose them depending on the offending party. Responses to cyber safety matters should occur promptly and be tailored to the individual circumstances, the specific stakeholders, and the broader impact on the school community. Reports related to any technological platform or device used should receive equal consideration, regardless of whether a school-issued or private device is involved. (Popovac, 2017)

6.1. Policy Development and Compliance

Students are vital partners in shaping a culture of effective cyber safety. As educators strive to equip learners with relevant skills and knowledge, they also depend on student input to augment organizational understanding of challenges, trends, and emerging threats. While both formal policies and informal guidance articulate institutional commitments to student cyber safety, thoughtful policy development and adherence to established, domain-specific frameworks can strengthen cyber safety initiatives (Al-Tajer & Adeyemi Ikuesan, 2022).

Policies support cyber safety efforts by defining specific expectations and reference points. Institutional stakeholders routinely develop a range of policies, both external and internal, that govern organizational activities and operational parameters. Relevant international, national, regional, and local policies accompany institutional policies and provide further guidance. External digital policies operate independently of the institution but set specific parameters for browsing, engagement, and participation within publicly accessible domains. Adherence to these external policies may guide cyber safety efforts for environments and settings beyond the institution.

6.2. Roles of Stakeholders: Students, Educators, Parents, and Administrators

Cyber safety awareness is a fundamental issue on today's campuses, thus making timely interventions a moral and practical imperative. Schools and colleges have a special responsibility to protect students from cyber-related threats, and as recognised centres of learning, they also have a ethical duty to promote proactive awareness of such threats (Faucher et al., 2020). However, the scope and dimension that such awareness should take, and how it should be achieved, depend on responses to specific questions. The present study consists of an investigation into the online activities of students in

educational environments. The objective is to gain a clearer insight into the ferocity of cyber threats they face, and hence to guide an effective design of cyber safety awareness programmes either by institutional leaders or administrators, parents.

Analysis of the digital footprint and its infrastructure clarifies where the issue still stands. Examined in these global [educational] settings, the existing online engagements among learners give a good overview of contemporary levels and cyber safety challenges faced (Putnam, 2019). That said, emphasising aspects of educational surroundings will continue to add value and thereby sharpen the focus further.

6.3. Incident Reporting and Response Protocols

Effective cyber safety awareness and education initiatives are supported by clear policies and procedures that govern the actions of various members of the school or college community. In particular, the syllabus should stipulate the details of reporting mechanisms for all stakeholders and outline the processes for investigating and acting on incidents. Such transparency promotes responsible online behavior among students, as they are assured that the institution will take action to safeguard them from harm.

Well-publicized reporting mechanisms encourage students and parents to report incidents of cyber harassment even if they are reluctant to do so. Reporters should be able to speak directly to someone trained in cyber issues, rather than going through a generic online form. A spirit of cooperation should also underline the interaction between school authorities and the police or other parties investigating cybercrime, especially in the case of a serious offense. All incidents should be recorded and made available for audit purposes; while by their very nature they are not likely to fall under the RTI Act, disclosure in suitably sanitized form is still recommended, and such openness fosters stakeholder trust and confidence.

Incident processing thus involves multiple stages and a variety of participants. Students and parents alike are encouraged to report incidents; to facilitate this, school/college guidelines detail the IT and non-IT staff members empowered to receive those reports. The responsibility of such personnel is to act as first points of contact for individuals seeking help about cyber safety-related issues.

7. Technology Tools and Safeguards

Safety permeates all areas of human life. The nuances of personal safety shifted considerably with technological advancement such that cyber safety awareness is now almost as crucial as the conventional notion of safety. Technology enters classrooms and permeates daily life, so students—the youngest tranche of the population—require education regarding efficient and effective safety in technology usage. The Department of Education (Government of India) has established the ‘Digital Shakti’ program to provide materials for students, teachers, and parents on digital safety, awareness, and self-defense against cyberbullying, cyber threats, and cyber crimes (Al-Tajer & Adeyemi Ikuesan, 2022).

7.1. Secure Devices and Network Practices

Students primarily access the Internet through personal devices. Security features should be maximized; devices must be kept updated, and unnecessary applications should be uninstalled. Wireless local access networks (WLANs) must be configured with strong encryption, firewall enabled, and trustworthy users only allowed. Router firmware must be updated, and guest access disabled. Public WLANs should serve as the Internet’s periphery: reports suggest unencrypted networks promote illegal activities, and students’ lack of awareness heightens infection risks.

User privacy settings should be reviewed yearly, and accounts of users likely compromised, such as online games with financial incentives or collection accounts, should not store personal or financial information. Student information should be shared only when beneficial. During online registrations, students should avoid “dodgy” offers and enter partial details. Only information relevant to service delivery should be presented, while metadata should be collected in aggregate form. Deactivating user accounts is advisable when services are no longer required.

7.2. Privacy Settings and Data Minimization

Emerging threats of cybercrimes, phishing scams, and bullying incident continue to trouble school and college-going students. Cyber safety education focuses on the provision of precautionary policies to continue the safe usage of online activities and keeping track of the evolving trends. Internet privacy, though has been a known topic for internet users, is still a concept much ignored by many of the kids. Data privacy tools are always a software need by an individual but many users are not aware of the availability due to lack of knowledge, education, or any training. Schools or Educational

institutions are at the foundation structure where many subjects are taught on a theoretical basis but do not teach on practical grounds. Cyber safety practices and precautions, a part of Cyber Safety education, should be taught as a Curriculum-based subject, or Integrated as a practical-based formative subject, which provides adequate knowledge about the usage of cyber tools that can help prevent any mishaps occurring.

Sufficient knowledge and guidance on Cyber Safety education can prevent the child from becoming a victim of Cybercrime, later pushing them to commit crimes that may affect their real-life activities (Aldhafferi et al., 2013). Since the introduction of the digital learning perspective, it is now possible to integrate and combine multiple subjects as per concern or school needs. Providing a knowledge-based foundation on Cyber Safety education can be integrated with subjects like information technology, computer science, or practical-based training on the use of cyber Logically and Sequentially. Schools and colleges conduct sessions to provide awareness about Cyber Safety and Protection, and not a complete technique to it. The privacy of Personal Data has become a major concern after the introduction of various online and software programs, and many Cyber Safety practices should be taught based on Children. If a child is unaware of the Cyber Safety practices or does not know how to prevent it, it is much likely that they will fall for it.

A privacy setting prohibits unwanted parties from viewing data and helps maintain personal information on an online platform (Chen et al., 2024). Popular social media programming also provides a privacy setting that allows the user to protect unwanted access. Depending upon the school, they have chosen to conduct an online platform on Google Meet, Zoom meeting, or Microsoft Teams platform, Data on Social Media is shared for an extension course, and various unnecessary parties go through the data, which may or may not be secured in various schools. Privacy on Online Social Media can be prevented by Board Security, Cloud security, Limiting privacy, Limiting owner access, restricting Wi-Fi Sharing Access, and not violating the Authentication Policy.

7.3. Safe Browsing, Authentication, and Access Control

Access control refers to mechanisms that determine who or what is permitted to enter or use a computing resource. Access control includes data authentication methods that enable users to authenticate themselves to computers or networks before being allowed to use them. Safe browsing refers to the practice of following specific guidelines while using the Internet in order to avoid harmful applications, malware, and other unwanted programs. Students operate devices with global Internet connectivity and using diverse services on a daily basis. As such, they are usually not only targeted but often vulnerable to attacks. However, they frequently lack basic knowledge on how to use safe passwords, authenticate websites, and therefore be able to identify and avoid the most common threats on the web (malicious websites).

Browsing the Internet can expose students to security risks. Most students visit untrustworthy sites at least sometimes and unsafe sites often lead to security threats. However, using a secure password (one that contains at least eight characters including lowercase letters, uppercase letters, numbers, and symbols) limits the risk of becoming a victim of identity theft or a victim of other Internet crimes. Furthermore, recent studies show that forcing students to choose a strong password helps to decrease the increase in password cracking success rate. School authorities can implement several security control measures, including content filtering and adopting the principle of least privilege.

8. Community and Cultural Dimensions

Efforts to promote cyber safety have a tendency to neglect issues of inclusivity and equity (Al-Tajer & Adeyemi Ikuesan, 2022). To make a meaningful difference, any strategy must consider participants' backgrounds, digital practices, and real-world circumstances. Community dimensions — including culture, geography, economy, and language — exert powerful influences on educational needs and opportunities. Countries, cities, and neighbourhoods exhibit distinct characteristics that shape daily life and consequently frame community and cultural dimensions.

Contemporary technology fosters varying patterns of usage and connectivity among young people. For instance, cyber safety risks differ markedly for minority and majority-language speakers (Thumronglaohapun et al., 2022). Many resources are available in widely-used languages such as Chinese and English; support for other complementary languages is often scarce. Holistic strategies must recognise such diversities and establish relevant contacts, allowing cyber safety to maintain meaning and local resonance.

8.1. Inclusivity and Equity in Cyber Safety Education

Effective cyber safety education among school and college students must be inclusive and equitable to be truly effective. The requirement for inclusivity emerges from the realization that individuals with disabilities, minority groups, and adolescents from marginalized sections of society are more vulnerable online than other groups. The Cyber Safety Awareness Initiative guidelines endorse such considerations, as do the UNESCO ICT in Education Principles, which advocate the elimination of discrimination, harassment, and bullying in educational contexts. It is essential that strategies and mechanisms regarding cyber safety are communicated in languages, dialects, and forms understood by all students, with a special focus on those belonging to vulnerable groups.

The dimension of equity relates to the recognition that the increased adoption of information and communication technologies—and the ever-widening digital divide—have had a disproportionately negative impact on communities that were already marginalized. Adolescents from communities and groups that lack the requisite resources, skills, or confidence to keep themselves safe online are more vulnerable to becoming victims of cyber crime and to being negatively affected by the consequences of other people's actions. Consequently, there is a need to increase resilience, preparedness, and cyber safety awareness among these sections of society. Cyber precautions should also be taken in such a way that individuals remain unharmed while exploring cyberspace for personal, professional, or educational purposes.

8.2. Cyber Safety in Diverse Cultural Contexts

The wider communities and cultures of students outside educational institutions significantly influence their uptake of cyber safety education. Experiencing prejudice or discrimination against the group or community to which they belong can generate cyber-bullying or hate crime directed at them. Such negative experiences, in turn, may cause them to use the Internet inappropriately, either as perpetrators themselves or as passive onlookers. At the same time, a supportive and trusting familial and peer environment can increase resilience, moderating and decreasing the likelihood of negative online experiences. Conversely, a lack of cohesion and support in their immediate environment may increase vulnerability. It is therefore essential to integrate cyber safety education with intercultural education so that positive engagement with others through cyber space becomes the norm, fostering respect for and celebration of difference.

Students' background cultures and local contexts also play a key role in shaping their online experiences and safety practices. Educational programs must pivot toward inclusive access and must consider local conditions, languages, and parameters so that any harm to society as a whole can be minimized. Similarly, while the content must provide adequate guidance to students from different cultural backgrounds, the medium must support effective comprehension. In multilingual settings, any connecting language must be for social communication rather than for education.

9. Evaluation and Evidence-Based Practice

Various aspects of the program can be evaluated to assess its overall effectiveness. The direct impact on program participants' knowledge, attitudes, and behavior regarding cyber safety constitutes the major indicator. Program adoption by schools and colleges is a requisite step toward generating improved cyber safety awareness. Indicators such as the number of schools engaged, the number of students reached, and positive feedback from student-participants can reflect uptake and receptivity. The ultimate goal extends beyond adopting the program into bringing about a reduction in incidents of cyber safety violations.

Evaluating the implementation process can provide insights into enhancing acceptance rates across wider networks. Several colleges and universities offer various forms of cyber safety education. Conducting a post-implementation impact assessment in these organizations would produce corroborating evidence of the program's effectiveness. Factors that facilitate or inhibit the program's adoption would identify actionable needs that could enhance awareness-building by offering stakeholders incentives to maintain a minimum level of safety in their school and college networks. Such preparedness would likewise support future evaluative work on cyber safety awareness programs. Reporting the educational needs of stakeholders within the formal cyber safety framework of a country could foster constructive collaboration with law enforcement and accreditation departments.

9.1. Metrics for Program Effectiveness

Program effectiveness metrics elaborate the interaction of security concepts and learning through cyber safety initiatives targeting high school and university students. Involving an integration model, embedding security topics in introductory coding courses, cybersecurity awareness seminars, and a field study of coding practices in high-level programming classes enhance security understanding. Embedded curricula, feedback analyses, participation rates, and quantitative data on performance and behavior further gauge effectiveness (Azzeh et al., 2022).

The SUNY Cyber-Security Awareness Campaign assessed changes in student familiarity and behavior following an event promoting secure coding practices. Interest statements, an interactive quiz, and follow-up surveys collected pre-event data and post-event reactions and changed intentions. A questionnaire for junior undergraduates addressed practice awareness; analytics on click rates per degree and question informed program-wide recommendations. Multi-collaborative campaign implementation and targeted assessment throughout the three-year initiative proved crucial to meeting broad cyber safety objectives across diverse learning units (L. Innocenzi et al., 2018).

9.2. Research Gaps and Future Directions

Cyber safety awareness is becoming an essential topic of academic research. Although several studies have been conducted on cyber safety with school and college students as the focal group, other areas remain unexplored. Therefore, several avenues and opportunities are available for conducting research in these areas.

First, there is a considerable lack of literature on the influence of awareness on the adoption of safe cyber habits among school and college students in several parts of the world, especially in developing countries. Even in developed countries, the interrelationship and effects of awareness on the adoption of cyber safety habits are not well explored. There is tremendous scope for research on various aspects of the cyber safety awareness–adoption continuum. This study seeks to explore and build upon this gap by examining the relationship between cyber safety awareness and its influence on adopting cyber safety habits among school and college learners in Goa, India.

Second, longitudinal studies aiming to explore changes in cyber safety awareness over a more extended period are scarce, elevating several aspects of cyber safety to a vital research opportunity.

Third, although many different models have been proposed for studying safety-related behavior in diverse fields, including a few specific to cyber safety, a detailed examination of such frameworks applied explicitly to cyber safety is limited. There is ample opportunity to critically analyze the various proposed frameworks and establish additional models for research to study the continuum of awareness, attitude, and behavior concerning cyber safety. A segment of the proposed study aims to review these different models and suggest new frameworks for cyber safety.

Lastly, while other dimensions of cyber safety, such as safe devices and safe browsing, have received considerable attention in the literature, online harassment is still a highly pertinent topic yet remains relatively less explored. Many concepts related to the subject invite further scrutiny, additional study of this subject remains relevant and timely.

The limited number of research studies focused on cyber safety awareness among school and college students provides excellent opportunities for new research. Such investigations are essential given the pervasive influence of cyberspace on young people and the growing volume of cyber threats directed at them in recent times. A partial exploration of cyber safety in this context, which addresses not only awareness but also safe devices and safe browsing, contributes to the knowledge base in both the Indian and international arenas (Al-Tajer & Adeyemi Ikuesan, 2022).

10. Conclusion

Explicit recommendations for cyber safety education throughout the school and college years urge knowledge-based engagement with the full range of risk types students face. Stakeholders—students, educational institutions, parents, community members, and the larger society—need to recognize cyber safety as a shared responsibility. Only through collaborative, focused efforts can realistic journeys toward safe digital engagement be charted and realized. Each discussion phase must be specialized, acknowledging the particular needs and issues facing different age groups and cultures. Of paramount importance is the equitable engagement of all communities and sections of students through supportive delivery. Cyber safety education is a gradually evolving area of concern, and the pathways students take through their lives need to be informed by increasingly resilient support on cyber safety issues from all stakeholders participating in the process.

For educational institutions, the need for a comprehensive, up-to-date, and relevant cyber safety program is more compelling than ever. A robust and realistic approach to cyber safety awareness and education ensures a secure learning environment that promotes positive behavior while serving as a critical component of the institutional development strategy. An effective program covers the breadth of the educational institution itself. It leverages students, faculty, and parents as the key partners in ensuring a safe online environment in which learning can prosper without fear or anxiety. All key members of the institution participate in not only recognizing issues but also in preventing incidents and shaping a more positive culture of conduct. Evaluation and restructuring on a consistent basis map progress, ensuring that incidents decrease and that confidence and empowerment flourish as students take ownership of their cyber safety journeys.

References:

[1]. Al-Tajer, M. & Adeyemi Ikuesan, R. (2022). Cyber Security Threat Awareness Framework for High School Students in Qatar. [PDF]

[2]. Goran, I. (2017). Cyber Security Risks in Public High Schools. [PDF]

[3]. Teimouri, M., Benrazavi, S. R., Griffiths, M. D., & Hassan, M. S. (2018). A model of online protection to reduce children's online risk exposure: empirical evidence from Asia. [PDF]

[4]. Jelovčan, L., Vrhovec, S., & Mihelič, A. (2021). Survey about cyberattack protection motivation in higher education: Academics at Slovenian universities, 2017. [PDF]

[5]. Venkata Prasad, N. (2011). Developing New Media Literacy Among Secondary School Students In Malaysia: Case Studies Of Media Making On Environmental Issues. [PDF]

[6]. Putnam, C. (2019). Teaching in a Digital Age: Internet Safety Education. [PDF]

[7]. Popovac, M. (2017). Beyond the School Gates: Experiences of Cyberaggression and Cyberbullying Among Adolescents in the U.K. [PDF]

[8]. Faucher, C., Cassidy, W., & Jackson, M. (2020). Awareness, Policy, Privacy, and More: Post-Secondary Students Voice Their Solutions to Cyberbullying. [PDF]

[9]. Aldhafferi, N., Watson, C., & S. M Sajeev, A. (2013). A Smart Wizard System Suitable for Use With Internet Mobile Devices to Adjust Personal Information Privacy Settings. [PDF]

[10]. Chen, Q., Tang, J., Zhu, Y., & Ling Chan, K. (2024). The role of school climate on student disclosure of private information and cyberbullying: a comparison of regular and vocational school students in China.

[11]. Thumronglaohapun, S., Maneeton, B., Maneeton, N., Limpiti, S., Manojai, N., Chaijaruwanich, J., Kummaraka, U., Kardkasem, R., Muangmool, T., Kawilapat, S., Juntaping, K., Traisathit, P., & Srikummoon, P. (2022). Awareness, perception and perpetration of cyberbullying by high school students and undergraduates in Thailand.

[12]. Azzeh, M., Mousa Altamimi, A., Albashayreh, M., & A AL-Oudat, M. (2022). Adopting the Cybersecurity Concepts into Curriculum The Potential Effects on Students Cybersecurity Knowledge. [PDF]

[13]. L. Innocenzi, R., Brown, K., Liggit, P., Tout, S., Tanner, A., Coutilish, T., & J Jenkins, R. (2018). Think Before You Click. Post. Type. Lessons learned from our University Cyber Security Awareness Campaign. [PDF]

Cite this Article:

Singh, A.V. & Madhesiya, V.K. (2026). Cyber safety awareness among school and college students. Axinova International Journal, 1(1), 37–47.

Journal URL: *https://axinovajournal.com/*