ISSN: 3107-6513

Cyber Awareness among College Students: The Role of Higher Education Institutions

Prof. (Dr.) Sumit Nandi[#1] and Dr. Rubi Das (Chakraborty)[*2]

[#]*Principal, Harishchandrapur College, Malda, West Bengal, India*
[*]*Assistant Professor, Department of Philosophy, Harishchandrapur College, Malda, West Bengal, India*

[1]sumitnandi5@gmail.com, [2]rubichakraborty84@gmail.com

Abstract—
College students now have unparalleled options for learning, communication, research and professional development thanks to the quick growth of information and communication technology, which has completely changed the educational landscape. Students are now more vulnerable to cyberthreats such phishing, identity theft, financial fraud, cyberbullying, disinformation, data breaches and privacy violations due to their growing reliance on digital platforms. As a result, cyber awareness is now a crucial part of digital literacy and responsible citizenship. The importance of cyber awareness among college students, the main cybersecurity issues, the connection between digital knowledge and online behavior and the role of higher education institutions in fostering a safe digital environment are all examined in this article. Using pertinent scholarly research and cybersecurity awareness campaigns, the study employs a conceptual and literature-based methodology. The conversation emphasizes that being knowledgeable with digital technologies does not guaranty that one will be able to identify or stop cyberthreats. It makes the case that academic understanding, hands-on training, ethical consciousness, and institutional support should all be included in cybersecurity education. The paper suggests creating easily accessible cybercrime reporting systems, holding frequent workshops, encouraging ethical social media use and incorporating cyber awareness into college curricula. It comes to the conclusion that in order to create knowledgeable, accountable and resilient digital citizens, cyber awareness needs to be viewed as an ongoing educational process rather than a one-time event.

Keywords— Cyber awareness; cybersecurity; digital literacy; cybercrime; phishing; data privacy; digital citizenship.

I. INTRODUCTION

The twenty-first century is characterized by the widespread use of digital technology in almost every sphere of human life. The internet, smartphones, social media, online learning platforms, digital payment systems and artificial intelligence have significantly transformed the educational experiences of students. College students increasingly depend on digital resources to access academic materials, communicate with teachers, participate in online examinations, apply for scholarships, undertake research, and explore employment opportunities. While these technology advancements have increased accessibility and convenience in education, they have also introduced new concerns. Cybercriminals utilize digital platforms to trick others, steal personal data, profit financially and interfere with online activity. Inadequate cybersecurity training, overconfidence in digital communication, poor password practices and a lack of knowledge about privacy protection can all make college students vulnerable.

The knowledge, attitudes and practical skills needed to identify online hazards and take appropriate action are referred to as cyber awareness. It entails being aware of online dangers, safeguarding private data, spotting dubious communications, employing safe authentication techniques and acting morally in digital settings. Cyber awareness is particularly important in higher education because students are not merely consumers of technology; they are also creators, communicators, researchers and future professionals. Their digital behaviour can influence their academic performance, financial security, personal reputation and professional opportunities.

According to research on university students' understanding of cybersecurity, there is sometimes a discrepancy between knowledge and preventive behavior. For instance, understanding of cyberthreats and the impact of cybersecurity breaches on social media use were investigated in 2025 research of undergraduate students at an Indian institution. Students' capacity to recognize phishing attempts and their adoption of protective measures have been the subject of other studies. These studies underline the importance of practical cybersecurity education alongside general awareness. Therefore, promoting cyber awareness among college students should be considered an important responsibility of higher education institutions.

Based on a study of pertinent literature, a few chosen academic studies and publicly accessible cybersecurity education tools, the current article employs a conceptual and descriptive research technique. The Indian Computer Emergency Response Team (CERT-In), the Ministry of Electronics and Information Technology, the Ministry of Education and research publications on cybersecurity awareness, phishing, and online safety have all been taken into consideration as secondary sources of information. The following categories—awareness of cyberthreats, digital security behavior, privacy protection, cyberbullying, institutional accountability and educational interventions—were used to thematically analyze the literature. This article does not report original fieldwork or primary survey findings. Its conclusions are based on the conceptual analysis of the selected literature and institutional guidance. The proposed

ISSN: 3107-6513

recommendations may be used to develop future empirical research among undergraduate students.

II. CYBERAWARENESS IN HIGHER EDUCATION

Cyber awareness encompasses more than just computer and mobile application skills. It entails being aware of the possible repercussions of digital activity and using online platforms to make wise judgments. Even if a student is adept at using digital learning platforms, social media, online banking and artificial intelligence tools, they might not be able to spot a strange website or a fake message. This difference shows that cybersecurity expertise and digital familiarity are not the same. Cyber awareness has four interconnected dimensions:

- **Technical awareness** involves understanding passwords, authentication, software updates, secure networks, malware and data protection.
- **Behavioural awareness** refers to developing safe online habits, such as verifying links, limiting personal information sharing and avoiding suspicious downloads.
- **Ethical awareness** concerns respecting others' privacy, avoiding online harassment, protecting intellectual property and using digital resources responsibly.
- **Legal awareness** involves understanding that online actions can have legal consequences and that cybercrime should be reported through appropriate channels.

An effective cyber awareness programme should address all four dimensions. A purely technical approach may fail to address misinformation, online harassment, privacy violations, and irresponsible digital communication.

III. MAJOR CYBER THREATS

A. Phishing and Social Engineering

Phishing is a cyberattack in which phony emails or websites pose as reputable businesses or people in order to steal private information. Messages on scholarships, test scores, admissions, internships, jobs, or account verification may be sent to students. These messages frequently instill a sense of urgency or provide alluring rewards. They might lead kids to phony websites that are intended to gather bank account information, passwords or other private data. A more comprehensive method known as "social engineering" uses human emotions, trust, fear, curiosity or urgency to sway behavior. A fake caller may pose as a customer service agent, bank representative, college administrator or police officer.

Purkait's (2013) study of anti-phishing awareness among Indian undergraduate students highlighted the vulnerability of students to deceptive online environments. This suggests that awareness programmes should teach students to evaluate messages critically rather than simply recognise the word phishing.

B. Online Financial Fraud

Students now have an easier time making financial transactions because to the growth of digital payments. However, there are serious risks associated with fraudulent money requests, phony QR codes, impersonation schemes and deceptive job or investment proposals.

Social media ads, messaging apps, or phone calls that promise fast money, scholarships, awards, or part-time work may be used to target students.

The fact that a UPI PIN is used to authorize a payment rather than only to receive money is a basic safety principle. PINs, passwords, and one-time passwords (OTPs) should never be shared by students with callers posing as representatives of banks or payment services. Financial awareness should also include verifying payment recipients, reviewing transaction details, and reporting suspected fraud promptly.

C. Identity Theft and Privacy Violations

By using unreliable websites and programs to share identity papers, phone numbers, personal photos, addresses or account credentials, college students may put themselves at risk. Additionally, malicious software, phony employment websites, online tests and false requests for document verification can all be used to obtain personal data. Students should be aware that material supplied online can be replicated, saved, shared or misused outside of its intended context. Making thoughtful choices about what information to share, with whom and for what reason is consequently necessary to maintain privacy.

D. Cyberbullying and Online Harassment

Cyberbullying refers to the use of digital communication to threaten, intimidate, humiliate, or repeatedly harass another person. It may occur through social networking platforms, messaging applications, online groups, or anonymous accounts. Common forms include spreading rumours, posting insulting comments, circulating private photographs without consent, impersonating individuals and deliberately excluding people from online communities.

Cyberbullying can undermine students' confidence, concentration, social relationships and sense of security. Educational institutions should provide confidential reporting channels, counselling support where appropriate and clear procedures for responding to complaints.

Students must understand that online communication does not remove the obligation to respect another person's dignity.

E. Misinformation, Disinformation and Deepfakes

AI-generated deepfakes, fake movies, altered photos and misleading news could mislead pupils and sway public opinion. False or erroneous information disseminated without necessarily aiming to mislead is referred to as misinformation. The ability to comprehend and apply artificial intelligence responsibly while being aware of its possible cybersecurity concerns is known as AI Cyber Awareness. In addition to safeguarding personal data when utilizing AI tools, it involves spotting deepfakes, voice-cloning schemes, AI-assisted phishing attempts and misinformation produced by AI. Because generative AI is developing so quickly, fraudsters may produce incredibly convincing phony messages, pictures, videos and voice recordings to trick people and influence their choices. When college students believe digital content without checking its legitimacy, they may be exposed to such hazards. As a result, pupils should acquire digital literacy, critical thinking skills, and the capacity to discern between authentic information and content created or altered by AI. Additionally, they should be aware of the privacy consequences of sharing sensitive data and use caution when uploading financial, academic, or personal information to AI platforms. Respect for

ISSN: 3107-6513

intellectual property, academic honesty, transparency and ethical values are also necessary for the responsible use of AI. To educate students for new digital issues, higher education institutions should host talks on AI-related concerns, practical workshops and awareness campaigns. The intentional production or dissemination of misleading information in order to deceive others is known as disinformation. Developing knowledgeable, watchful and morally upright digital citizens who can use AI safely and productively can be facilitated by incorporating AI cyber awareness into higher education.

Students should check publication dates, compare information from several trustworthy sources, confirm the original source of a claim and refrain from sending unverified content. Additionally, content produced by AI should be verified by reliable sources. Thus, media literacy and cybersecurity awareness must to be taught concurrently.

F. Malware, Unsafe applications and Public Wi-Fi

Malware, also referred to as malicious software, has the ability to corrupt devices, steal data, track behavior, or interfere with computer systems. Unsafe downloads, dubious email attachments, phony apps and hacked websites can all expose students to malware.

Risks can also arise from public Wi-Fi networks, especially when users disregard security alerts or use unprotected connections to access important accounts.

Installing software updates, using reputable app stores, avoiding unfamiliar attachments, turning on device locks and using secure connections for crucial transactions are all recommendations for students. They should never try to access systems without authorization or get around institutional security measures.

IV. AWARENESS VS ACTUAL BEHAVIOUR

The distinction between knowing what is safe and regularly putting it into practice is one of the main concerns in cybersecurity education. Even when a student knows that passwords shouldn't be shared, they could nonetheless use the same password for multiple accounts. Even though they are aware of the dangers of dubious links, someone else might click on one when a message seems to be from a reliable source. Convenience, overconfidence, a lack of real-world experience, peer pressure, time constraints or the compelling design of false messaging can all contribute to this gap.

This issue has been investigated from several angles by research involving university and undergraduate students. Hazarika (2025) looked at social media usage and cybersecurity breaches among Indian undergraduate students. Begum (2024) investigated cyber-safety awareness among Bengaluru college students. These studies add to the expanding body of knowledge regarding students' understanding, experiences, and online safety behaviors. This suggests that written instructions and lectures should not be the only methods used in cybersecurity education. Students should get the chance to evaluate hypothetical online situations, practice spotting questionable messages, and learn how to report instances. Practical training, repeated reminders, and supportive institutional policies can help translate awareness into safer behaviour.

V. RESPONSIBLE SOCIAL MEDIA USE

Social media now plays a significant role in the academic, social, and professional life of college students. It gives opportunities for cooperation, information exchange, networking and creative expression. However, excessive or negligent use could put students at risk for harassment, disinformation, privacy violations, and reputational harm. Students should check their privacy settings, limit access to private data, and exercise caution when interacting with strangers. They should refrain from needlessly disclosing financial information, passwords, personal papers, or real-time location information.

Respecting permission is another essential component of responsible social media use. It is improper to publish or distribute someone else's images, videos, private messages or personal information without their consent. It's important for students to keep in mind that online content could still be available years after it was first published. Careless posts can have an impact on future career, academic prospects and interpersonal connections. Thus, digital citizenship entails striking a balance between the right to free speech and accountability, decency and regard for others.

VI. ROLE OF HIGHER EDUCATION INSTITUTIONS

Higher education institutions have a significant responsibility to prepare students for safe participation in digital society. Cyber awareness should be integrated into institutional culture rather than treated as an occasional activity.

- **Integration into the Curriculum:** Essential cybersecurity principles should be included in relevant undergraduate courses, value-added programs, skill-development modules and digital literacy efforts offered by colleges. Basic cybersecurity knowledge is necessary for students in the arts, sciences, business and professional fields. It shouldn't be limited to students studying computer science.
- **Workshops and Awareness Seminars:** Regular seminars and workshops can introduce students to phishing, financial fraud, data privacy, cyberbullying, safe browsing and incident reporting. Cybersecurity professionals, law enforcement representatives, digital literacy experts and trained faculty members may contribute to these activities.
- **Practical Demonstrations:** Students can recognize dubious email addresses, verify the legitimacy of websites, spot deceptive QR-code requests and set up safe account settings with the aid of hands-on demonstrations. Any simulated phishing activity should be approved, private and intended to teach rather than to humiliate or punish.
- **Institutional Cybersecurity Policies:** Colleges should develop clear policies concerning the use of institutional email, learning management systems, computer laboratories, Wi-Fi networks and digital records. Access permissions, secure authentication, software updates, backups and responsible data handling should be maintained according to institutional requirements.
- **Student Cyber Awareness Clubs:** Cyber awareness clubs run by students might provide peer-learning sessions, poster contests, tests, demonstrations and discussions. By encouraging students to share factual information with

ISSN: 3107-6513

their families and communities, these activities can raise awareness outside of the classroom.

- **Collaboration with Government Initiatives:** Government-developed cybersecurity awareness programs and resources are available for use by Indian educational institutions. Cybersecurity awareness resources are published by CERT-In, and cybersecurity knowledge and digital safety are promoted through the Information Security Education and Awareness (ISEA) program. Additionally, the Ministry of Education offers higher education institutions a cyber hygiene manual. Structured campus programs can be supported by these resources.

VII. RECOMMENDED CYBER SAFETY PRACTICES

Cyber safety is the most important thinking in the digital age. Most of the students in colleges and universities use mobile phones or laptops or other digital devices for financial transactions. Some of the recommended use for safety purposes is as follows:

- **Password and account security:** Use strong, unique passwords and enable multifactor authentication wherever available. Never share account credentials with friends or unknown individuals.
- **Device security:** Keep operating systems and applications updated. Use screen locks and download software only from trusted sources.
- **Link verification:** Examine unexpected links and attachments carefully. Access banking, examination, scholarship and government services through verified official websites.
- **Financial protection:** Never disclose a UPI PIN, OTP, or banking password. Verify payment requests independently and contact the bank promptly if fraud is suspected.
- **Privacy protection:** Share only necessary personal information. Review application permissions and social media privacy settings.
- **Responsible communication:** Do not harass others, spread rumours, impersonate people, or circulate private content without consent.
- **Incident reporting:** Preserve relevant evidence and report cyber incidents through appropriate official channels. In India, suspected cybercrime can be reported through the National Cyber Crime Reporting Portal at https://www.cybercrime.gov.in. For urgent reporting of cyber financial fraud, the national helpline number is **1930**.
- **Continuous learning:** Cyber threats evolve, so students should regularly update their knowledge through reliable educational resources and institutional training. Students from a variety of academic fields and socioeconomic backgrounds should be able to participate in the awareness program. Activities should refrain from gathering needless personal information and should not reveal the errors or experiences of specific pupils. Changes in knowledge, performance in simulated circumstances, comprehension of reporting processes and self-reported adoption of safe behaviors can all be used to gage how effective it is. While maintaining participant privacy, the institution may compare baseline and follow-up outcomes where practical.

VIII. CONCLUSION

College students' cyber awareness is a crucial component of modern higher education. While digital technologies have made learning, communication, research and job prospects more accessible, they have also made people more vulnerable to financial fraud, phishing, identity theft, cyberbullying, privacy violations, and false information. Lack of knowledge is not the main problem. It is the challenge of converting information into responsible and consistent online behavior. Students need to learn how to recognize dangers, safeguard personal data, critically assess digital content, respect others' privacy and promptly report cyber occurrences.

Through curricular integration, hands-on workshops, student-led campaigns, explicit institutional rules and cooperation with government cybersecurity programs, colleges and universities can address these issues. To create a safer digital learning environment, educators, administrators, students and technology experts must work together. Therefore, it is important to view cyber awareness as an ongoing process that involves ethical principles, practical skills, information and responsible decision-making. Higher education institutions may safeguard their communities and equip students to engage in an increasingly digital world with confidence and responsibility by funding cybersecurity instruction. Ultimately, the objective is not merely to produce technologically skilled graduates but to develop informed, ethical, vigilant and responsible digital citizens.

REFERENCES

[1] N. Begum, "Cyber safety consciousness among the students pursuing higher education: A study of selected colleges and universities in Bengaluru—the capital city of Karnataka", Indian Journal of Public Administration, 70(3), 2024. https://doi.org/10.1177/00195561241271582.

[2] CERT-In. (n.d.), Awareness booklets, Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology, Government of India. https://www.cert-in.org.in/AwarenessBooklets.jsp.

[3] H. J. Hazarika, "Impact of cybersecurity breaches on social media: A case study on undergraduate students", Information Polity, 2025. https://doi.org/10.1177/09557490251340833.

[4] Ministry of Electronics and Information Technology, Government of India. (n.d.), Information Security Education and Awareness (ISEA) programme. https://isea.gov.in/about/

[5] Ministry of Education, Government of India. (n.d.), Publications: Handbook on basics of cyber hygiene for higher education institutions, University Grants Commission. https://www.ugc.gov.in/publication/ebook.

[6] S. Purkait, "Assessing anti-phishing awareness among undergraduate students in India", International Journal of Applied Research on Information Technology and Computing, 4(1), 2023, pp. 26–41. https://doi.org/10.5958/j.0975-8089.4.1.003.

[7] National Cyber Crime Reporting Portal. (n.d.), Report cybercrime, Government of India. https://www.cybercrime.gov.in/

[8] National Council of Educational Research and Training. (n.d.). *Cyber hygiene*. Central Institute of Educational Technology. https://www.ciet.ncert.gov.in/activity/chyg.