



A Study on Cybercrime Awareness Among Undergraduate Students in India: An Empirical-Analytical Review Based on Recent Indian Evidence

*Durgesh Patel

Indira Gandhi Krishi Vishwavidyalaya, Raipur, Chhattisgarh, India

*Corresponding Author's email: ajaypatel2552003@gmail.com

The rapid expansion of smartphones, social media, online learning, digital payments and cloud-based academic services has increased the exposure of undergraduate students to cyber risks. This article examines cybercrime awareness among undergraduate students in India by synthesizing recent Indian studies and national cybercrime statistics. The review focuses on awareness of phishing, malware, identity theft, financial fraud, social engineering, privacy risks, password security, multi-factor authentication and cybercrime reporting. Recent evidence shows an important gap between students' familiarity with digital technologies and their practical cybersecurity preparedness. For example, a 2025 study of 185 undergraduate students in Arunachal Pradesh reported that only 10.81% demonstrated high cybercrime awareness, while most students fell in moderate or low awareness categories. A 2025 case study of 300 undergraduate students in Assam reported that 72% claimed awareness of threats such as phishing, malware and identity theft, but only 25% had received formal cybersecurity training. At the national level, NCRB data recorded 86,420 cybercrime cases in India in 2023, up from 65,893 in 2022; fraud accounted for 59,526 cases, or 68.9% of registered cybercrime cases. The evidence indicates that cyber safety education should move beyond general awareness and develop practical skills, including verification of messages and links, privacy management, secure authentication, incident reporting and recognition of social-engineering tactics. The article concludes with recommendations for universities, teachers, students and policymakers and identifies directions for future empirical research.

Keywords: Cybercrime awareness; undergraduate students; cybersecurity; phishing; digital literacy; social engineering; online safety; India; higher education

Introduction

Digital technology has become an integral part of undergraduate education in India. Students routinely use smartphones and laptops for learning management systems, email, social networking, online examinations, digital payments, file sharing and communication. This digital dependence creates substantial educational opportunities, but it also creates opportunities for cybercriminals to exploit weak passwords, excessive trust, poor privacy settings, phishing messages, malicious links, impersonation and financial scams. Cybercrime awareness should therefore be understood as more than knowing that cybercrime exists. Effective awareness includes the ability to recognize common threats, judge the credibility of digital requests, protect personal and academic information, use secure authentication practices, and know how and where to report an incident. The distinction between technological familiarity and security competence is important because students may be highly active online without consistently applying protective behaviors. The national context demonstrates the scale of the problem. According to the National Crime Records Bureau (NCRB), 86,420 cybercrime cases were registered in India in 2023, compared with 65,893 in

2022, representing a 31.2% increase. Fraud was the recorded motive in 59,526 cases in 2023, accounting for 68.9% of cybercrime cases in the NCRB classification (NCRB, 2023). These figures concern registered cases and should not be interpreted as the total prevalence of cyber incidents, because many incidents may remain unreported.

Objectives of the Study

- To examine the level and dimensions of cybercrime awareness among undergraduate students in India.
- To identify major cyber threats relevant to undergraduate students, including phishing, malware, identity theft, financial fraud and social engineering.
- To synthesize recent empirical evidence from Indian higher-education settings.
- To examine the gap between awareness, formal cybersecurity training and practical safety behavior.
- To suggest measures for strengthening cyber safety education in universities and colleges.

Research Questions

- What is the reported level of cybercrime awareness among undergraduate students in different Indian settings?
- Which cyber threats and safety practices appear to be least understood?
- Does access to technology or general digital familiarity necessarily translate into secure online behavior?
- What role can higher-education institutions play in improving practical cyber safety and reporting awareness?

Methodology

This article uses a structured narrative review and secondary-data synthesis rather than presenting newly collected primary survey data. The evidence base consists of recent peer-reviewed or journal-published studies concerning Indian undergraduate or higher-education students, supplemented by official Indian government sources, particularly NCRB/Open Government Data and the National Cyber Crime Reporting Portal. Studies were selected because they directly addressed cybercrime/cybersecurity awareness, cyber-safety consciousness, phishing awareness or related protective behavior among students. Because the included studies differ in sample size, location, instruments and sampling methods, their percentages are not pooled into a single national prevalence estimate. Instead, each finding is presented in its original study context. This is important because evidence from one university, district or state cannot automatically be generalized to all undergraduate students in India.

National Cybercrime Context in India

NCRB's Crime in India 2023 data show that registered cybercrime cases increased from 65,893 in 2022 to 86,420 in 2023. The increase illustrates the growing importance of cyber safety, although registration trends can be influenced by reporting behavior, police capacity and changes in classification or awareness.

Year	Registered cybercrime cases	Change	Selected observation
2020	50,035	—	Official NCRB/PIB series
2021	52,974	+5.9%	Increase over 2020
2022	65,893	+24.4%	Increase over 2021
2023	86,420	+31.2%	68.9% had fraud as recorded motive

Source: NCRB, Crime in India 2023; Ministry of Home Affairs/PIB summaries. Percent changes calculated from the reported counts. The 2023 motive distribution reported 59,526 fraud-motivated cases out of 86,420 total cases.

Evidence from Indian Undergraduate and Higher-Education Studies

Arunachal Pradesh: descriptive evidence

Ering, Ering and Rajhans (2025) investigated cybercrime awareness among 185 undergraduate students across three colleges in Arunachal Pradesh. Using a standardized Cybercrime Awareness Scale, the study reported that 10.81% of students demonstrated high awareness, while the majority were in moderate or low awareness categories. The authors also reported no statistically significant difference by gender or academic stream. The study supports the view that general student status or academic discipline alone does not guarantee strong cybercrime awareness.

Assam: awareness versus formal training

Hazarika (2025) examined cybersecurity breaches and social-media use among 300 undergraduate students at The Assam Royal Global University. The study reported that 72% of participants claimed awareness of threats including phishing, malware and identity theft, whereas only 25% had received formal cybersecurity training. This difference is important: self-reported awareness can coexist with limited structured training, suggesting that universities may need to provide repeated, practical cybersecurity education rather than relying on students' informal digital experience.

Bengaluru: cyber-safety consciousness in higher education

Begum (2024) studied cyber-safety consciousness among students in selected colleges and universities in Bengaluru. The study discusses the role of government initiatives, UGC and AICTE and emphasizes institutional measures for creating a safer virtual environment for students. Its findings are useful for understanding cyber safety as an institutional responsibility rather than solely an individual responsibility.

Rural higher-education students

Kumbhakar and Kumar (2025) examined cyber-security awareness among rural undergraduate and postgraduate students in India using a self-constructed Cyber Security Awareness Test. Among 148 participants, the reported mean score was 16.30 (SD = 4.97), and 39.19% scored below the mean. The study identified gaps in concepts including phishing, multi-factor authentication and pretexting. These results indicate that cybersecurity education should address both basic concepts and practical recognition of social-engineering techniques.

Nursing students in Nashik

Chaudhari et al. (2021) assessed cybercrime and cyber-safety awareness among 60 undergraduate nursing students in Nashik. The study reported a low level of cyber-safety knowledge and found associations with several demographic and internet-use characteristics. Although the sample was small and institution-specific, the study illustrates that cyber-safety gaps can occur among students in professional courses as well as in technology-oriented disciplines.

Phishing awareness among Indian undergraduates

Purkait (2013) investigated anti-phishing awareness among undergraduate students in India using a simulated phishing scenario. The study reported that students, including those with computer knowledge, visited the simulated phishing website while overlooking browser security information. This older study remains relevant because phishing depends not only on technical knowledge but also on attention, judgment and susceptibility to persuasive cues. Its age should, however, be considered when applying the finding to today's platforms and threat environment.

Comparative Summary of Selected Evidence

Study	Location/context	Sample	Key reported finding	Main implication
Ering et al. (2025)	Arunachal Pradesh	185 UG students	10.81% high awareness; majority moderate/low	Need structured cyber-safety education

Study	Location/context	Sample	Key reported finding	Main implication
Hazarika (2025)	Assam Royal Global University	300 UG students	72% reported threat awareness; 25% formal training	Awareness does not equal training
Kumbhakar & Kumar (2025)	Rural India	148 UG/PG students	39.19% scored below sample mean	Gaps in phishing, MFA and pretexting
Chaudhari et al. (2021)	Nashik	60 nursing UG students	Reported poor cyber-safety knowledge	Professional students also need targeted education
Purkait (2013)	India	UG students	Students overlooked phishing/security cues	Practical phishing education is important

Note: These studies use different instruments and samples. Their percentages should not be interpreted as a pooled national estimate.

Major Dimensions of Cybercrime Awareness

Phishing and social engineering: Students should be able to identify suspicious links, urgent requests, impersonation, fake rewards, fake academic notices and requests for credentials or payment.

Password and authentication security: Awareness should include unique passwords/passphrases, password-manager use where appropriate, and multi-factor authentication for important accounts.

Privacy and identity protection: Students should understand the risks of oversharing personal information, public profiles, insecure permissions and reuse of personal identifiers.

Financial cyber fraud: Awareness is especially important for UPI, banking and online shopping because fraud was the most common recorded motive in NCRB's 2023 cybercrime classification.

Malware and unsafe downloads: Students should recognize risks from unknown attachments, cracked software, suspicious applications and untrusted downloads.

Cyberbullying, harassment and stalking: Cyber safety education should also address abusive communication, impersonation, non-consensual sharing and appropriate reporting channels.

Incident reporting: Awareness is incomplete if students do not know what to do after an incident. In India, the National Cyber Crime Reporting Portal and helpline 1930 provide official reporting routes, including for online financial fraud.

Discussion

The reviewed evidence suggests three broad patterns. First, undergraduate students are digitally active but awareness levels are uneven. Second, knowing the names of cyber threats is not equivalent to possessing practical protective skills. The difference between 72% self-reported awareness and 25% formal training in the Assam study is a useful illustration, although it should not be generalized to all Indian students. Third, cyber safety needs to be treated as a recurring educational competency. Threats, interfaces and scam techniques change quickly, so a one-time orientation session may have limited long-term value. The evidence also cautions against equating academic or technical background with cybersecurity competence. The Arunachal Pradesh study did not find significant differences by academic stream, while the earlier phishing study showed that computer knowledge did not necessarily prevent students from interacting with a simulated phishing website. These findings point toward the importance of behavioral training, realistic examples and repeated practice.

At the institutional level, colleges and universities can strengthen cyber resilience through induction modules, periodic phishing-awareness exercises conducted ethically, short digital-safety assessments, clear incident-reporting procedures, and integration of cyber safety into student orientation and digital-literacy programmes. Institutions should also communicate that reporting an incident promptly is preferable to hiding it out of embarrassment or fear.

Recommendations

- Introduce a compulsory short cyber-safety module for first-year undergraduate students.
- Use practical scenario-based exercises on phishing, impersonation, fake scholarship/job messages, account takeover and digital-payment fraud.
- Teach multi-factor authentication, secure password practices, privacy settings and device-update habits.
- Display clear institutional reporting channels and link students to official cybercrime reporting mechanisms.
- Conduct refresher awareness activities at least once each academic year because cyber threats evolve.
- Train faculty and administrative staff because students may receive fraudulent messages impersonating institutional authorities.
- Develop targeted modules for non-technical disciplines rather than assuming that cybersecurity is relevant only to computer-science students.
- Encourage universities to conduct local baseline surveys before and after awareness programmes so that interventions can be evaluated.
- Include digital ethics, consent, privacy, cyberbullying and responsible social-media use alongside technical security.

Limitations

This article is a secondary synthesis and does not claim to represent a new national survey. The cited studies differ in geography, sample size, sampling method, measurement instruments and definitions of awareness. Some are institution-specific and therefore cannot be generalized to all Indian undergraduates. In addition, NCRB figures represent registered cases and do not measure the full number of cyber incidents. Future research should use larger, multi-state probability samples and validated instruments, and should measure actual behavior—not only self-reported awareness.

Conclusion

Cybercrime awareness is an increasingly important component of undergraduate education in India. National crime data show a substantial rise in registered cybercrime, while student-focused studies reveal uneven awareness and a recurring gap between general familiarity with cyber threats and formal cybersecurity training. The available evidence supports a shift from occasional awareness campaigns toward continuous, practical and institutionally supported cyber-safety education. Universities can contribute significantly by teaching students how to recognize manipulation, protect accounts and personal information, respond to financial or identity-related incidents, and report cybercrime promptly. A safer digital learning environment ultimately depends on a combination of informed student behavior, responsible institutional practices and accessible reporting mechanisms.

References

1. Begum, N. N. (2024). 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), 579–592. <https://doi.org/10.1177/00195561241271582>
2. Chaudhari, M. S., Dulgaj, B., Valvi, K., Valvi, M., Dive, N., Kothwal, S., & Shaikh, T. (2021). A study to assess the awareness regarding cybercrime and cyber safety among undergraduate students from selected nursing institute of Nashik City. *International*

- Journal of Advances in Nursing Management*, 9(1), 84–86. <https://doi.org/10.5958/2454-2652.2021.00021.4>
3. Ering, O., Ering, M., & Rajhans, R. (2025). Cybercrime Awareness Among Undergraduate Students: A Descriptive Study. *International Journal of Scientific Research in Science and Technology*, 12(2), 1346–1352. <https://doi.org/10.32628/IJSRST251222733>
 4. Hazarika, H. J. (2025). Impact of cybersecurity breaches on social media: A case study on undergraduate students. [Research article]. <https://doi.org/10.1177/09557490251340833>
 5. Kumbhakar, M. M., & Kumar, N. (2025). Cyber Security Awareness Among Higher Education Students. *National Journal of Education*, 23(1). Banaras Hindu University.
 6. Ministry of Home Affairs, Government of India. (2024). Increase in Cyber Crimes. Press Information Bureau, 7 February 2024. (NCRB data for 2020–2022).
 7. Ministry of Home Affairs, Government of India / National Crime Records Bureau. (2026). Crime in India – 2023. Open Government Data Platform India.
 8. Purkait, S. (2013). Assessing Anti-Phishing Awareness among Undergraduate Students in India. *International Journal of Applied Research on Information Technology and Computing*, 4(1), 26–41. <https://doi.org/10.5958/j.0975-8089.4.1.003>
 9. Indian Cyber Crime Coordination Centre (I4C). (n.d.). National Cyber Crime Reporting Portal and Cyber Crime Helpline 1930. Government of India. <https://cybercrime.gov.in/>