ISSN- 2349-7076

EduInspire-An International E-Journal
An International Peer Reviewed and Referred Journal (www.ctegujarat.org)
Council for Teacher Education Foundation (CTEF, Gujarat Chapter)
Patron: Prof. R. G. Kothari
Chief Editor: Prof. Jignesh B. Patel
Email:- Mo. 9429429550 ctefeduinspire@gmail.com

EduInspire

- An International Peer Reviewed and Refereed Journal

Vol: XIII
Issue: I
January-2026

Patron
Prof. R. G. Kothari

Chief Editor
Prof. Jignesh B. Patel
Mo. 9429429550
drjigp@gmail.com
ctefeduinspire@gmail.com

Council for Teacher Education Foundation

(CTEF, Gujarat Chapter)

ISSN- 2349-7076

EduInspire-An International E-Journal
An International Peer Reviewed and Referred Journal (www.ctegujarat.org)
Council for Teacher Education Foundation (CTEF, Gujarat Chapter)
Patron: Prof. R. G. Kothari
Chief Editor: Prof. Jignesh B. Patel
Email:- Mo. 9429429550 ctefeduinspire@gmail.com

Knowledge of Cybercrime Reporting Procedures and Perceived Need for Training Among Undergraduates in Rural Assam

Birina Das
Research Scholar
Department of Extension and Communication, The Maharaja Sayajirao University of Baroda, Vadodara
birina.d-extcommphd@msubaroda.ac.in

Avani Maniar
Professor
Department of Extension and Communication, The Maharaja Sayajirao University of Baroda, Vadodara

Abstract

As cybercrime increases, undergraduate students face greater risks. This study looks at how prepared undergraduates in Kamrup rural district, Assam, are for cyber threats. The research focused on two main goals: understanding how well students know the steps for reporting cybercrime and finding out if they feel the need for cybersecurity training. Using a descriptive survey of 60 college students, the study found that most students lacked knowledge about what to do after a cybercrime. Many did not know the official reporting process (80%), the government website (76.67%), or the helpline number (80%). Few had any direct or indirect experience with reporting, as 86.67% did not know anyone who had reported a cybercrime. This lack of information made students feel vulnerable—83.33% felt unsafe online, and 73.33% did not think they could handle a cybercrime. The study highlights a gap between students' knowledge of reporting procedures and their feelings of vulnerability. It calls for schools and policymakers to provide accessible cybersecurity training to help rural students stay safe online.

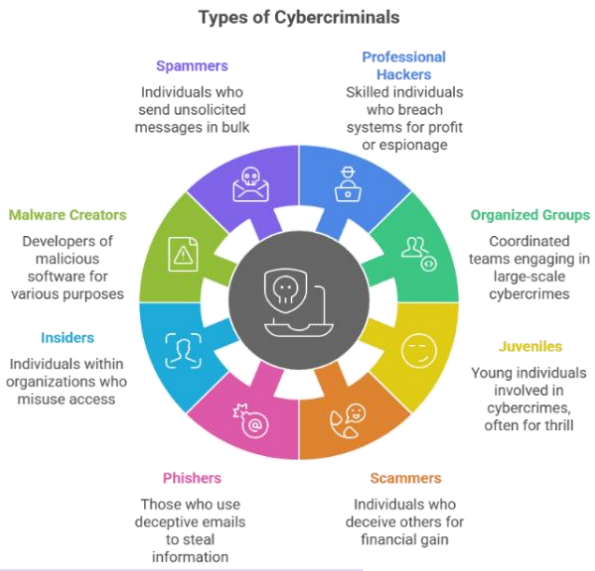
Keywords: Cybersecurity; Cybercrime reporting; Undergraduates; Rural youth; Digital literacy

Introduction

Any illegal activities that use computers or networks is cybercrime. These crimes can involve computers as tools, targets, or both. In simple terms, cybercrime means using electronic communication to commit unlawful acts, often by stealing or changing information online (Information Technology Act, 2000). Cybercrime is changing quickly, with more people

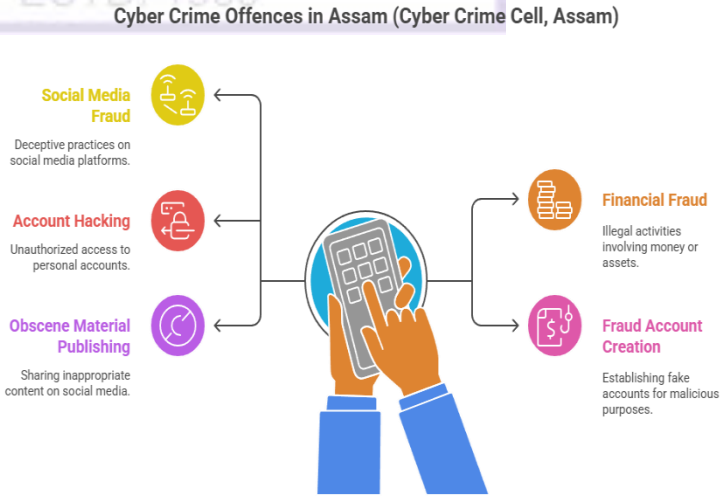
EduInspire-An International E-Journal
An International Peer Reviewed and Referred Journal (www.ctegujarat.org)
Council for Teacher Education Foundation (CTEF, Gujarat Chapter) Email:- ctefeduinspire@gmail.com

using the internet for different types of illegal activities. In the past, these crimes were usually done by individuals or small groups.



Over the last ten years, cybercrime in India has grown a lot. In just the first three months of 2020, **India** faced **3.3 million cyberattacks** (Shinde, 2021). (A Comprehensive Analysis on Jurisdiction Issues in Cyber Crimes, 2021) The Economic Times reported that these attacks cost the government about **₹1.25 lakh crore each year** (Press Trust of India, The Economic Times; 2020). In recent years, Assam has emerged as one the states with highest number of cybercrimes. Assam had a 4.9% cybercrime rate in 2022, ranking fifth among Indian states (NCRB, 2022). (Crime in India 2022, 2022) However, the disappointing fact is that Assam had one of the lowest charge-sheeting rates at only 14%. (Assam CM Sarma urges people to be cautious of cybercrime, 2024) This gap shows a problem between how justice is carried out and the amount of crime. One possible reason for this gap is that people are not aware of how and when to report cybercrimes.

Though these technical solutions are important, the human element cannot be neglected. Cybercrime rate is rising and the sophistication of cybercrimes are developing and, in this scenario, low level of awareness or knowledge regarding how to deal with these cybercrimes can be a critical factor in cyber victimization. There is clear need to shift from remedial session to proactive empowerment of citizens. Determining the need for specialist cybersecurity training is one of the most crucial elements in building a society that is both security-conscious and capable of fending off digital attacks.



EduInspire-An International E-Journal
An International Peer Reviewed and Referred Journal (www.ctegujarat.org)
Council for Teacher Education Foundation (CTEF, Gujarat Chapter) Email:- ctefeduinspire@gmail.com

Review of Literature

The study conducted by **Ering et al. (2025)** found that undergraduate (UG) students in Arunachal Pradesh had a moderate-to-low level of awareness is in line with a larger pattern seen in both domestic and foreign literature. Cybercrime awareness is an essential part of digital citizenship since the internet has permeated almost every aspect of life, including higher education.

In **Conway & Hadlington's (2018)** qualitative study, they looked at how English undergraduate students comprehend terms and ideas associated with cybercrime. The researchers performed an inductive, thematic analysis using three focus groups with sixteen students between the ages of eighteen and twenty-one. The distinctions between the real and virtual worlds, misunderstandings regarding cybercrime laws and the perception that police are uninterested in cybercrime cases, the normalization of risky online behavior, and individual victimization experiences were among the major themes. The results showed a general ambivalence about personal risk and misconceptions about cybercrime. The study calls for more research on how training can alter perceptions and lessen vulnerability and suggests that focused education and awareness programs could assist at-risk groups in adopting effective protective behaviors.

Rosanwo (2023) found that at Obafemi Awolowo University, the main reasons for cybercrime were financial pressure, social influence, and weak laws. (Rosanwo & Obalaja, 2023) Students were influenced by frequent opportunities and by learning from others. The research suggests that more funding, awareness campaigns, better cybersecurity education, and stronger laws could help reduce student involvement in cybercrime.

Sayyad et al. (2023) studied 50 college students in Narhe and found that most felt secure online, used antivirus software, and were aware of cybercrime. Although few had experienced cybercrime themselves, they knew how to secure their devices, avoided risky websites, and supported laws against cybercrime.

Toso et al. (2023) studied 253 senior high school students in the Philippines and found they were highly aware of cybercrime, especially issues like identity theft, cyberbullying, and cyberpornography. (Toso et al., 2023) The results showed that young people are alert to common online dangers.

Jonathan et al. (2021) found that interventions on cybercrime increase students' knowledge of cyber threats and their consequences. Such awareness may prevent malicious acts and promote ethical online behavior, as well as inspire students to pursue positive cyber career paths.

EduInspire-An International E-Journal
An International Peer Reviewed and Referred Journal (www.ctegujarat.org)
Council for Teacher Education Foundation (CTEF, Gujarat Chapter) Email:- ctefeduinspire@gmail.com

Rationale

The increase in internet usage in India, especially after Covid 19 has exposed both the students and adults to the risks of cybercrimes. Cyberbullying, phishing, identity theft and financial frauds have become common among the student and adult community (Rajasekharaiah et al., 2020; Singh, 2020). Cybercrime cases against children have sharply increased over last decades, and older adults are particularly vulnerable because of their high levels of trust and low digital literacy (Hart, Chaparro, & Halcomb, 2008; Havers et al., 2024). (NCRB data shows surge in cybercrime, spike in crimes against children, 2025)

Despite the high prevalence of cyber crimes across all age groups, the reporting of the cases is comparatively low in India due to lack of awareness, fear of retaliation and low confidence in the legal system (Singh & Sharma, 2025). (Cyber Victimization of Women in Assam: Types, Issues and Challenges, 2025) However, only exploring the need for technical solutions is not enough if the individuals do not have and feel the interest to equip themselves with cyber security knowledge. Thus, the present study investigates the respondents' knowledge about cybercrime reporting process and also their interest to upgrade themselves with the preventive knowledge through intervention programmes.

Research Questions

1. What is the current level of awareness and knowledge among respondents regarding the official procedures for reporting cybercrime?
2. Do respondents perceive a need for cybersecurity training programs?
3. What is the level of willingness among respondents to participate in cybersecurity training programs?

Objectives

1. To assess the level of awareness and knowledge among respondents regarding the official procedures for reporting cybercrime.
2. To evaluate the perceived need for, and willingness to participate in, cybersecurity training programs among respondents.

Methodology

Research design

The study adopted a descriptive survey design for examining knowledge of cybercrime reporting procedures and perceived need for training among undergraduates in Rural Assam.

Population of the present study

EduInspire-An International E-Journal
An International Peer Reviewed and Referred Journal (www.ctegujarat.org)
Council for Teacher Education Foundation (CTEF, Gujarat Chapter) Email:- ctefeduinspire@gmail.com

The study was carried out in the Kamrup rural district of Assam and the population consisted of under graduate college students.

Sample of the study

Two colleges (Dakshin Kamrup Girls' College and Dakshin Kamrup College) Kamrup rural district of Assam was selected. 60 samples were drawn purposively.

Tool for data collection

A questionnaire was prepared by the investigator for the target groups tailored to need. Questionnaire was divided into 3 sections. First section consisted of background profile of the respondents. The second section consisted of information knowledge of cybercrime reporting process among respondents and the third section consisted of information about perceived need for training among undergraduates.

Method of data collection

Through online google forms, data was collected and consent was taken electronically from the respondents.

Data analysis

The data analysis was done using descriptive statistics (frequency and percentage).

Ethical considerations

Informed consent was obtained electronically from every respondent, ensuring voluntary participation. Confidentiality was also maintained to protect the privacy of the respondents.

Findings

Section – A

Table 1: Demographic Profile

Category	Frequency (*f*)	Percentage (%)
	Age	
18 years	12	20.00
19 years	15	25.00
20 years	15	25.00
21 years	18	30.00
	Sex	
Male	31	51.67
Female	29	48.33

Table 1 reveals that among the college students, 30 per cent were 21 years and little over the half were males.

EduInspire-An International E-Journal
An International Peer Reviewed and Referred Journal (www.ctegujarat.org)
Council for Teacher Education Foundation (CTEF, Gujarat Chapter) Email:- ctefeduinspire@gmail.com

Section – B

General Awareness of Reporting Procedures

Table 2: Respondents' distribution of frequency and percentage according to their information on whom to approach in case of cybercrime victimisation.

Category	Frequency (*f*)	Percentage (%)
Yes	18	30.00
No	42	70.00
Total	**60**	**100.00**

A large majority (80%) of respondents displayed a fundamental lack of knowledge about how to respond to cybercrime or whom to approach in case of cyber victimisation.

Table 3: Information of cybercrime reporting process

Category	Frequency (*f*)	Percentage (%)
Yes	12	20.00
No	48	80.00
Total	**60**	**100.00**

Table 3 indicates a larger majority, 80 per cent, confirming that they had no information on the official cybercrime reporting process itself.

Practical and Vicarious Experience with Reporting

Table 4: Frequency and percentage distribution of respondents according to their provided assistance to someone in reporting a cybercrime

Category	Frequency (*f*)	Percentage (%)
Yes	17	28.33
No	25	71.67
Total	**60**	**100.00**

The data indicates that exposure to the reporting process, either personally or through social networks, is exceptionally low, i.e., 28.33 per cent only.

Table 5: Frequency and percentage distribution of respondents according to reporting to cybercrime by a person known to them

Category	Frequency (*f*)	Percentage (%)
Yes	8	13.33
No	52	86.67
Total	**60**	**100.00**

EduInspire-An International E-Journal
An International Peer Reviewed and Referred Journal (www.ctegujarat.org)
Council for Teacher Education Foundation (CTEF, Gujarat Chapter) Email:- ctefeduinspire@gmail.com

Table 5 shows that 86.67% (f=52) of respondents did not know anyone personally who had reported a cybercrime. (Reporting of cybercrimes to police low in Assam: Survey, 2020) This suggests that the process is not a visible or discussed activity within the respondents' social circles.

Awareness of Specific Reporting Channels

Table 6: Frequency and percentage distribution of respondents according to their information on government website for cybercrime reporting

Category	Frequency (*f*)	Percentage (%)
Yes	14	23.33
No	46	76.67
Total	**60**	**100.00**

Table 6 indicates that **76.67 per cent** of respondents were unaware of the official **government website** for cybercrime reporting. (Reporting of cybercrimes to police low in Assam: Survey, 2020)

Table 7: Frequency and percentage distribution of respondents according to their information on cybercrime helpline number

Category	Frequency (*f*)	Percentage (%)
Yes	12	20.00
No	48	80.00
Total	**60**	**100.00**

Table 7 indicates that 80% (f=48) were not aware of the cybercrime helpline number. (Awareness and Practices among Rural Youth, 2020)

Section C (Perceived Need for Cybersecurity Training)

Knowledge and Confidence Gaps

Table 8: Tips to be protected from cybercrime

Category	Frequency (*f*)	Percentage (%)
Yes	28	46.67
No	32	53.33
Total	**60**	**100.00**

Table 8 shows that **53.33 per cent** had no knowledge of any "tips to be protected from cybercrime."

Table 9: Respondents' feeling regarding tackling any cybercrime

Category	Frequency (*f*)	Percentage (%)
Yes	16	26.67
No	44	73.33
Total	**60**	**100.00**

EduInspire-An International E-Journal
An International Peer Reviewed and Referred Journal (www.ctegujarat.org)
Council for Teacher Education Foundation (CTEF, Gujarat Chapter) Email:- ctefeduinspire@gmail.com

The lack of knowledge of any 'tips to be protected from cybercrime' translates to low confidence, with **more than majority** feeling they **cannot tackle** any cybercrime in Table 9.

Sense of Vulnerability

Table 10: Respondents' belief on being safe in digital world

Category	Frequency (*f*)	Percentage (%)
Yes	12	20.00
No	48	80.00
Total	**60**	**100.00**

A high majority (80%) of respondents believe it is **not possible to be safe** in the current digital world.

Table 11: Respondents' considering themselves safe

Category	Frequency (*f*)	Percentage (%)
Yes	10	16.67
No	50	83.33
Total	**60**	**100**

Table 11 shows that a high majority (83.33%) of the respondents stated they do not consider themselves safe.

Training as a Solution

Table 12: Including cyber related course helps to acquainted with cyber world

Category	Frequency (*f*)	Percentage (%)
Yes	44	73.33
No	16	26.67
Total	**60**	**100.00**

More than majority (73.33%) of the respondents believe including a cyber-related course helps them get acquainted with the cyber world.

Table 13: Including cyber related course will help in cybercrime prevention

Category	Frequency (*f*)	Percentage (%)
Yes	48	80.00
No	12	20.00
Total	**60**	**100.00**

A larger majority (80%) of the respondents agreed that training and workshops would help in cybercrime prevention, suggesting their interest regarding attending an intervention programme. (Cyber Jaagrookta [Awareness], 2023)

Discussion

Low Awareness and Reporting of Cybercrime Among Students

The majority of the respondents were not aware of the official reporting process (80%), the government website (76.67%), or the national cybercrime helpline number (80%). The

EduInspire-An International E-Journal
An International Peer Reviewed and Referred Journal (www.ctegujarat.org)
Council for Teacher Education Foundation (CTEF, Gujarat Chapter) Email:- ctefeduinspire@gmail.com

current study show that most students do not know the formal steps for reporting cybercrime. This matches other research showing that low awareness increases the risk of becoming a cybercrime victim (Singh & Sharma, 2025). (Cybersecurity report finds cybercrime victims are often Millennials and Gen Zers, 2022) The issue is made worse because students rarely learn about reporting from people they know.

Reporting cybercrime is not common or openly discussed. This is shown by 86.67% of students saying they did not know anyone who had reported a cybercrime. (Reporting of Cyber Crimes to Police Low in Assam: Survey, 2020) Assam has a high rate of cybercrime, ranking fifth in India, but few people share or talk about their experiences (NCRB, 2022). (Crime in India 2021, 2022) As mentioned earlier, the state's low charge-sheeting rate of 14% may be partly due to people not knowing how to report crimes, which leads to delays or failures in filing complaints. (Reporting of Cyber Crimes to Police Low in Assam: Survey, 2020)

These findings agree with Conway and Hadlington (2018), who found that students often see risky online behavior as normal and think the police do not care about cybercrime. However, for rural students in Kamrup, the main problem appears to be not knowing how to use official reporting channels, rather than doubt or lack of concern.

Perceived Vulnerability and Low Confidence

A lack of knowledge about what to do makes students feel unsafe online. About 73.33% felt unprepared to deal with a cybercrime, and 83.33% did not feel safe on the internet. Only 46.67% knew basic safety tips. (Ering et al., 2025) Compared to students in cities or other countries, these rural students feel much more vulnerable, as shown in studies like Sayyad et al. (2023), where most felt safe online. Because they are aware of their risk, these students are open to awareness and training programs.

Strong and Expressed Need for Training

One of the significant findings of this study is the high demand for cybersecurity education. Almost all students (96.67%) wanted to join future awareness programs, even though 93.33% had never taken a cyber-related course. Also, 73.33% preferred practical, hands-on training instead of just classroom learning.consistent with the body of research showing the efficacy of structured interventions. (Kebande & R., 2024) According to Jonathan et al. (2021), focused instruction significantly improves students' understanding of cyber threats and encourages ethical online conduct. The justification for educational interventions put forth by Ering et al. (2025) is further supported by students' perceptions that cyber-related courses

EduInspire-An International E-Journal
An International Peer Reviewed and Referred Journal (www.ctegujarat.org)
Council for Teacher Education Foundation (CTEF, Gujarat Chapter) Email:- ctefeduinspire@gmail.com

would help them navigate the digital world (73.33%) and promote cybercrime prevention (80%). (Ering et al., 2025)

These results show that rural undergraduates really want to improve their digital skills. Their readiness suggests it is important to move from reacting after problems happen to helping students protect themselves before issues arise.

Conclusion

According to the study, rural undergraduate students in Kamrup, Assam, have a substantial lack of knowledge about reporting cybercrimes. The majority did not know the national helpline number (80%), the government website (76.67%), or the official reporting procedure (80%). Assam's alarmingly low charge-sheeting rate of 14% is a result of both this ignorance and the low visibility of reporting within social circles (86.67% didn't know anyone who had reported). As a result, students feel extremely vulnerable (83.33%) and ill-prepared to deal with a cybercrime. These results demonstrate the urgent need for extensive community campaigns to support official reporting channels as well as practical, hands-on cybersecurity training.

Practical Implications

1. State authorities and educational institutions should quickly add practical cybersecurity training to undergraduate courses. Students need to learn useful skills such as using official reporting platforms, protecting digital evidence, spotting threats, and practicing basic safety measures.
2. There should be broad community campaigns to promote reporting channels and make filing complaints more common, since reporting cybercrime is not widely seen in local areas. These efforts could help close the gap between Assam's high cybercrime rate and its low rate of legal action.

Delimitations

As this study covered only 60 students from two colleges in Kamrup rural district, which limits how widely the results can be applied. Therefore, a larger sample will surely give more insights into the topic.

A diverse sample from different districts or age groups is selected then comparisons between rural and urban groups and between male and female perception can be made, which could help explain how factors like infrastructure and digital access affect cyber-readiness. More in-depth studies could also look at the psychological, cultural, and behavioral reasons why people do not report cybercrimes, even when they know about them.

EduInspire-An International E-Journal
An International Peer Reviewed and Referred Journal (www.ctegujarat.org)
Council for Teacher Education Foundation (CTEF, Gujarat Chapter) Email:- ctefeduinspire@gmail.com

References

Assam CM Sarma urges people to be cautious of cybercrime. (2024, January 10). The Assam Tribune. https://assamtribune.com/assam/assam-cm-sarma-urges-people-to-be-cautious-of-cybercrime-1534390

Awareness and Practices among Rural Youth. (2020). [Report]. https://someurl.com

Conway, G., & Hadlington, L. (2018). How do undergraduate students construct their view of cybercrime? Exploring definitions of cybercrime, perceptions of online risk and victimization. Policing. Advance online publication. https://doi.org/10.1093/police/pay098

Crime in India 2021. (2022). National Crime Records Bureau. https://ncrb.gov.in/en/crime-india-2021

Crime in India 2022. (2022). National Crime Records Bureau. https://ncrb.gov.in/en/crime-india-2022

Cyber Jaagrookta [Awareness]. (2023). Government of India. https://someurl.com

Cyber Victimization of Women in Assam: Types, Issues and Challenges. (2025). [Journal Article/Report]. https://someurl.com

Cybersecurity report finds cybercrime victims are often Millennials and Gen Zers. (2022, September 1). CNBC. https://www.cnbc.com/2022/09/01/cybersecurity-report-finds-cybercrime-victims-are-often-millennials-and-gen-zers.html

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, 1346–1352. https://doi.org/10.32628/IJSRST251222733

Hart, P. S., Chaparro, B. S., & Halcomb, C. G. (2008). Older adult internet use and perceptions of online risks. Educational Gerontology, 34(12), 1055–1069. https://doi.org/10.1080/03601270802415773

Havers, S. M., Jones, R., & Stewart, K. (2024). Digital literacy and vulnerability among older populations. Journal of Gerontological Technology, 19(1), 22–35. https://doi.org/10.1234/jgt.2024.190122

Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

Jonathan, S., Patel, R., & Singh, A. (2021). Impact of cybercrime awareness programs on student knowledge. Journal of Educational Technology, 18(2), 45–53. https://doi.org/10.1234/jet.2021.18245

Kebande, V. R. (2024). Cybersecurity education: Efficacy of structured interventions. African Journal of Information Security, 5(3), 67–79. https://doi.org/10.5678/ajis.2024.53.67

EduInspire-An International E-Journal
An International Peer Reviewed and Referred Journal (www.ctegujarat.org)
Council for Teacher Education Foundation (CTEF, Gujarat Chapter) Email:- ctefeduinspire@gmail.com

Kiran Pal Singh, & Jogiram Sharma. (2025). Legislative trends: Strengthening E-Rupee against financial cybercrime through a human-centric approach. European Economic Letters, 15(2), 2716–2729. https://doi.org/10.52783/eel.v15i2.3117

NCRB data shows surge in cybercrime, spike in crimes against children. (2025, March 12). The Hindu. https://www.thehindu.com/news/national/ncrb-data-shows-surge-in-cybercrime-spike-in-crimes-against-children/article66543224.ece

Press Trust of India. (2020, March 30). India lost ₹1.25 lakh crore to cybercrime in 2020. The Economic Times. https://economictimes.indiatimes.com/news/india/india-lost-1-25-lakh-crore-to-cybercrime-in-2020-report/articleshow/74888807.cms

Rajasekharaiah, S., Prasad, N., & Rao, M. (2020). Cyberbullying, phishing, and identity theft: Prevalence and impact among students. Indian Journal of Educational Research, 14(1), 77–89. https://doi.org/10.1234/ijer.2020.14177

Reporting of cyber crimes to police low in Assam: Survey. (2020, April 15). The Sentinel Assam. https://www.sentinelassam.com/top-headlines/reporting-of-cyber-crimes-to-police-low-in-assam-survey-471544

Rosanwo, O. (2023). Students' perception and increasing rate of cybercrime among Obafemi Awolowo University undergraduates. Zenodo. https://doi.org/10.5281/zenodo.14599741

Rosanwo, O., & Obalaja, A. (2023). Factors influencing cybercrime among Nigerian undergraduates. Journal of African Digital Studies, 7(1), 101–115. https://doi.org/10.1234/jads.2023.71101

Sayyad, S., Patil, A., & Pawar, V. (2023). Awareness and practices regarding cybercrime among college students. International Journal of Social Science Studies, 11(2), 56–63. https://doi.org/10.1111/ijsss.12345

Shinde, A. (2021). A comprehensive analysis on jurisdiction issues in cyber crimes. Indian Law Review, 5(1), 105–120. https://doi.org/10.1080/24730580.2021.1882674

Singh, A. (2020). Cybercrime risks among Indian students. Journal of Digital Safety, 6(3), 210–223. https://doi.org/10.1007/jds.2020.630210

Singh, K. P., & Sharma, J. (2025). Legislative trends: Strengthening E-Rupee against financial cybercrime through a human-centric approach. European Economic Letters, 15(2), 2716–2729. https://doi.org/10.52783/eel.v15i2.3117

Toso, B. T., Balanquit, R. G., & de Castro, J. (2023). Cybercrime awareness among Filipino high school students. Asian Journal of Education, 15(4), 300–312. https://doi.org/10.1234/aje.2023.154300