

Cybercrime Victimisation Among College Students in Coimbatore: Extent, Forms, And Impact

Poojitha.V¹, Kalanithi Raja K², Karkuvel Raja.M³, Siva Chidambaram B⁴

^{1,2,3} III BA Criminology, Department of Criminology and Forensic Science, Nehru Arts and Science College, Coimbatore, Tamil Nadu, India.

⁴ Assistant Professor, Department of Criminology and Forensic Science, Nehru Arts and Science College, Coimbatore, Tamil Nadu, India.

Abstract—In the contemporary digital era, the widespread use of the internet among college students has significantly increased their exposure to cyber threats. This study examines the extent and forms of cybercrime victimisation among college students in Coimbatore, with a focus on understanding awareness levels, behavioural patterns, and the impact of cyber incidents. The research identifies various forms of cybercrime, including phishing, identity theft, cyberbullying, hacking, and online financial fraud, which have become increasingly common due to rapid digitalisation. Using a structured questionnaire administered to 115 undergraduate students, the study analyses their experiences with cybercrime, frequency of victimisation, and preventive measures adopted. The findings reveal that a substantial number of students spend considerable time online, thereby increasing their vulnerability to cyber threats. Lack of awareness, weak cybersecurity practices, and excessive sharing of personal information are identified as key risk factors. The study also highlights the psychological, academic, and financial consequences of cybercrime victimisation. It emphasises the need for improved digital literacy, awareness programmes, and institutional interventions to ensure safer online practices. Ultimately, the research contributes to understanding the growing cyber risks among students and underscores the importance of proactive measures to mitigate cybercrime in educational environments.

Index Terms—Cybercrime; Victimisation; College Students; Cybersecurity Awareness.

I. INTRODUCTION TO CYBERCRIME AND STUDENT VULNERABILITY

The rapid advancement of digital technology has transformed the way individuals interact,

communicate, and access information. Among the most active users of digital platforms are college students, who rely heavily on the internet for academic activities, social networking, entertainment, and financial transactions. While this digital integration has enhanced convenience and connectivity, it has simultaneously increased the vulnerability of students to cybercrime.

Cybercrime refers to illegal activities conducted through computers, mobile devices, or internet-based platforms. These crimes include phishing, hacking, identity theft, cyberbullying, and financial fraud. Unlike traditional crimes, cybercrimes transcend geographical boundaries, making them more complex to detect and control. Students, due to their frequent online presence and relatively limited awareness of cybersecurity practices, often become easy targets for cybercriminals.

The increasing dependency on digital tools has created an environment where students unknowingly expose themselves to risks. Activities such as sharing personal information on social media, using public Wi-Fi networks, and engaging in online transactions without adequate security measures contribute to their vulnerability. Furthermore, the lack of awareness about cyber laws and reporting mechanisms exacerbates the problem.

Cybercrime victimisation not only affects students financially but also has psychological and academic implications. Victims may experience stress, anxiety, reduced academic performance, and loss of confidence. These consequences highlight the need to study cybercrime among college students in a

comprehensive manner. This study focuses on understanding the extent and forms of cybercrime victimisation among college students in Coimbatore. By analysing their experiences and awareness levels, the research aims to provide insights into the growing issue and suggest effective preventive measures. The introduction thus establishes the significance of addressing cybercrime as a major concern in the digital age.

II. CONCEPTUAL FRAMEWORK: DIGITAL CRIME, COMPUTER CRIME, AND CYBERCRIME

The terms digital crime, computer crime, and cybercrime are often used interchangeably, yet they possess distinct conceptual meanings. Understanding these differences is essential for analysing cybercrime victimisation effectively. Digital crime is a broad term encompassing all offences involving digital technology. It includes both traditional crimes facilitated by digital tools and new forms of crime emerging from technological advancements. Computer crime, on the other hand, specifically refers to offences where computers are either the primary target or the main instrument of the crime. Examples include hacking, data theft, and malware attacks. Cybercrime represents a wider category that primarily involves crimes committed through the internet. These offences occur in cyberspace and include activities such as phishing, identity theft, cyberbullying, and online fraud. Cybercrime is characterised by its transnational nature, anonymity, and rapid evolution.

The conceptual framework of cybercrime also involves understanding the relationship between offenders, victims, and technology. Cybercriminals exploit vulnerabilities in digital systems and human behaviour to carry out illegal activities. Victims, particularly students, may unknowingly facilitate these crimes through risky online behaviour. The theoretical understanding of cybercrime highlights the role of routine activities and opportunity structures. Students who frequently engage in online activities, such as social media usage and online shopping, are more likely to encounter cyber threats. This framework emphasises the need for awareness and preventive strategies to reduce victimisation.

III. EVOLUTION OF CYBERCRIME IN THE DIGITAL ERA

The evolution of cybercrime is closely linked to the development of computer technology and the internet. In the early stages, computers were large, expensive machines used primarily by government institutions and research organisations. During this period, computer-related crimes were minimal due to limited access. With the introduction of personal computers and the expansion of the internet, technology became more accessible to the general public. This accessibility led to the emergence of new forms of crime, including hacking, virus distribution, and data theft. The digital revolution further accelerated the growth of cybercrime, as individuals began using the internet for communication, commerce, and social interaction.

In recent years, the proliferation of smartphones, social media platforms, and digital payment systems has significantly increased cybercrime incidents. College students, being active users of these technologies, are particularly vulnerable. Cybercriminals exploit platforms such as social media and online banking to target unsuspecting users.

The evolution of cybercrime has also been marked by increasing sophistication. Modern cybercrimes involve advanced techniques such as phishing scams, ransomware attacks, and identity theft. These crimes are often organised and operate across international borders, making them difficult to investigate. The continuous evolution of technology necessitates the development of advanced cybersecurity measures. Understanding the historical progression of cybercrime helps in identifying trends and formulating effective prevention strategies.

IV. GLOBAL AND INDIAN SCENARIO OF CYBERCRIME

Cybercrime has emerged as a global issue affecting individuals, organisations, and governments. The widespread use of digital technology has resulted in significant financial losses and security challenges worldwide. Countries across the globe report increasing cases of cybercrime, highlighting its pervasive nature.

Globally, cybercrime impacts economic stability, business operations, and national security. Developed

nations have established specialised agencies to combat cyber threats, yet the problem persists due to the anonymity and borderless nature of cyberspace. In India, cybercrime has witnessed a steady increase over the years. The rapid growth of digital payments, e-commerce, and internet usage has contributed to this rise. Official data indicates a significant increase in cybercrime cases, reflecting the expanding digital landscape.

The legal framework in India addresses cybercrime through multiple laws, including the Information Technology Act and other related statutes. However, challenges such as lack of awareness, underreporting, and limited enforcement capabilities hinder effective control. The Indian scenario underscores the need for comprehensive cybersecurity policies and awareness programmes. As students form a major segment of internet users, addressing cybercrime among them is crucial for ensuring digital safety.

V. FORMS OF CYBERCRIME AFFECTING COLLEGE STUDENTS

College students encounter various forms of cybercrime due to their extensive online activities. One of the most common forms is phishing, where attackers use fake messages or emails to obtain sensitive information. Identity theft is another serious issue, involving the misuse of personal data for fraudulent purposes.

Cyberbullying and online harassment have become prevalent among students, affecting their mental health and social relationships. Social media scams, including fake profiles and deceptive offers, further contribute to victimisation. Malware attacks and hacking incidents pose significant risks to students' digital security. These attacks can result in data loss, financial fraud, and unauthorised access to personal accounts.

Online financial fraud, particularly in digital payment systems, has increased in recent years. Students who frequently use online banking and payment apps are vulnerable to scams such as fake refund messages and QR code fraud. Understanding these forms of cybercrime is essential for developing targeted preventive measures. Awareness and education play a crucial role in reducing the risk of victimisation.

VI. RESEARCH METHODOLOGY AND DATA ANALYSIS

The study adopts a quantitative research design to analyse cybercrime victimisation among college students in Coimbatore. Data was collected from 115 undergraduate students using a structured questionnaire administered through an online platform. The sampling technique employed was snowball sampling, allowing respondents to share the questionnaire with others. This method facilitated data collection from a diverse group of students across different academic levels. The questionnaire included questions related to internet usage, social media behaviour, awareness of cybercrime, and personal experiences with cyber threats. Data analysis was conducted using statistical tools such as percentages and tabular representation.

The findings reveal that a significant proportion of students spend more than three hours online daily, increasing their exposure to cyber risks. Social media usage is also high, with many students engaging in online activities for extended periods. The analysis highlights the correlation between online behaviour and cybercrime victimisation. Students with higher internet usage and lower awareness levels are more likely to experience cyber threats.

VII. CAUSES AND IMPACT OF CYBERCRIME VICTIMISATION

Several factors contribute to cybercrime victimisation among college students. High internet usage, lack of awareness, weak passwords, and excessive sharing of personal information are major risk factors. The use of public Wi-Fi networks further increases vulnerability. The impact of cybercrime is multifaceted, affecting students emotionally, academically, and financially. Victims often experience stress, anxiety, and loss of confidence. Cyberbullying and harassment can lead to severe psychological distress.

Academic performance is also affected, as victims may struggle to concentrate on studies. Financial losses resulting from online fraud can create additional stress for students. Social relationships may be disrupted due to cyber incidents, leading to isolation and reduced trust in digital platforms. These impacts highlight the seriousness of cybercrime and the need for effective intervention strategies.

VIII. PREVENTIVE MEASURES AND CYBERSECURITY PRACTICES

Preventing cybercrime requires a combination of awareness, education, and technological measures. Students must adopt safe online practices, such as using strong passwords and enabling two-factor authentication. Avoiding suspicious links and verifying the authenticity of websites are essential steps in preventing cyber threats. Limiting the sharing of personal information on social media can reduce the risk of identity theft.

Educational institutions play a crucial role in promoting cybersecurity awareness. Workshops, seminars, and training programmes can equip students with the knowledge needed to navigate the digital world safely. Government initiatives and legal frameworks must also be strengthened to address cybercrime effectively. Encouraging students to report cyber incidents without fear is vital for controlling cybercrime.

IX. CONCLUSION

The study of cybercrime victimisation among college students in Coimbatore reveals a growing concern in the digital age. The increasing reliance on the internet for academic, social, and financial activities has exposed students to various cyber threats. This research highlights the extent, forms, and impact of cybercrime, emphasising the need for immediate attention. The findings indicate that a significant number of students are vulnerable to cybercrime due to high internet usage and limited awareness. The prevalence of phishing, identity theft, cyberbullying, and online fraud underscores the complexity of the issue. These forms of cybercrime not only affect students financially but also have serious psychological and academic consequences.

One of the key observations is the lack of adequate cybersecurity practices among students. Weak passwords, excessive sharing of personal information, and the use of unsecured networks contribute to victimisation. Addressing these behavioural factors is essential for reducing cyber risks. The study also highlights the importance of awareness and education in preventing cybercrime. Educational institutions must take proactive measures to promote digital literacy and cybersecurity practices. Government

policies and legal frameworks should be strengthened to ensure effective enforcement and support for victims.

In conclusion, cybercrime is a multifaceted problem requiring a holistic approach. By fostering awareness, improving digital habits, and implementing robust security measures, it is possible to create a safer online environment for students. This study contributes to the understanding of cybercrime victimisation and provides a foundation for future research and policy development.

REFERENCES

- [1] Anderson, J., and L. Rainie. "The Future of Cybersecurity." Pew Research Center, 2019.
- [2] Holt, Thomas J., and Adam M. Bossler. *Cybercrime in Progress*. Routledge, 2016.
- [3] Kumar, S. "Cybercrime Trends in India." *Journal of Digital Studies*, 2020.
- [4] Patel, R. "Digital Literacy and Cyber Safety." *Education and Technology Review*, 2022.
- [5] Ramesh, K. "Cyberbullying among College Students." *Indian Journal of Social Research*, 2019.
- [6] Sharma, P., and R. Gupta. "Cybercrime Awareness among Students." *Journal of Cyber Studies*, 2021.
- [7] Verma, A., and S. Singh. "Online Banking Fraud among Youth." *Indian Journal of Criminology*, 2022.
- [8] Wall, David S. *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press, 2017.