European Economic Letters
ISSN 2323-5233
Vol 13, Issue 4 (2023)
http://eelet.org.uk

Analysis of Cybercrime against Indian Youth on Social Media

Sakshi Tiwari[1], Sushil Kumar Rai[2], Varsha Sisodia[3]

[1]Research Scholar, School of Media and Communication Design, IMS Unison University. India
[2]Associate Professor, School of Media and Communication Design, IMS Unison University. India
[3]Assistant Professor, Times School of Media, Bennett University India
Corresponding author Email ID: sakshi.tiwari@iuu.ac

Abstract:

This paper provides an in-depth analysis of cybercrimes targeted at Indian youth on social media platforms and explores their various forms, including online harassment, cyberbullying, identity theft, phishing, and financial fraud. The paper also investigates the underlying factors contributing to the vulnerability of Indian youth on social media and finally provides recommendations for enhancing awareness, education, and knowledge of new literacies among Indian youth to combat cybercrimes effectively.

Keywords: Cybercrime, Youth, Cyberbullying , Identity theft, Digital Literacy Skills

1. Introduction

In today's digital era, as technology continues to advance and societies become increasingly interconnected and reliant on the internet and social media, the vulnerability of young individuals to cybercrime has emerged as a significant concern. India in particular has been witnessing a steep rise in cybercrime cases, with a total of 52,430 cybercrime cases reported in different states of India in the year 2021 (NCRB Crime Report, 2021) and more than 27 million Indian adults facing cyber theft in the same year.

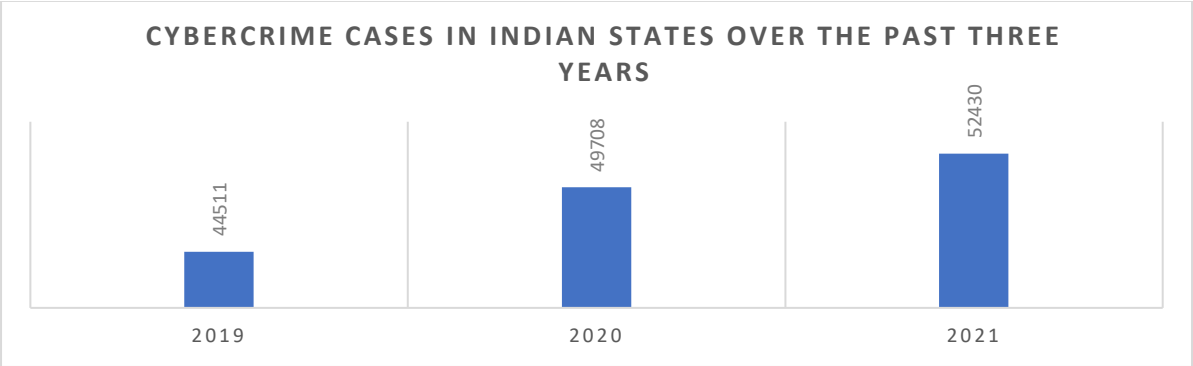

***Figure: 1*;**

Source: NCRB Crime Report, 2021 Vol.2, Page. No 785

Figure 1. Depicts the reported cases of cybercrime in Indian states over the past three years, revealing a noticeable upward trend in the numbers each year.

This is an alarming situation for the country, as India is home to one of the world's youngest populations, with its youth standing out as the most prominent users of social media.

Presently, India has the second-highest number of internet users in the world, with 759 million active internet users accessing the internet at least once a month. Further, it is estimated that the number of internet users in India will continue to grow and reach 900 million by 2025. Notably, the COVID-19 pandemic increased the number of internet users in India by 47 million (Kemp, 2021). The McKinsey Global Institute Digital India report also points out that India

is one of the world's largest and fastest-growing digital consumer marketplaces, with the public and private sectors driving the expansion (Kaka, N. et al., 2019) and the rapid development and acceptance of technology will continue to profoundly shape various aspects of users' lives.

In this digital age, internet has become the most preferred medium for our day-to-day communication, and has transformed the entire world into a global village where people are interacting freely without any boundary of time or space. Moreover, social media is a central focus of internet use and billions of people actively use social media platforms like Facebook, Instagram, Twitter, and others. In fact, these platforms have become indispensable for today's youth and have significantly accelerated the pace of information sharing and networking. A study conducted by Tripathi (2017) highlights that over ninety percent of young individuals rely on the internet on a daily basis, with approximately seventy percent maintaining active accounts on popular social media platforms like Facebook and Twitter. Further, it is reported in a research by Narula and Jinadal (2015) that the younger generation is drawn to social media due to its appeal and addictive nature however, their awareness regarding social media is still lacking, and whether or not they understand the potential consequences of sharing sensitive information on social media still remains uncertain.

Observing the growing need for a digitalized society and enabling digital empowerment in India, the Indian government has been putting all its efforts towards providing high-speed internet services to people residing in any part of the country. To achieve this, the government of India had already launched its "Digital India Flagship Programme" in the year 2015. However, several studies have asserted that the increased dependence of users on the internet worldwide is making them susceptible to cybercrime. (Iqbal & Beigh, 2017). In fact, Symantec, a security solutions provider ranked India second among the nations highly targeted for cybercrimes through social media in 2014. In fact, according to a report published in the Hindustan Times website, every sixth cybercrime in India is committed through social media. It is important to acknowledge the fact that even though the increased uptake of the internet and social media has provided ample prospects for young people to connect, communicate and interact with others (Boer et al.,2021), on the other side, cybercrimes using social media platforms are increasing, and users are progressively making themselves vulnerable to security dangers.

As per the Indian National Youth Policy (2014), youth are defined as those aged 15 to 29. The United Nations Population Fund **(UNPF)** projects that India will continue to have one of the youngest populations in the world until 2030. Therefore, this study aims to analyse the growing problem of cybercrime in India against youth on social media platforms. The study further delves into understanding the various forms of cybercrime committed against youth on social media, the factors contributing to growing cybercrime, and lastly, offers preventive measures that can be used to create a safer cyberspace for Indian youth. This research is based on qualitative methodology, drawing data from secondary sources such as reputable journals, websites, and newspapers, and the focus of this study is solely on cybercrime against the youth of India.

2. Review of Literature

Undoubtedly, the internet and digital communication technologies have created enormous opportunities for people of all ages, including youth, to contribute and accumulate information (Halder & Jaishankar, 2014). Children born since the late 1990s have grown up in a world reliant on technology, thus making it impossible for them to imagine their lives without being connected. Particularly social media has seamlessly integrated into the lives of the younger generation in such a way that the line between reality and fiction has completely blurred. For them, social media is not just a mere medium to pass off their boredom but has significantly impacted their exposure to new environments, knowledge, and education (Tripathi, 2017). They express all their emotions on the internet, including love and hatred, aggression, and violence (Tripathi, 2017), and for them. These sites (SNSs) have created a phenomenon that engages millions of Internet users worldwide, especially young people (Wilson et al., 2011) and according to the Social Media for Youth and Civic Engagement in India Report, India has more than 250 + million users using social networking sites and Facebook is considered to be the most famous social media platform throughout the world.
However, the advancement of technology has also significantly increased the fear of misuse of technology and several studies have opined that emerging internet technology and its widespread knowledge, will lead to security issues and increased cybercrimes (Ganesan & Mayilvahanan, 2017). In the wake of Digital India, studies have suggested that

cybercrimes will proliferate in India to a greater extent (Mali et al., 2018). A study (Soomro & Hussain, 2019) states that PC users spend more than 12 minutes engaging on social networking sites during an hour-long internet session. In contrast, mobile internet devotes more than 18 minutes to social networking sites. However, logging into social media and going through the contents frequently is not advised, as one is likely to fall victim to a syndrome known as "Fear of Missing Out (FOMO)," for which many people have already sought psychological advice. A study highlights that the suppression of cybercrimes can have a profound effect on individuals, leading to emotional distress and a decreased willingness to participate in cyberspace (Balabantaray et al., 2023). Cybercrime leaves a huge impact on youth by making them depressed to the point of self-harm. Girls who are affected by cybercrime have gone through severe mental agony (Malar, 2012).

Additionally, cyberbullying on social networking sites is an emerging societal challenge related to the undesirable use of technology (Chan et al., 2019) and has become very common and personalised. Cyberbullies carefully find and publicly humiliate their targets on social media, often by sending them hurtful messages (Shivashankar & Prakash, 2018). Cyber pornography is another commonly committed offence on social media, and mostly youngsters become victims of this through cyber stalking and malware (Umarhathab et al., 2009). Moreover, with the proliferation of social media, Identity theft is another severe problem evolving on social media platforms due to the sharing of excessive personal details on social networking sites (Das & Jyoti, 2011; Bhardwaj et al., 2017). Also, as social media platforms do not own copyrights for the content posted by users, anti-social behaviour on social media platforms is spiking (Sunith, 2020). Careless use of social media increases the risks of phishing, personification, and duplication of accounts (Verma et al., 2017).

In addition, lack of proper training, education, and awareness of cybercrime among Indians has also contributed to the growth in cybercriminal activities (Sreehari et al., 2018). The lack of strict laws for curbing cybercrimes in India has also led to increasing cases of cyberbullying (Tripathi, 2017). A study stated that the lack of fear in a society leads individuals to become more prone to engaging in inappropriate behaviour, and the internet has paved the way for such forms of open deviant behaviour to exist (Sen, 2013).

3. Discussion

On the basis of the analysis of the available literature and sources, this study investigated the meaning of cybercrime, the different forms of cybercrime prevailing against youth, the reasons behind the growing cybercrime against youth and the ways through which youth can protect themselves from cybercrime threats.

3.1 Meaning of Cybercrime

Cybercrime is an umbrella term for various offences and behaviours committed online. This crime is also known as computer crime, computer-related crime, virtual crime, or digital crime Though cybercrime involves the use of computers, sometimes computers are also the target. Cybercrime includes phishing, identity theft, cyberstalking, and cyberbullying (Kethineni, 2020). Due to rapid globalisation, the low cost of mobile phones and easy access to the internet, there has been an increase in cybercrimes like cyberbullying and cyber defamation. In most cases, it has been found that cybercrimes are processed knowingly and have a serious impact on society, encompassing threats to national defence, psychological disorder, or economic disruption (Saini, et al., 2012). Additionally, in India, young people are both perpetrators and victims of cybercrimes since they spend hours browsing. Furthermore, to date, many countries around the world are not equipped with the infrastructure to handle cybercrime (Arora, 2016), and often, it has been observed that cybercriminals carry out criminal activities in countries with weak or non-existent laws related to cybercrime.

Common Forms of Cybercrimes committed against Youth in India on Social Media

Cyberbullying: Using digital communication tools (such as the internet and mobile phones) to make another person angry, sad, or scared.

Cyber Pornography: An act where cyberspace is used to display, distribute, or present obscene material.

Identity theft: It occurs when someone steals the personal information of users to open new accounts, or engage in other criminal activities in their name.

Hacking: Compromising digital devices and networks by gaining unauthorised access to a computer system or account.

Cyber Defamation: It is a crime wherein a computer connected to the internet is used to defame a person or organization.

Cyberstalking: A crime in which one person is stalked, harassed, and abused using electronic means to express anger, retaliation, or rage.

Phishing: A type of fraud in which people are duped into supplying financial or personal information, such as a username and password, to access their accounts. Phishers use various social engineering and email spoofing technologies to deceive their victims.

Romance Scams: Romance scams occur when a criminal assumes a false online identity to gain a victim's affection and trust. The scammer then uses the illusion of a romantic or close relationship to manipulate and steal from the victim.

Sextortion: A crime where the perpetrator typically entices and induces the victim to share private and nude photographs or videos over the phone, which are then stored and saved by the perpetrator for future extortion.

3.2 Reasons Behind Cybercrime Against Youth

The susceptibility of young individuals to cybercrime often stems from their media usage patterns and inclination to share personal information on social media platforms. In their quest to increase their friend count on social networking sites, youngsters often befriend unfamiliar individuals and jeopardise their privacy and security. Inexperience with technology, participation in fraudulent activities such as responding to an unknown email, providing personal information to unknown users, and errors in decision-making have further led to increasing cybercriminal activities against youth (Monteith et al., 2021). The overuse of social networking sites and lack of awareness have also increased cybercrime by several folds. It has further been reported in several studies that social media users generally receive spam messages and calls, which they avoid to reporting leading to the reoccurrence of the same event. Several studies have argued that the absence of stringent laws to address cybercrime in India has resulted in a rise in cybercrime cases. The use of the internet on mobile devices has given a massive boost to cyberattacks (Thakkar & Mulani, 2014). Additionally, individuals hesitance to report incidents of cybercrime due to the social stigma associated with it is providing a boost to such crime (Tripathi, 2017).

Youth's vulnerability is significantly increasing due to a lack of awareness about IT activities and cybercrime, as well as the challenges in tracing cybercriminals. Further, the growing reliance on technology has made cyberattacks more disastrous (Jang-Jaccard & Nepal, 2014). and their limited knowledge about technology and insufficient understanding of cybercrime make them more susceptible to online threats. Additionally, the difficulty in identifying and apprehending cybercriminals adds to the risks faced by young individuals. Besides, the youth of today may be media-savvy but not essentially digitally literate. Several studies of contemporary times have highlighted that young people often lack information and media literacy skills which they require in order to be competent communicators in the current century. The new literacy skills that can help them successfully analyze, understand and evaluate information and make right decisions about its uses. The large user base and the level of trust on the part of social media users are also facilitating.

3.3 Ways to Protect the Youth

As technology continues to advance, it is crucial for people worldwide to be mindful of the information they share on social media and networking sites. Safeguarding personal data online is essential to minimize the risk of hacking and falling victim to criminal activities (Pavlik, 2017). To prevent cybercrime, especially among young individuals, it is important to refrain from sharing personal information on social networking sites. Additionally, using updated antivirus

software is necessary to protect against virus attacks. Employing two-factor authentication for all online services adds an extra layer of security against stolen passwords. Also, the users should avoid clicking on links, downloading files, or opening email attachments from unknown senders (Mokha, 2017).

With numerous websites offering a wide range of content, users must pay close attention to the source. This is particularly important considering past instances of misinformation, data breaches, and the dissemination of fake news. Further, to protect oneself, it is important for users to double-check the spelling of the website, the URL, and the HTTP address. Moreover, the use of public Wi-Fi in places like restaurants, railway stations, airports, and hotels should be avoided because public Wi-Fi networks are susceptible to man-in-the-middle attacks, where hackers can easily intercept and access personal information shared between a user and an application. To mitigate this risk, it is advisable to refrain from using public Wi-Fi altogether. (Deora & Chudasama, 2021).

Additionally, to promote online safety, it is important to organize training programs and workshops that focus on topics such as "How to Stay Safe on the Internet" and "Cyber Safety and Hygiene." Additionally, educating youth about Indian cyber laws can help protect them in case they become victims of cybercrime. Digital literacy and social media literacy should be incorporated into educational initiatives for young people.

Given the current landscape of cybercrime, the involvement of parents and teachers is crucial. They can play a valuable role in monitoring and preventing the negative effects of cybercrimes on young individuals, empowering them to navigate social media responsibly and avoid unsafe practices (Gupta & Nawal, 2019). By fostering competence and promoting regulated behavior, parents and teachers can significantly contribute to the online safety and well-being of young people.

4. Conclusion

As observed by the present trends, social media is a powerful platform for committing cybercrime in India. Numerous studies indicate that as the number of internet users in the country grows, cybercrimes are also expected to grow. The dream of Digital India can only become a reality when the government implements proper scrutiny and control measures against cyber threats. Moreover, as India has a significant percentage of a young population, it becomes essential to keep them aware of the dangers of cybercrime, such as cyberbullying, cyber pornography, identity theft, hacking, cyber defamation, cyber stalking, phishing, romance scams, and sextortion.

Additionally, several factors contribute to the vulnerability of the youth against cybercrime in India. Firstly, their habit of sharing excessive personal information online. Secondly, their inexperience with technology leaves them unaware of potential risks. The youth also lack the necessary skills to navigate the digital landscape safely, making them more vulnerable. Additionally, their involvement in fraudulent activities, driven by a lack of proper decision-making skills, further increases their susceptibility to cybercrime.

Therefore, to protect youth, it becomes crucial to promote safe online practices. It is important for individuals to remain vigilant when securing their personal data online. Implementing strong privacy settings, using unique and strong passwords, and being cautious while sharing personal information can significantly reduce the risk of being hacked or falling victim to criminal activities.

Educational programs on cyber safety, cyber etiquette, knowledge of digital and social media literacies, and awareness of Indian cyber laws should be imparted to empower and safeguard youth against criminal activities in cyberspace. As with the advent of social media, media literacy has become an increasingly important skill as it enables users to generate, analyze, rate, and create their own media and more importantly, understand and navigate Social media literacy is less talked about and needs to be articulated along with the digital literacy. New literacies will better help the youth of today filter impurity from messages and understand the real purpose of the message. It is an armour to protect viewers from purposeful messages trying to create a misperception or attitude towards the matter or subject. Though, people who use social media need similar skills to those required to manage print and broadcasting, what is new here is that social media also includes skills that are necessary to be able to create texts and images. Also, individuals should remain vigilant to secure their personal data online to reduce the risk of being hacked and falling victim to criminal activity. Lastly, by fostering a culture of digital hygiene and providing the necessary resources, a safer online environment can be created for the youth in India. In conclusion, with the increasing prominence of social media and the growth of cybercrime in India, it is crucial to prioritize the safety and awareness of the youth.

References

1. Arora, B. (2016). Cyber Crimes Schemes and Behaviors. *Perspectives in Science.*
2. *https://www.researchgate.net/publication/304907065_Cyber_Crimes_Sche mes_and_Behaviors*.
3. Balabantaray, S. R., Mishra, M., & Pani, U. (2023). A SOCIOLOGICAL STUDY OF CYBERCRIMES AGAINST WOMEN IN INDIA: DECIPHERING THE CAUSES AND EVALUATING THE IMPACT ON THE VICTIMS. *International Journal of Asia-Pacific Studies*, *19*(1).
4. Bhardwaj, A., Avasthi, V., & Goundar, S. (2017). Impact of social networking on Indian youth-A survey. *International Journal of Electronics and Information Engineering*, *7*(1), 41-51.
5. Boer, M., Stevens, G. W., Finkenauer, C., de Looze, M. E., & van den Eijnden, R. J. (2021). Social media use intensity, social media use problems, and mental health among adolescents: Investigating directionality and mediating processes. *Computers in Human Behavior*, *116*, 106645.
6. Chan, T. K., Cheung, C. M., & Wong, R. Y. (2019). Cyberbullying on social networking sites: The crime opportunity and affordance perspectives. *Journal of Management Information Systems*, *36*(2), 574-609.
7. Deora, R. S., & Chudasama, D. (2021). Brief study of cybercrime on an internet. *Journal of Communication Engineering & Systems*, *11*(1), 1-6.
8. Ganesan, M., & Mayilvahanan, P. (2017). Cyber Crime Analysis in Social Media Using Data Mining Technique. International journal of pure and applied mathematics, 116(22), 413-424.
9. Gupta, A., & Nawal, N. (2019). Impact of Cyber Crimes on Young Adults in India. *Journal of Advances and Scholarly Researches in Allied Education [JASRAE]*, *16*(16), 2043-2049(7. https://doi.org/10.29070/JASRAE
10. Halder, D., & Jaishankar, K. (2014). Use and Misuse of Internet by Semi-Urban and Rural Youth in India: A Baseline Survey Report (2013). *Available at SSRN 2378968*.
11. H. Saini, Y.S. Rao, T.C. Panda, Cybercrime and Their Impacts: A Review, International Journal of Engineering Research and Application, vol.2, Issue2, pp.202-209, 2012.
12. Iqbal, J., & Beigh, B. M. (2017). Cybercrime in India: trends and challenges. *International Journal of Innovations & Advancement in Computer Science*, *6*(12), 187-196.
13. Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973-993.
14. Kaka, N., Madgavkar, A., Kshirsagar, Gupta, R., A. Manyika, J. Bahl.K, Gupta, S. (2019). Digital India: Technology to transform a connected nation. Available at:
15. https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20india%20technology%20to%20transform%20a%20connected%20nation/mgi-digital-india-report-april-2019.pdf.
16. Kemp, S. (2021). Internet users in India. Available at: https://datareportal.com/reports/digital-2021-india.
17. Kethineni, S. (2020). Cybercrime in India: Laws, Regulations, and Enforcement Mechanisms. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 305-326.
18. Kshetri, N. (2016). Cybercrime and cybersecurity in India: causes, consequences and implications for the future. Crime, Law and Social Change, 66, 313-338.
19. Malar, M. N. (2012). Impact of cyber crimes on social networking pattern of girls. *international Journal of Internet of Things*, *1*(1), 9-15.
20. Mali, P., Sodhi, J. S., Singh, T., & Bansal, S. (2018). Analysing the Awareness of Cyber Crime and Designing a Relevant Framework with Respect to Cyber Warfare: An Empirical Study. International Journal of Mechanical Engineering and Technology, 9(2).
21. Mokha, A. K. (2017). A study on awareness of Cyber Crime and security. *Research Journal of Humanities and Social Sciences*, *8*(4), 459-464.
22. Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing cybercrime since the pandemic: Concerns for psychiatry. *Current psychiatry reports*, *23*(4), 1-9.
23. M. (2019). *Cyber Crime: It's Impact on Youth* (2nd ed., pp. 233-39). Indian Journal of Law and Human Behavior. https://doi.org/10.21088/ijlhb.2454.7107.5219.19
24. Narula, S., & Jindal, N. (2015). Social media, indian youth and cyber terrorism awareness: A comparative analysis. *J Mass Communicat Journalism*, *5*(246), 2.

25. Pavlik, K. (2017). Cybercrime, hacking, and legislation. *Journal of Cybersecurity Research (JCR)*, *2*(1), 13-16.
26. Sen, A. (2013). Linking cyber crime to the social media: A case study of victims in Kolkata. V J. Jaishankar (ur.), SASCV 2013 Proceedings, 378-382.
27. Shalaginov, A., Kotsiuba, I., & Iqbal, A. (2019, December). Cybercrime investigations in the era of smart applications: Way forward through big data. In *2019 IEEE International Conference on Big Data (Big Data)* (pp. 4309-4314). IEEE.
28. Shivashankar, B. S., & Prakash, G. (2018). A Critical Analysis of Cyber Bullying in India-with Special Reference to Bullying in College. *International Journal of Pure and Applied Mathematics*.
29. Soomro, T. R., & Hussain, M. (2019). Social Media-Related Cybercrimes and Techniques for Their Prevention. Appl. Comput. Syst., 24(1), 9-17.
30. Sreehari, A., Abinanth, K. J., Sujith, B., Unnikuttan, P. S., & Jayashree, M. (2018). A STUDY OF AWARENESS OF CYBER CRIME AMONG COLLEGE STUDENTS WITH SPECIAL REFERENCE TO KOCHI. International Journal of Pure and Applied Mathematics, 119(16), 1353-1360.
31. Sunith, C. K. (2020). Use and misuse of social media among Indian youth. *Journal of Humanities and Social Science*, *25*(1), 31-41.
32. Thakkar, S., & Mulani, M. Safeguarding Against Cyber Crimes Spreading Through Mobile Devices.
33. Tripathi, V. (2017). Youth violence and social media. Journal of Social Sciences, 52(1-3), 1-7.
34. Umarhathab, S., Rao, G. D. R., & Jaishankar, K. (2009). Cyber crimes in India: A study of emerging patterns of perpetration and victimization in Chennai City. *Pakistan Journal of Criminology*, *1*(1), 51-66.
35. Verma, R. K., Kumar, S., & Ilavarasan, P. V. (2017). Government portals, social media platforms and citizen engagement in India: Some insights. *Procedia computer science*, *122*, 842-849.
36. Wilson, K., Fornasier, S., & White, K. M. (2010). Psychological predictors of young adults' use of social networking sites. *Cyberpsychology, behavior, and social networking*, *13*(2), 173-177.