The nexus of social media and cybercrime: challenges and mitigation strategies

Dr. Anil Kumar Saini

Assistant Professor, Department of Sociology, Government P.G. College, Bazpur (U.S. Nagar), Uttarakhand, India

*Corresponding Author: Dr. Anil Kumar Saini

Received 9 March 2026; Accepted 13 Apr 2026; Published 6 May 2026

DOI: https://doi.org/10.64171/JSRD.5.S1.192-196

Abstract

India's rapid digital transformation, supported by affordable smartphones, expanding internet access, and growing digital literacy, has made social media a central part of daily life. With more than 700 million internet users, platforms such as Facebook, Instagram, X, YouTube, and LinkedIn have transformed communication, networking, and information sharing across the country. However, this digital expansion has also increased exposure to cyber threats, making cybersecurity a major concern in India. This study explores the growing link between social media use and cybercrime, focusing on common threats such as phishing, identity theft, malware attacks, cyberbullying, misinformation, account hacking, and online fraud. Cybercrime cases have risen significantly, especially after the COVID-19 pandemic increased digital dependency. Women and youth remain particularly vulnerable due to limited cybersecurity awareness and unsafe online practices. Although India has introduced legal and institutional measures, including the Information Technology Act, 2000, gaps in enforcement, awareness, and victim support continue to exist. The study concludes that ensuring safe digital growth requires stronger laws, improved digital literacy, better cybersecurity practices, institutional cooperation, and responsible digital citizenship to balance technological advancement with online safety.

Keywords: Social media, Cybercrime, Cybersecurity, Digital India, Online fraud, Cyberbullying, Misinformation, Identity theft, Digital literacy, Information technology act, India

Introduction

India has one of the largest online populations globally, with a growing internet user base of over 700 million. This growth is attributed to affordable smartphones, improved internet infrastructure, and government initiatives promoting digital literacy. The COVID-19 pandemic has further accelerated the digital transformation, with more people relying on the internet for work, education, communication, and entertainment. However, internet usage patterns vary across regions and socioeconomic segments. Internet facilities serve as the backbone of social media engagement, providing the essential infrastructure, connectivity, and accessibility required for users to connect, communicate, and interact on various social media platforms. Social media platforms have revolutionized communication, networking, and information dissemination, transforming the way individuals, businesses, and organizations interact in the digital age. However, they also expose users to unprecedented risks, undermining trust, privacy, and security. The pervasive threat of cybercrime engenders feelings of vulnerability, anxiety, and mistrust among users, eroding the sense of safety and autonomy in online interactions. Businesses and organizations face reputational damage, operational disruptions, and legal liabilities from social media-enabled cybercrime. The proliferation of misinformation and disinformation campaigns on social media poses existential threats to democratic processes, public discourse, and social cohesion. Policymakers, law enforcement agencies, and industry stakeholders face formidable challenges in combating social media-enabled cybercrime and safeguarding digital ecosystems from malicious exploitation. A multifaceted approach involving legal frameworks, regulatory measures, technological innovations, and community engagement initiatives is necessary to mitigate risks and foster a culture of digital citizenship and responsibility.

Social media

Social media is a global network of online platforms and applications that enable users to create, share, and interact with content, connecting with others worldwide. Its roots can be traced back to the early days of the internet, with the modern era taking shape in the late 1990s and early 2000s. Key milestones in the emergence of social media include Friendster, MySpace, Facebook, Twitter, YouTube, Instagram, Snapchat, and LinkedIn. Friendster was one of the earliest social networking sites to gain mainstream attention, allowing users to create profiles, connect with friends, and share updates and photos. MySpace was popular among teenagers and young adults, offering users the ability to customize their profiles with music, videos, and graphics. Facebook, founded by Mark Zuckerberg and his college roommates at Harvard University, quickly rose to prominence as the preeminent social media platform. Twitter introduced the concept of microblogging, allowing users to share short, 140-character messages.

YouTube revolutionized online video sharing, enabling users to upload, view, and share videos on a global scale. Instagram pioneered photo and video sharing through visually appealing images and short videos, gaining popularity among millennials and Gen Z users. Snapchat introduced ephemeral messaging, revolutionizing user engagement with multimedia content. LinkedIn emerged as the leading professional networking platform, connecting professionals, recruiters, and businesses for networking, job hunting, and professional development.

Cybercrime

Cybercrime is a criminal activity that exploits digital system vulnerabilities, compromises data integrity, and harms individuals, organizations, or societies. It emerged in the 1970s-1980s, with unauthorized access to computer systems, data theft, and malware dissemination. The 1990s saw a significant increase in cybercrime activities due to the growth of the internet and commercialization of online services. The early 2000s saw the emergence of sophisticated cyber threats, such as computer viruses, worms, and denial-of-service attacks. The mid-2000s saw the proliferation of social media platforms and online communities, providing cybercriminals with new avenues for exploitation. The late 2000s-present have seen cybercrime become increasingly sophisticated and organized, with ransomware, data breaches, cyber espionage, and state-sponsored hacking emerging as prominent threats.

Cybercrimes such as cyber defamation, pornography, stalking, fraudulent transactions, and hacking are prevalent on social media, with existing legislation like the Information Technology Act and Indian Penal Code addressing these issues [1]. According to the Intelligence Fusion & Strategic Operations, or Cyber Crime Unit, of the Delhi Police, these crime methods are "fake TRAI or FedEx courier company callers", "home job or Telegram fraud", "sextortion", "fake family member or friend in distress", and "OTP or link-based cheating". The latest National Crime Records Bureau (NCRB) data showed that Delhi registered 685 cybercrime cases in 2022 as against 345 in 2021 and 166 in 2020 [2]. Among the complaints received, ransomware, business e-mail compromise schemes, and the criminal use of cryptocurrency were among the top incidents reported. According to the FBI's Internet Crime Report 2021, India has been ranked among the top five countries by the number of total victims compared to the United States, accounting for 3,131 cybercrime in 2021 [3].

The COVID-19 pandemic has led to a rise in cybercrimes, including cyberbullying, defamation and fraud. In India, many people are unaware of these crimes and their consequences. The Indian government has taken measures to prevent cybercrimes, but there is still a need for compensation and justice for victims [4]. The Indian government has enacted laws to combat cybercrimes, including the IT Act, 2000, IPC, IEA, Banker's Books Evidence Act, 1891, and Reserve Bank of India Act, 1934. International cooperation is crucial to address cybercrimes [5].

Forms of cybercrime facilitated by social media

Social media platforms have provided fertile ground for cybercriminals to engage in various illicit activities, exploiting the inherent features of these platforms to target users, disseminate malicious content, and perpetrate cybercrime. Some of the prominent forms of cybercrime facilitated by social media include:

- **Phishing attacks:** Phishing attacks involve the use of deceptive emails, messages, or links to trick users into divulging sensitive information such as login credentials, financial details, or personal data. Cybercriminals often create fake social media profiles or pages impersonating legitimate entities to lure victims into clicking on malicious links or providing confidential information.
- **Identity theft:** Social media platforms contain a wealth of personal information about users, including their names, birthdays, locations, interests, and relationships. Cybercriminals exploit this information to steal identities, create fake accounts, or commit fraud. Identity theft on social media can lead to financial losses, reputational damage, and privacy violations for victims.
- **Malware distribution:** Social media platforms serve as distribution channels for malware, including viruses, worms, Trojans, and ransomware. Cybercriminals use social engineering tactics to trick users into downloading malicious attachments, clicking on infected links, or installing compromised applications. Malware distributed via social media can compromise the security of users' devices, steal sensitive information, or disrupt normal operations.
- **Social engineering attacks:** Social engineering attacks manipulate human psychology to deceive users and gain unauthorized access to their accounts or sensitive information. Cybercriminals employ tactics such as pretexting, baiting, and pretexting to exploit trust, curiosity, or fear. Social media platforms provide fertile ground for social engineering attacks, as users often share personal information and engage in interactions with unknown individuals or entities.

Over the past 91 days, 230 *Amdavadis* have been targeted by cybercriminals, resulting in nearly 10 victims every hour. The Cyber cell of Gujarat CID has observed new social engineering tactics and issued warnings through social media and helplines. Over 30,000 SIM cards have been deactivated after citizens reported them to the helpline [6].

Cyberbullying and online harassment

Social media platforms are commonly used for cyberbullying and online harassment, where individuals are targeted with abusive, threatening, or offensive behaviour. Cyberbullies leverage the anonymity and reach of social media to intimidate, humiliate, or ostracize victims, leading to psychological distress, social isolation, and even self-harm. Cyberbullying and online harassment can have profound consequences for victims' mental health and well-being.

Cyberbullying, affecting 50% of individuals, primarily at school, is a significant threat. Symptoms include anxiety, depression, and suicidal attempts. To combat it, individuals should seek guidance, counselling, report the issue, and trust others. Authorities should provide counselling rooms in

schools and limit personal information sharing at work. Blocking fake individuals is the only key step to tackling cyberbullying fully [7]. Online abuse in India affects over half of survey respondents, with women and others lacks support. Harassment leads to loss of trust on platforms, and over half want stricter community standards and reporting mechanisms. Thirty% are unaware of laws protecting them from online harassment, with Uttar Pradesh having the highest number of cybercrime cases in 2013 [8].

Spread of misinformation and disinformation

Social media platforms have become battlegrounds for the spread of misinformation and disinformation, where false or misleading content is disseminated to manipulate public opinion, sow discord, or advance political agendas. Cybercriminals and malicious actors exploit the virality and algorithmic amplification mechanisms of social media to propagate fake news, conspiracy theories, and propaganda, undermining trust in credible sources of information and exacerbating societal divisions.

Social media platforms are being used to spread rumours and incite violence, leading to increased regulatory compliance costs and concerns over inadequate cybersecurity and privacy protections in India [9]. The politicization and commodification of hate through social media hoaxes pose threats to national security and stability, requiring active roles from the state, industry, and society to protect cyberspace [10].

Account takeovers and credential theft

Social media accounts are frequently targeted for takeover by cybercriminals seeking to steal personal information, hijack user identities, or perpetrate scams. Account takeover attacks involve unauthorized access to users' accounts through password theft, credential stuffing, or social engineering techniques. Once compromised, cybercriminals may exploit hijacked accounts to spread spam, phishing links, or malicious content to the victim's contacts or followers.

Online scams and fraud

Social media platforms are rife with scams and fraudulent schemes aimed at deceiving users into parting with their money, personal information, or valuable assets. Common online scams include romance scams, investment fraud, lottery scams, and advance fee fraud, where victims are promised false rewards or financial returns in exchange for upfront payments or sensitive information.

Online frauds in India have caused a loss of Rs. 10,319 crore between April 2021 and December 2023. However, Rs. 1,127 crore, comprising 9-10% of the total defrauded money, could be saved through timely intervention via the citizen financial cyber fraud reporting and management system (CFCFRMS) and the '1930' financial cyber fraud helpline. The I4C is consulting banks and working on standard operating procedures for timely restoration [11].

In summary, social media platforms have become fertile breeding grounds for cybercrime, offering cybercriminals unprecedented opportunities to exploit user trust, manipulate digital ecosystems, and perpetrate illicit activities at scale. As the digital landscape continues to evolve, it is imperative for users, platform providers, and policymakers to remain vigilant, adopt robust security measures, and promote digital literacy to mitigate the risks posed by cybercrime in the social media era.

Mitigation strategies and best practices

Mitigating cybercrime requires a multi-faceted approach that involves collaboration between stakeholders, implementation of robust security measures, and fostering a culture of cyber resilience.

The internet is a powerful communication tool, but it's also vulnerable. To protect against cybercrimes, intrusion detection techniques should be designed and implemented, and preventive measures should be followed by individuals, institutions, and governments, as neither can solve the problem alone.[12] India, with 1.3 billion people, has the lowest data charges globally. However, the increasing scope of cyber threats necessitates the implementation of cyber security measures like firewalls, strong passwords, antivirus, and prevention of cyber-attacks. India's reactive approach to protecting cyber systems needs to be changed to a proactive one, requiring awareness, amendments, penal provisions, and cyber security policies to protect rights and privacy while upholding the rule of law [13].

Here are some key mitigation strategies and best practices:

User education and awareness

Promoting cyber awareness and digital literacy among users is paramount in preventing cybercrime. Educate users about common cyber threats, phishing scams, and social engineering tactics. Encourage them to practice good cyber hygiene, such as using strong, unique passwords, enabling two-factor authentication, and being cautious when clicking on links or downloading attachments.

There is a lack of cybersecurity awareness among the general population in both rural and urban areas, necessitating more information security awareness programs, which can be effectively delivered through social media [14].

Indian youth, despite being prolific users of social media, show limited awareness and concern about the threats of cyber terrorism, underlining the need for targeted awareness campaigns [15].

Security training and employee awareness

Organizations should provide comprehensive cybersecurity training to employees to raise awareness about potential threats and best practices for maintaining security. Training sessions can cover topics such as phishing awareness, password management, secure remote work practices, and incident response procedures.

Cybercrimes cause shock and embarrassment for victims, leading to a lifelong negative impact on their emotional and mental well-being. They act as a barrier to women's empowerment and require a coordinated effort from the legal system, regulatory agencies, and judiciary. Modern web-based applications should be used by these agencies, and governments should take legislative measures to protect human

rights, especially women's rights. Public awareness and education about women's rights and legal remedies can help eradicate cybercrimes. The global community must also work together to improve grievance redressal mechanisms and institutions [16].

Implement strong authentication mechanisms

Utilize strong authentication mechanisms, such as multi-factor authentication (MFA) or biometric authentication, to enhance the security of user accounts and prevent unauthorized access. MFA adds an extra layer of protection by requiring users to provide multiple forms of identification before gaining access to sensitive systems or data.

Regular software updates and patch management

Keep software, operating systems, and applications up to date with the latest security patches and updates. Regularly apply patches to address known vulnerabilities and reduce the risk of exploitation by cyber attackers. Implement automated patch management systems to streamline the process and ensure timely updates across the organization.

Cybercriminals exploit personal information shared on social media, leading to crimes like cyberbullying, harassment, and identity theft, highlighting the importance of securing personal information and the difficulty for social networking sites to regularly update privacy policies [17].

Network segmentation and access controls

Implement network segmentation to divide the network into separate segments or zones based on user roles, departments, or data sensitivity levels. Apply access controls and least privilege principles to restrict access to sensitive resources and minimize the impact of potential security breaches.

Data encryption and Data Loss Prevention (DLP)

Encrypt sensitive data both in transit and at rest to protect it from unauthorized access or interception. Implement data loss prevention (DLP) solutions to monitor and control the movement of sensitive data within the organization's network and prevent data leakage or exfiltration.

Endpoint protection and security solutions

Deploy robust endpoint protection solutions, such as antivirus software, firewalls, intrusion detection/prevention systems (IDS/IPS), and endpoint detection and response (EDR) tools, to safeguard endpoints from malware, ransomware, and other malicious threats. Implement centralized management and monitoring of endpoint security to detect and respond to security incidents in real time.

Incident response and cybersecurity incident management

Develop and regularly test an incident response plan to effectively respond to cyber incidents, minimize their impact, and restore normal operations quickly. Establish clear escalation procedures, roles, and responsibilities for incident response team members and conduct regular table top exercises to validate the effectiveness of the plan.

Collaboration and information sharing

Foster collaboration and information sharing among industry peers, government agencies, and cybersecurity organizations to exchange threat intelligence, best practices, and emerging trends in cybercrime. Participate in industry-specific information-sharing forums, threat intelligence platforms, and cybersecurity alliances to enhance situational awareness and collective defence against cyber threats.

Compliance and regulatory compliance

Ensure compliance with relevant cybersecurity regulations, industry standards, and data protection laws applicable to your organization. Stays informed about regulatory requirements and maintain documentation of security policies, procedures, and risk management practices to demonstrate compliance and mitigate legal and regulatory risks.

India's Information Technology Act, 2000, does not specifically address women's rights to life, education, health, food, and work. An expert group has been formed to study cybercrimes and develop a road map for effective tackling. The Cyber Crime against Women and Children (CCPWC) scheme has been approved. Cybercrimes targeting women include stalking, defamation, sex, obscene material, and trespassing into privacy domains. Women are more vulnerable to cybercrime due to increased virtual traffic [18].

The cybercrime against women is increasing at a very fast rate new offences like trolling and gender bullying are emerging as new field of cybercrime. But the IT Act 2000 does not include such crimes and the process of investigation is not appropriate. Act do not provide any remedy to cyber tolling and gender bullying which is one of the lacunae of the act. There is a need to create separate cell for the investigation. Special training must be given be the officers to deal with the cybercrimes against women. Judicial system of the country should try to tackle the problem of cybercrimes against women effectively [19].

By adopting a proactive and holistic approach to cybersecurity, organizations can enhance their resilience against cyber threats, protect sensitive data, and safeguard the integrity of digital assets in an increasingly interconnected and dynamic threat landscape. Cybercrime mitigation requires continuous vigilance, collaboration, and investment in people, processes, and technologies to stay ahead of evolving cyber threats and defend against emerging risks effectively. Changes in Indian regulations on social media, such as weakening encryption and increased monitoring, are responses to the misuse of platforms for activities like spreading fake news and vigilante violence [20].

Social media has become an integral part of life in India, with a vast number of users engaging on various platforms. This widespread use has brought about significant cybersecurity challenges, including the rise of cybercrimes and the spread of misinformation. In conclusion, the relationship between social media and cybersecurity in India is complex and multifaceted. While social media has brought about positive changes in connectivity and digital literacy, it has also opened the door to various cyber threats. The Indian population faces challenges

in cybersecurity awareness, and there is a pressing need for more robust legal frameworks and awareness campaigns to address the prevalence of cybercrimes. Additionally, the government's response to these challenges includes increased regulation and monitoring of social media activities to prevent the spread of misinformation and protect national security.

References

1. Thrupti NS, Kurbet K, Koujalagi A. Security threats in Indian cyberspace by social media and cyberhoaxes. Int J Trend Sci Res Dev, 2018. doi:10.31142/IJTSRD13040.
2. NDTV. Online job fraud, sextortion: how cyber criminals dupe people [Internet]. New Delhi: NDTV, 2023 Dec 7 [cited 2026 Feb]. Available from: https://www.ndtv.com/india-news/online-job-fraud-sextortion-how-cyber-criminals-dupe-people-4643210
3. Mumbai Bureau. India among top five victims of cybercrime: FBI report [Internet]. The Hindu BusinessLine, 2022 May 30 [cited 2026 Feb]. Available from: https://www.thehindubusinessline.com/info-tech/india-among-top-five-victims-of-cybercrime-fbi-report/article65475805.ece
4. Reddy S. Analytical study on cyber crimes in India [Internet]. SSRN, 2021 Jun 15 [cited 2026 Feb]. Available from: https://ssrn.com/abstract=4258578. doi:10.2139/ssrn.4258578.
5. Sarmah A, Sarmah R, Baruah AJ. A brief study on cyber crime and cyber laws of India. Int Res J Eng Technol, 2017, 4(6).
6. Times of India. Ahmedabad sees 230 cybercrime victims every day [Internet], 2023 Jul 16 [cited 2026 Feb]. Available from: https://timesofindia.indiatimes.com/city/ahmedabad/city-sees-230-cybercrime-victims-every-day/articleshowprint/101791732.cms
7. Taneja S, Pal R, Vishwakarma S, Kumar R. A case study on cyber bullying. Int Res J Adv Sci Hub, 2020, 2(7).
8. Aggarwal V, Shruti. Cybercrime victims: a comprehensive study. Int J Creat Res Thoughts. 2018;6(2):640-648.
9. Gulzar U. A critical appraisal of crime over social networking sites in the context of India. In: Cybercrime and social networking studies. Hershey (PA): IGI Global; 2020. p. 93-112. doi:10.4018/978-1-7998-1041-4.ch006.
10. Khan A, Islam K. Social media monitoring in India: a circumstantial analysis. Commun Technol eJournal. 2020. doi:10.2139/ssrn.3623334.
11. Times of India. India saw 129 cybercrimes per lakh population in 2023 [Internet], 2024 Jan 4 [cited 2026 Feb]. Available from: https://timesofindia.indiatimes.com/india/india-saw-129-cybercrimes-per-lakh-population-in-2023/articleshowprint/106524847.cms
12. Dar SA, Lone NA. Cybercrime in India. Sambodhi. 2020;43(4):VIII.
13. Singh A. A study on emerging issues of cyber attacks and security in India. Int J Adv Res Ideas Innov Educ. 2021;7(1):405-410.
14. Ganguly N, Kumaraguru P. The positive and negative effects of social media in India. Commun ACM. 2019;62:98-99. doi:10.1145/3345671.
15. Almadhoor L. Social media and cybercrimes. Turk Online J Qual Inq. 2021;12:2972-2981. doi:10.17762/TURCOMAT.V12I10.4947.
16. Sharma A, Singh A. Cyber crimes against women: a gloomy outlook of technological advancement. Int J Law Manag Humanit. 2018;1(3):1-12.
17. Gupta R. A solution paper on cyber security awareness campaign lacking in rural and urban area of India. Int J Res Appl Sci Eng Technol, 2021. doi:10.22214/ijraset.2021.37446.
18. Sharma D. Cyber crime in India: are women a soft target? [Internet]. Legal Service India; [cited 2026 Feb]. Available from: https://www.legalserviceindia.com/legal/article-639-cyber-crime-in-india-are-women-a-soft-target.html
19. Mishra S. Dimensions of cybercrime against women in India: an overview. Int J Res Anal Rev, 2018, 5(4).
20. Navaneetha B, Atchaya J. SWOT analysis of cyber security in social media. Int J Manag Soc Sci. 2018;8:183-185.