Victims of Cybercrimes: Are they protected enough?

competingcompetitions.com/policy-problems/victims-of-cybercrimes

By Kritika Vatsa

January 10, 2025

In the modern digital age, seemingly harmless online communications have transformed into sophisticated traps designed to exploit human vulnerabilities. What appears to be an unbelievably good investment opportunity, a life-changing lottery win, or a persuasive request from a stranger is often a very well-crafted scheme designed to deceive.

The digital revolution in India has undoubtedly been transformative, connecting millions of people to the global network and creating unprecedented opportunities for communication and commerce. Yet, this technological progress has opened new ways for cybercriminals, who continuously evolve their strategies to target individuals across urban and rural landscapes. The impact of cybercrime extends far beyond mere financial loss. These digital crimes strike at the fundamental human need for trust, leaving victims not just monetarily damaged but also socially disoriented. Each fraudulent interaction weakens the digital ecosystem's credibility, further creating a chain of anxiety and scepticism.

This article examines the demographics most vulnerable to cybercrimes, explores the specific crimes they face, and evaluates the recourse mechanisms available to them. It also addresses systemic gaps and offers improvement solutions. By focusing on the impacts on people who are vulnerable, this analysis highlights the human cost of cybercrime and the need for strong protective measures.

What are Cybercrimes?

To fully understand the impact of cybercrimes on victims, it is essential first to grasp the inherent complexity of defining these digital offences. Establishing a universally agreed-upon definition of cybercrime is difficult due to multiple interconnected factors. One such factor is the rapidly evolving technological landscapes. Technological advancements outpace legislative frameworks, enabling criminals to adapt their methods more quickly than legal systems can respond.

Moreover, the terminology itself remains fluid, as various terms like “cyberspace crime,” “computer crime,” and “electronic crime” are used interchangeably. This lack of a shared lexicon among professionals in the field makes it challenging to establish a single, universally accepted definition.

Adding to that, International variations in cybercrime legislation further complicate definitional efforts. Different jurisdictions interpret digital offences through unique legal and cultural lenses, leading to a fragmented global approach to understanding these crimes. Academic and professional fields contribute to this complexity by approaching cybercrime from diverse disciplinary perspectives, emphasising different aspects of digital criminal behaviour.

Despite these definitional challenges, what remains consistent is the profound potential for the harm these activities can cause to individuals, organisations, and society at large. From that perspective, the definition that emerges – one that is widely acceptable is this: cybercrimes refer to illegal activities that are carried out by using digital technologies, such as computers, networks, and connected devices.

Unlike traditional crimes, cybercrimes are inherently dependent on technology and often evolve rapidly due to advancements in digital tools and platforms. On a broader level, it can be divided into two main categories: cyber-dependent crimes, which can only be committed in the digital environment like hacking, ransomware and cyber-enabled crimes, where technology is used to support traditional criminal activities like fraud and cyberbullying.

What types of Cybercrimes are committed?

Cybercrime in India manifests itself in various forms, targeting a wide range of digital offences that affect individuals, businesses, and critical infrastructure. The nature of these crimes is diverse, each posing unique challenges to the victims.

Financial fraud is India's most prominent and devastating form of cybercrime, with the banking sector bearing the brunt of these attacks. Statistical evidence from the Reserve Bank of India shows an alarming picture of a continuous increase in cyber threats. Between **2020 and 2024 alone, over INR 3,207 crore was lost because of 5,82,000 cyber fraud cases.**

In particular, the financial year of 2024 has witnessed a dramatic increase in cyber fraud incidents across India. The number of reported cases has skyrocketed, representing an almost four times increase, **from 75,800 in the previous fiscal year to an alarming 292,800 cases in 2024.** These attacks manifest through various scams, including phishing, where attackers pose as legitimate institutions and trick individuals into revealing sensitive financial information, advance fee frauds promising large sums of money, and credit card or bank loan scams that exploit people's economic vulnerabilities.

Social media has also emerged as a critical space for cybercrime. In particular, cyberstalking has become increasingly common, involving persistent harassment through electronic communication. Additionally, cyberbullying has seen an estimated 50 per cent increase, with social media platforms providing anonymous spaces for perpetrators to intimidate and harm their victims. Online romance scams have also become widespread, with criminals building false relationships to exploit victims' trust and extract financial resources. According to a recent McAfee study published in 2024, 39 % of users reported that their online conversations with potential love interests were interactions with scammers. The report highlighted the digital vulnerability, with 77 % of Indians encountering fake profiles and AI-generated photos on dating platforms and social media.

Beyond financial and social media-based crimes, India faces a diverse digital threats. Cyber defamation has become a critical issue, with individuals using online platforms to spread false and damaging statements that can cause substantial emotional distress. Extortion schemes have also emerged, where cybercriminals use personal information to threaten individuals and demand ransom.

The complexity and variety of these cybercrimes highlight the sophisticated tactics used by digital criminals. Recognising the growing threat, India has begun implementing comprehensive measures to combat cybercrime. Major technological hubs like Bangalore, often called the “cybercrime capital of India,” have established dedicated cybercrime cells, with eight new police stations announced in 2018 to handle the increasing number of cases. Moreover, regulatory bodies are actively promoting cybersecurity awareness to better protect citizens. For example, the Reserve Bank of India has introduced an initiative to provide a comprehensive booklet on cyber hygiene practices to help customers understand and guard against digital threats.

Who are the Victims of Cybercrime?

Cybercrime has emerged as a significant threat. It affects diverse groups of people, but specific demographics in India are disproportionately targeted due to their unique vulnerabilities. Among them, young adults, children, women, e-commerce users, and banking customers are the most affected.

Young adults in the 20–29 age group frequently use digital platforms, making them easy targets for online scams. Their tech savvy often overshadows their lack of awareness about sophisticated cyber threats, exposing them to phishing, job fraud, and online romance scams. The attraction of quick financial gains or emotional appeals often blinds them to the risks, making them susceptible to exploitation.

Children and women represent another critically vulnerable segment, experiencing a 50 per cent increase in cybercrimes, mainly through digital platforms like chat rooms. Cybercriminals exploit the naivety of children and the societal vulnerabilities of women.

These groups face multiple forms of digital victimisation, including cyber-stalking, bullying, sexual solicitation, and even child pornography.

The reasons behind their increased vulnerability are multifaceted, including social norms, gender inequalities, and a reluctance to report incidents due to potential social stigma or lack of support systems. Predators exploit online spaces, using sophisticated methods to target these groups, leveraging their perceived vulnerability and the anonymity of digital platforms.

Another group heavily targeted is e-commerce users, as India's massive online shopping population presents an attractive opportunity for cybercriminals. With over 46 million users engaged in online shopping and social networking, the potential for exploitation is immense due to the vast amount of personal and financial data these platforms handle.

> The severity of these e-commerce threats can be inferred by global statistics that showed that the average data breach cost in 2022 was $4.35 million and required 277 days for complete breach identification and containment.

Banking customers are also equally at risk, with national and private banks experiencing substantial financial losses through cyber-attacks. This has created a climate of distrust, particularly among senior citizens who may become hesitant to utilise online banking services. The increase in phishing attacks, SIM swap scams, and unauthorised transactions has eroded trust in online banking services.

It becomes apparent that the victims of cybercrime are not confined to a single demographic but span across age groups, genders, and socioeconomic backgrounds. While each demographic faces unique vulnerabilities, from children encountering online predators to seniors falling prey to banking scams, the common thread is the severe impact these crimes have on their victims.

The impact of cybercrime on Victims

The financial impact of cyber crimes is particularly significant, with the banking sector being the most affected. In India alone, **2017-18 witnessed over 2,000 reported cases of cyber fraud related to online banking, resulting in an apparent loss of approximately Rs 109.6 crore.** Young adults aged 20-29 are especially susceptible, often falling prey to sophisticated online scams that trick them into revealing sensitive financial information or making fraudulent payments.

> The economic ramifications extend beyond individual losses, with global predictions suggesting annual cybercrime costs could reach $6 trillion, potentially weakening businesses through data breaches, ransomware attacks, and operational disruptions.

The emotional and psychological trauma of cybercrime goes far beyond financial losses. Victims, particularly women and children, endure excessive harassment through cyber stalking and bullying that results in deep psychological distress. The constant threats and invasion of privacy can trigger severe anxiety, depression, and overwhelming feelings of helplessness. Sexual exploitation, including child pornography and online sexual solicitation, leaves particularly devastating psychological scars that impact victims' long-term well-being and personal development. Moreover, the potential for reputational damage through online defamation or non-consensual sharing of intimate images creates an additional layer of trauma, often leading to social isolation and intense shame.

The broader societal implications of cybercrime are equally concerning. The pervasive threat of digital attacks erodes public trust in critical institutions, creating a climate of digital scepticism that can hinder technological progress and financial inclusion. Senior citizens, in particular, become increasingly hesitant to engage with online banking and digital services, potentially exacerbating existing technological disparities. This erosion of trust extends to government agencies and businesses, threatening society's fundamental social and economic fabric.

What recourse do Victims have?

Victims of cybercrime have several immediate channels for reporting and seeking assistance. The primary point of contact is often the local police station or specialised cybercrime cell, where trained personnel can handle these technology-related cases. These cells have the expertise and resources necessary to begin investigations promptly. Additionally, the Indian government has modernised the reporting process by establishing the Cyber Crime Reporting Portal **(www.cybercrime.gov.in)**, which allows victims to file complaints and submit evidence digitally. This online platform works with the Cyber Crime Coordination Centre (I4C) to efficiently handle cases.

Additional protections are in place for victims of financial cyber fraud, particularly in cases involving digital payments. Banks and e-wallet companies maintain dedicated helplines and complaint mechanisms for reporting unauthorised transactions or fraudulent activities. Swift reporting through these channels helps freeze suspicious transactions and prevent further financial loss.

Further, the Information Technology Act of 2000 provides the required legal support for fighting cybercrime in India by offering substantial protection across various digital offences. Computer-related offences, covered under Section 66 of the Act, carry significant penalties, including imprisonment of up to three years and fines of up to 5 lakh rupees. The Act particularly emphasises protecting personal information and privacy, with Section 66C addressing ***identity theft*** and Section 66E covering ***privacy violations****.* These provisions ensure that victims have legal recourse against those who misuse their personal information or violate their privacy online.

The Act also provides strong deterrents against online fraud and impersonation. Section 66D targets explicitly ***those who cheat by impersonating others*** using computer resources, while Section 66B addresses the ***dishonest reception of computer resources or communication devices***. Both offences can result in imprisonment of up to three years and substantial fines, providing victims with clear legal pathways for seeking justice.

Content-related offences are addressed with particular severity under the IT Act. Section 67, which deals with the ***publication of obscene material in electronic form**,* provides for escalating penalties with repeat offences. First-time convictions can result in three years of imprisonment and fines up to 5 lakh rupees, while subsequent convictions carry enhanced penalties of up to five years imprisonment and fines up to 10 lakh rupees. Section 67A, addressing ***sexually explicit material***, carries even more substantial penalties, with first convictions potentially resulting in five years imprisonment and fines up to 10 lakh rupees.

Beyond the legal framework, victims can also seek specialised support from organisations like **CERT-In (Indian Computer Emergency Response Team)**. This national agency provides expert guidance on handling cybersecurity incidents and can be particularly valuable for victims navigating complex technical aspects of their cases. Many states have also established dedicated cybercrime helpline numbers and specialised cyber cells, providing victims with local support and resources.

The key to effectively utilising these resources is prompt action and proper documentation. Victims should immediately document all details of the incident, preserve evidence such as screenshots or emails, and maintain records of all communications with authorities. Regular follow-up with investigating agencies and, when necessary, seeking legal counsel can significantly improve the chances of a successful resolution.

Verdict: Are Victims protected enough?

The current response infrastructure of cybercrime that we have in India faces significant challenges that create hindrances in effective resolution. Despite the establishment of specialised cybercrime cells across states several critical barriers persist. A critical issue is the lack of public awareness, particularly acute in rural areas, where many victims remain unaware of crucial reporting mechanisms such as the National Cyber Crime Reporting Portal and cybercrime cells. Even among those aware of these reporting mechanisms, many hesitate to come forward due to social stigma or lack of confidence in the system.

Resource constraints further exacerbate these challenges. Many cybercrime cells operate with insufficient manpower, inadequate training, and limited technological tools. The cross-border nature of cybercrimes adds another layer of complexity, making investigation and prosecution particularly challenging when perpetrators operate across international boundaries. For victims of financial fraud, the process of fund recovery is too long and uncertain, often lost in bureaucratic procedures that provide little immediate relief. Perhaps most concerning is the lack of **comprehensive victim support services**, especially for vulnerable groups like women and children who face additional social barriers.

The creation of the Digital Personal Data Protection (DPDP) Act last year is a significant step in the direction of assisting the victims. This legislation provides a strong framework for protecting personal data and enforcing accountability for data breaches. However, since it has yet to be implemented, its assistance to the victims of cyber crimes is still out of reach.

Also Read: ***India's Privacy Law: A Critical Analysis of Loopholes and Concerns***

Overall, a more victim-centric approach is crucial for meaningful reform. This includes developing comprehensive support services offering psychological counselling, legal assistance, and financial guidance. Special attention must be paid to vulnerable groups through dedicated helplines and support centres. By combining stronger legal frameworks with enhanced support systems, India can move towards a more effective response to the evolving challenges of cybercrime.

Conclusion:

In conclusion, India’s cybercrime landscape presents a complex challenge, demanding urgent and comprehensive action. The victims, spanning all ages and demographics, endure not only financial loss but also significant emotional and psychological trauma. While legal frameworks and reporting mechanisms exist, their efficacy is hampered by a lack of awareness, resource constraints, and the evolving nature of cyber threats.

To truly combat cybercrime, a multi-pronged approach is essential. Enhanced public awareness, bolstered law enforcement capabilities, and strengthened international cooperation are crucial steps. A victim-centric model that prioritises support, swift investigation, and accessible justice must be the cornerstone of India’s response. By empowering individuals and communities, focussing on the needs of victims, fostering trust in digital systems, and relentlessly pursuing cyber criminals, India can pave the way towards a secure and resilient digital future for all its citizens.

Kritika Vatsa [Author]