BEHIND THE SCREEN: THE HUMAN COST OF CYBERCRIME IN INDIA

Sukrati Sharma, B.A.LL.B. (Hons.), Asian Law College, Noida.

Yashasvi Panwar, B.A.LL.B. (Hons.), Asian Law College, Noida.

ABSTRACT

India has experienced a huge digital revolution, with increased technological proficiency and connection resulting in more digital accessibility and inclusivity for its population. While these improvements are cause for national pride, especially given India's achievements in the IT sector, the significant growth in cybercrime is a serious and growing worry. Any illegal behaviour that uses a computer as a tool, target, or means to perpetrate more violations is considered cybercrime, commonly referred to as "Internet crimes." Phishing, cyberstalking, ransomware, and financial fraud are all on the rise, resulting in not just economic losses but also serious psychological and emotional suffering for victims, particularly women.

With more than 700 million Indians using digital platforms, people and organizations are more vulnerable than ever. Women are disproportionately targeted in cyberstalking and harassment cases, with occurrences of revenge pornography and online abuse rising year after year. Scams are becoming more sophisticated, and they are affecting professionals, financial literacy, and teenagers equally. Despite existing legislation such as the IT Act of 2000, India lacks a strong personal data protection law, and many cybercrime cases go unsolved due to antiquated technology, insufficient coordination, and jurisdictional gaps.

This paper investigates the scope of cybercrimes affecting India, analyzes criminal motivations, emphasizes the disproportionate impact on women and vulnerable groups, and explores major legal cases. To protect India's digital society from the growing human and financial consequences of cybercrime, it also analyzes the reasons that contribute to its growth, reviews the legal and infrastructure solutions that are currently in place, and suggests multi-layered preventive and mitigation strategies. In support of this analysis, an original survey was undertaken to collect empirical data on the type, frequency, and effects of cybercrime, which increased the depth and usefulness of the research findings.

Keywords: Cybercrime, Fraud, Survey Research, Women, IT Act 2000, Digital Inclusion

I. Introduction

India has seen a massive digital revolution, with increased technology sophistication and connection leading to improved digital accessibility and inclusivity for its citizens. From villages to block levels, these digital shifts are particularly noticeable in rural areas. Even if these advancements are a source of pride for the country, especially given the outstanding accomplishments in the IT industry, the sharp increase in cybercrimes is a serious and expanding worry. Cybercrimes have increased nationwide as more people use computers and the Internet in their homes and places of employment.

Cybercrime in India encompasses a range of offenses involving the unauthorized, dishonest, or fraudulent use of computers, networks, or digital devices. Governed primarily by the Information Technology Act, 2000 (IT Act), this legislation provides a comprehensive legal framework to address cyber offenses. The Act broadly defines cybercrime as any unlawful act or omission punishable under the IT Act or any other applicable law, where computers or digital devices are used as instruments or targets of crime. Section 43 of the Act[1] mandates compensation for damages caused by unauthorized access, while Section 66[2] criminalizes such acts when done with dishonest intent, prescribing penalties including imprisonment of up to three years, fines up to ₹5 lakh, or both. The Act covers various offenses including hacking, identity theft, cyber terrorism, publication of obscene material, data theft, and privacy violations, with punishments calibrated to the severity of the crime. Serious offenses like cyber terrorism may attract life imprisonment, underscoring the Act's robust approach to maintaining cybersecurity and legal accountability in India's evolving digital landscape.[3]

India, despite passing cybercrime and e-commerce laws in 2000, still lacks a comprehensive personal data protection law. The IT Act 2000 provides legal recognition to electronic records and digital signatures, supporting e-commerce and e-governance[4]. However, vague provisions grant law enforcement broad access to user data, raising significant privacy concerns. With over 700 million internet users and a surge in digital transactions, India faces growing

[1] The Information Technology Act 2000, s 43
[2] The Information Technology Act 2000, s 66
[3] LSI, Legal Service in India (LSI), "Cybercrime in India" <https://www.legalservicesindia.com/law/article/2266/6/CYBER-CRIME-IN-INDIA?id=2266&u=6> accessed on 12 June 2025
[4] Next IAS, Next IAS Contributors, "Cybercrime in India" < https://www.nextias.com/blog/cybercrime-in-india/#What_is_the_IT_Act_2000_for_Cybercrime> accessed on 12 June 2025

cybersecurity threats, including data breaches and financial losses.[5]

From the perspective of the victim, the extent and gravity of cybercrime and cyberfraud in India have increased. The swift digitization of personal communication, payment networks, and banking has made regular people more vulnerable to increasingly complex cyberthreats. Victims frequently experience psychological and emotional suffering in addition to monetary loss. According to a 2024 article in *The Hindu Business Line*[6], "victims of financial fraud, identity theft, phishing, and scams frequently feel betrayed, powerless, and anxious. The difficulties of finding the offenders and the frequently drawn-out, arduous procedure of getting justice or restitution exacerbate this feeling of violation."

A. Research Objectives

This research paper aims to analyze the growing landscape of cybercrime in India, focusing on the various types of cyber offenses affecting individuals and organizations, especially crimes targeting women and vulnerable groups. It critically examines the effectiveness of existing legal frameworks, primarily the Information Technology Act, 2000, in addressing cyber threats. Finally, the paper proposes comprehensive preventive strategies and legal reforms to strengthen cybersecurity infrastructure, improve enforcement, and foster digital safety and resilience across India.

B. Research Methodology

This research paper incorporated a mixed-methods approach, combining qualitative legal analysis with quantitative survey data. To assess the impact and prevalence of cybercrimes in India, a structured survey was disseminated through Google Forms across various digital platforms including WhatsApp, SMS, Instagram, and email. The survey collected responses from 111 participants across different age groups, educational backgrounds, and professions, with the majority falling in the 18–35 age bracket representing India's most digitally active demographic. Questions focused on the types of cybercrimes experienced, mental health repercussions, awareness of the cybercrime reporting portal, and common points of contact for

[5] Raghib Raghib, Dr Syed Mohammad Raghib, "Cyber Security and Data Protection in India: A National Concern" < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4953130> accessed on 13 June 2025
[6] Sindhu Hariharan, "NSSO Survey" < https://www.thehindubusinessline.com/info-tech/only-18-of-indians-have-ability-to-report-a-cybercrime-via-official-channels-nsso-survey/article69683219.ece> accessed on 15 June 2025

fraud (e.g., social media, phone calls, messages). The results were analyzed to identify patterns and trends in victimization and public awareness, thereby helping to frame the broader discussion around digital vulnerabilities and legal responses.

C. Bibliography

The research paper references key legal documents including the *Information Technology Act, 2000* and relevant provisions of the *Indian Penal Code (IPC)*. Important judicial cases such as *Shreya Singhal v. Union of India*, *Mahesh Kumar Poddar v. State of Jharkhand*, and *State of Tamil Nadu v. Suhas Katti* were used to illustrate the legal response to cybercrimes. Statistical data and reports were sourced from *The Hindu Business Line* (2024) and the *National Commission for Women*. Real-life cybercrime incidents like the *Cosmos Bank cyberattack (2018)* and the *Vijay Mallya-Kingfisher scam* were included to contextualize digital vulnerabilities. Primary data was collected through a 2025 online survey conducted via Google Forms.

II. Background

An enormous network of interconnected gadgets has been created because of the integration of technology into daily life during the 1990s[7], revolutionizing the way both individuals and organization's function[8]. Cybercrime, or illegal activity carried out through networks or computer systems, has increased as a result of this digital revolution[9]. Cybercrime has spread throughout the world and is posing serious problems for security systems. Digital technological breakthroughs have increased productivity, but they have also created new opportunities for hackers to take advantage of, underscoring the essential need for sophisticated cybersecurity safeguards.

The past ten years have seen an increase in cyberattacks and the hazards they pose, underscoring the vital significance of protecting information systems and sensitive data. Cybercrimes pose serious threats to both persons and organizations, ranging from identity theft and online harassment to financial fraud and phishing scams. Governments, law enforcement

[7] Irfan Attari Kashmiri, "India's Tech Revolution" < https://brighterkashmir.com/indias-tech-revolution > accessed on 15 June 2025
[8] Sudhanshu Sekhar Tripathy, "A comprehensive survey of cybercrimes in India over the last decade" < https://mail.ijsra.net/sites/default/files/IJSRA-2024-1919.pdf> accessed on 16 June 2025
[9] Redteam Cybersecurity Labs, "A Brief History of Cybercrime" < https://theredteamlabs.com/a-brief-history-of-cybercrime/> accessed on 16 June 2025

organizations, and cybersecurity teams have responded by stepping up their efforts to counter these attacks[10]. Cybercrime events have significantly increased in India in recent years, with ransomware, data breaches, and social engineering attempts accounting for a large portion of these cases.

Individuals and companies are becoming more susceptible to cyber risks as a result of the rapid adoption of digital payment systems, the growth of e-commerce, and the increasing penetration of online services. Due to the sensitive nature of the data, they manage, the banking, healthcare, and government sectors are among the main industries impacted. Public awareness, cybersecurity education, and strong legislative frameworks are becoming more and more important in the fight against these threats.

III. Cyber Crimes

Traditional crimes like fraud and forgery have given way to a variety of new crimes known as "cyber-crimes," which have certain unusual characteristics. These crimes are the result of the misuse of computers and the associated electronic media. "Any criminal activity that uses a computer either as an instrument, target, or a means for perpetuating further crimes or offenses or contraventions under any law" is the definition of cybercrime, commonly referred to as "Internet crimes." Cybercrimes are crimes committed with the use of computers or relating to computers, especially through the Internet, according to the Legal Dictionary[11].

These offenses encompass not only computer use but also the Internet, cyberspace, and the World Wide Web's tools and methods. "Unlawful acts wherein the equipment transforming the information, be it a computer or a mobile device, is either a tool or a target or both" is a straightforward definition of these offenses[12]. Joseph-Marie Jacquard[13] created a loom that could repeat a sequence of stages in the weaving of unique fabrics, but his own workers sabotaged it because they thought it would jeopardize their way of life and conventional job.

[10] Cyber Mithra, "History of Cybercrime" < https://cybermithra.in/2024/05/12/history-of-cybercrimes-part-3/> accessed on 16 June 2025
[11] Legal Dictionary, "Cybercrime" < https://legaldictionary.net/cybercrime/> accessed on 20 June 2025
[12] LawBhoomi, "Crime: Concept, Stages and Elements" < https://lawbhoomi.com/crime-concept-stages-and-elements/> accessed on 20 June 2025
[13] Arshi Khan, "The First Recorded Cybercrime Took Place in the Year 1820" < https://www.scribd.com/doc/71120466/The-First-Recorded-Cyber-Crime-Took-Place-in-the-Year-1820> accessed on 21 June 2025

This event, which occurred in 1820, is regarded as the first cybercrime in history[14].

In the recent case of *Mahesh Kumar Poddar v The State of Jharkhand*[15], which was determined on May 13, 2022, the petitioner contested his conviction for offenses involving forgery, cheating, and cybercrime. It was claimed that Poddar and others obtained many SIM and ATM cards to conduct illicit financial transactions and opened numerous bank accounts using falsified documentation. His bank account had ₹21,85,037 during the investigation, for which he was unable to offer a good reason in accordance with Section 313 CrPC. Despite the fact that some witnesses did not explicitly name him, the investigating officer and the bank manager provided crucial proof that he was involved. Based on the financial trail and accompanying documentation, the trial court found him guilty. The High Court noted the gravity of the offense and the evidence against Poddar when he requested that his sentence be suspended and that he be released on bail. As a result, bail was refused, and the only way to renew the bail plea is to serve half of the sentence.

IV. Types of Crimes

- **Email Frauds**

Email accounts can be compromised through several methods, each posing significant security risks. Sharing two-factor authentication codes with scammers gives attackers direct access to accounts, bypassing traditional password protections. These techniques may result in the installation of malware on the victim's device and the loss of login credentials. Scammers can also use malware to read saved passwords or take screenshots[16].

- **Social Media Frauds**

Online social networks like Facebook, Instagram, Twitter, and LinkedIn are seeing an increase in the number of users creating profiles. Fake profiles, on the other hand, are very common and frequently spam real users with offensive or unlawful content. Online threats, stalking,

[14] Chaintech,"1820 Textile Industry: Weaving the Threads of the First Cybercrime" < https://www.chaintech.network/blog/1820-textile-industry-weaving-the-threads-of-the-first-cybercrime/ > accessed on 24 June 2025

[15] *Mahesh Kumar Poddar v State of Jharkhand,* Criminal Appeal No. [433 of 2021], Jharkhand High Court (13 May 2022)

[16] Cybercrime Unit Delhi Police, "Email Frauds" < https://cyber.delhipolice.gov.in/emailfraud.html> accessed on 25 June 2025

cyberbullying, hacking, fraud, purchasing illicit goods, vacation robberies, making phony profiles, and forming phony online friendships are among the common crimes performed on social media[17]. Victims frequently don't know whether to notify the police, and these crimes frequently go unpunished or are not taken seriously. Understanding these dangers and taking precautions to keep oneself and others safe on social media is essential.

In the case of *Emeka Fabian v State by Cyber Crime Police*[18], the petitioners, who are both Nigerian nationals, were charged by the Cyber Crime Police on February 18, 2016, with online fraud and cheating by fabricating documents and abusing social media and the internet to trick and defraud innocent people out of their money. They had overstayed their visas, broken multiple provisions of the Foreigners Act, the Passports Act, and associated regulations, and neglected to register their residences with local authorities, according to the probe. Although the petitioners were foreign nationals, the court stated that the seriousness of the charges, which included forging documents, using multiple SIM cards, and committing cybercrimes, as well as the possibility of additional illegal stays, justified the denial of bail, even though the offenses were not punishable by death or life in prison. Because of this, the Karnataka High Court denied the bail request and ordered that the trial be held quickly.

- **Online Transaction Frauds**

Card details like the card number, validity, and a three-digit private One-Time-Password (OTP) are all unlawfully accessed in fraudulent online purchases[19]. By pretending that the OTP is required for account verification, scammers may trick account holders into disclosing it. Avoiding providing account numbers with trustworthy businesses, keeping an eye on credit reports and bank and credit card statements, saving card information online, and avoiding usage of a credit card on public computers are all examples of preventive measures.

- **Net Banking/ATM Frauds**

SIM Swap is a fraud scheme where scammers use a customer's phone number to obtain a new

[17] Cybercrime Unit Delhi Police, "Social Media Crimes" <https://cyber.delhipolice.gov.in/socialmediacrimes.html> accessed on 25 June 2025
[18] *Emeka Fabian V. State by Cyber Crime Police,* Criminal Petition No. [570/2016], Karnataka High Court (18 February 2016)
[19] Cybercrime Unit Delhi Police, "Online Transaction Frauds" <https://cyber.delhipolice.gov.in/onlinetransactions.html> accessed on 25 June 2025

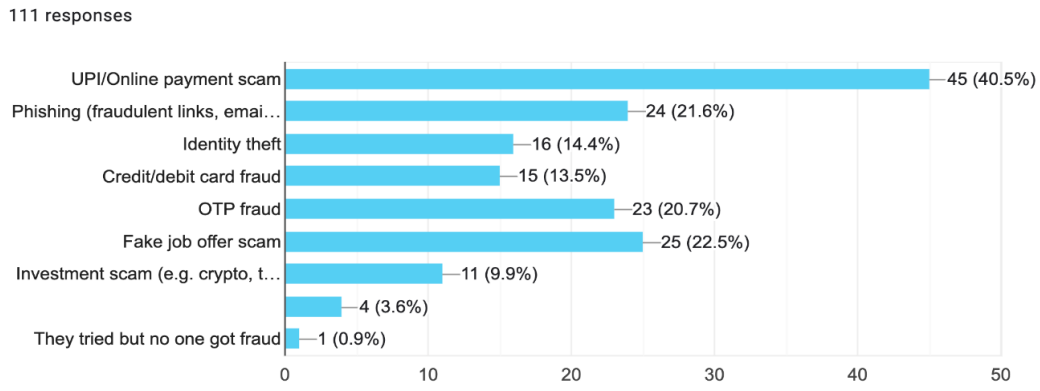
SIM card, enabling them to receive financial transactions and a One Time Password (OTP)[20]. They use phishing, vishing, or smishing to obtain consumer information, block the SIM, and enter the operator's location. Phishing involves stealing personal data via SMS, phone calls, and emails.

- **Fake Call Frauds**

Fake call scams, sometimes referred to as voice phishing or vishing, occur when people get phone calls from banks posing as technical teams or representatives[21]. In order to facilitate illicit financial activities, the caller deceived the victim into divulging private and sensitive information, including an OTP, credit/debit card number, CVV number, expiration date, secure password, ATM pin, and online banking login credentials.

- **Cheating Scams**

Senders that engage in cheating schemes promise substantial sums of money in return for a fee[22]. The scammers then ask for money to pay for the transfer's expenses. Victims frequently say they were chosen for a job abroad, won the lottery, or were promised inexpensive products. Large sums of money are deposited for a variety of expenses, trapping them in a staged process. Usually conducted from overseas, these scams include the placement of funds into Indian courier or offshore accounts.



Graph 1: Types of crime faced by Human Victims

[20] Cybercrime Unit Delhi Police, "Net Banking/ATM Frauds" <https://cyber.delhipolice.gov.in/netbanking.html> accessed on 25 June 2025
[21] Cybercrime Unit Delhi Police, "Fake Calls Frauds" < https://cyber.delhipolice.gov.in/fakecallsfrauds.html> accessed on 26 June 2025
[22] Cybercrime Unit Delhi Police, "Cheating Scams" < https://cyber.delhipolice.gov.in/cheatingscams.html> accessed on 26 June 2025

A survey was conducted to gain insights into the prevalence and nature of cybercrimes experienced by individuals. The survey gathered responses from 111 participants across various age groups, educational backgrounds, and professions, with a majority falling within the 18–35 age bracket, representing a digitally active demographic. To reach a broad and diverse audience, the survey was disseminated using Google Forms via WhatsApp, SMS, Instagram, and other social media platforms, ensuring ease of access and higher participation. According to the findings, 40.5% of respondents experienced UPI/online payment scams, making it the most common type of cybercrime reported. This was followed by 22.5% who encountered fake job offer scams, 21.6% who faced phishing attacks, and 20.7% who suffered OTP fraud. Other forms of cybercrime reported included identity theft (14.4%), credit/debit card fraud (13.5%), and investment scams (9.9%). Additionally, 3.6% of respondents reported attempted but unsuccessful frauds, while 0.9% stated that no one in their circle had been defrauded.

The survey results highlight the widespread nature of online fraud and underscore the urgent need for enhanced digital literacy, awareness campaigns, and stricter cybersecurity measures. These findings also point to a growing trend in targeted scams that exploit financial systems and employment-related vulnerabilities, especially among younger internet users.

V. Cybercrime Provisions under the Information Technology Act, 2000

The Information Technology Act, 2000[23], forms the backbone of India's cyber law regime and plays a vital role in regulating cyber activities and addressing various forms of cybercrimes. It prescribes penalties and liabilities to safeguard digital transactions, ensure privacy, and maintain the integrity of computer systems and electronic data.

Section 66A[24] previously criminalized the sending of offensive, false, or misleading information through computers or communication devices with the intent to cause annoyance, inconvenience, danger, or harm. This offence carried a punishment of up to three years of imprisonment and a fine. However, in the landmark case of *Shreya Singhal v Union of India*[25], the Supreme Court of India struck down Section 66A, ruling it unconstitutional on the grounds that it was vague, overly broad, and violative of the fundamental right to freedom of speech

[23] Information Technology Act, 2000
[24] Information Technology Act 2000, s 66A
[25] *Shreya Singhal v Union of India,* Writ Petition (Criminal) No. 758 of 2014, Supreme Court of India (24 March 2015)

and expression under Article 19(1)(a) of the Constitution.

Section 66E[26] addresses privacy violations by penalizing individuals who knowingly capture, publish, or transmit images of a person's private body parts without their consent. This section applies even in situations where the victim has a reasonable expectation of privacy, whether in public or private spaces. The punishment under this section includes imprisonment of up to three years, a fine of up to ₹2 lakh, or both.

Section 66F[27] pertains to cyber terrorism and prescribes life imprisonment for any act carried out using computer resources that threatens the sovereignty, integrity, security, or unity of India, or that causes terror among the public. This section reflects the gravity with which the law treats cyber activities that have national security implications.

Section 67[28] deals with the publication or transmission of obscene electronic material that can corrupt or deprave viewers. For a first offence, the punishment includes imprisonment of up to three years and a fine of up to ₹5 lakh, while subsequent offences can result in imprisonment of up to five years and a fine of up to ₹10 lakh. Section 67A[29] is a related provision that criminalizes the publication or transmission of sexually explicit content in electronic form. The first conviction under this section may lead to imprisonment of up to five years and a fine of up to ₹10 lakh, whereas a second conviction can result in up to seven years of imprisonment and a similar fine. In the case of *Jitender Singh Grewal v The State of West Bengal*[30], the accused had created a fake Facebook account in the victim's name and uploaded obscene images. He was charged under several sections of the Indian Penal Code (including Sections 354A, 354D, 500, 509, and 507) as well as Section 67A of the IT Act. The trial court denied him bail, and the Calcutta High Court upheld this decision, reinforcing the seriousness of such offences.

Lastly, Section 72[31] of the Act ensures the confidentiality of electronic records by punishing individuals who, while exercising powers under the IT Act, access personal information and disclose it without the consent of the concerned individual. This section aims to protect the

[26] Information Technology Act 2000, s 66E
[27] Information Technology Act 2000, s 66F
[28] Information Technology Act 2000, s 67
[29] Information Technology Act 2000, s 67A
[30] *Jitender Singh Grewal v. The State of West Bengal,* Criminal Miscellaneous No. 7252 of 2018, Calcutta High Court (17 September 2018)
[31] Information Technology Act 2000, s 72

privacy of data accessed during official or authorized duties and carries a penalty of up to two years' imprisonment, a fine of up to ₹1 lakh, or both.

Together, these provisions form a comprehensive legal framework to combat cybercrimes in India, promote responsible digital behaviour, and safeguard the rights and interests of users in the digital space.

VI. Individuals and Entities Commonly Affected by Cyber Offenses

Many demographics in India are impacted by cybercrime; however, according to recent data and trends, some groups are more vulnerable than others. It may surprise you to learn that a large percentage of cybercrime victims in India are highly educated people[32]. About 48% of victims of cybercrime, including IT specialists and workers in the business sector, have a high level of education. This demographic is frequently the target of sophisticated frauds that take advantage of their financial resources and online activity.

Targeted cybercrimes against women occur far too frequently. The National Commission for Women reports that 54.8% of women had been the victim of cyberbullying. In India, women make up 56% of victims of cyberstalking. Gender-specific cybercrimes, such as online harassment, cyberbullying, cyberstalking, and revenge pornography, disproportionately target women. The number of reported cases of revenge porn rose from 91 in 2019 to 227 in 2020, a 148% rise in a single year.

Cybercrimes regularly target individuals using digital financial services. In India, financial fraud is regularly the most common form of cybercrime. A total of ₹179 crore was lost in 205,347 instances of online banking fraud in 2020[33]. Victims of ATM card fraud are frequent, and thieves frequently use hacking techniques or skimming devices.Cybercrime in India is a growing concern, with Uttar Pradesh having the highest number of cases in 2018. Tamil Nadu and Telangana have seen significant increases in cybercrime cases[34]. Teenagers and young adults are particularly vulnerable. The number of cybercrime incidents has risen by 57%

[32] Akshaya R, Saravanan C, Divya T.L, "A Novel Approach for Building Cybercrime Prediction and Analysis Model" < https://ieeexplore.ieee.org/abstract/document/10816938> accessed on 28 June 2025
[33] Sudhanshu Sekhar Tripathy, "A comprehensive survey of cybercrimes in India over the last decade" < https://mail.ijsra.net/sites/default/files/IJSRA-2024-1919.pdf> accessed on 30 June 2025
[34] Press Information Bureau Delhi (PIB), "Cybercrime and Frauds" < https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=1883066> accessed on 2 July 2025

between 2020 and 2022, highlighting the need for comprehensive cybersecurity knowledge and defensive measures.

VII. Digital Harassment and Abuse of Women via Cyber Offenses

In India, the following are the most prevalent forms of cybercrime directed at women:

- **Online harassment:** Using social media and other digital channels to send women disrespectful, abusive, or threatening messages or remarks. One of the most common types of cybercrime against women, it causes a great deal of dread and emotional pain. According to studies, 54.8% of women have been the victim of cyberbullying[35].

- **Cyberstalking:** A pattern of persistent online harassment in which a woman's online activities are followed, observed, or tracked via messaging apps, emails, or social media. India has seen a 91% spike in cyberstalking incidents in recent years, with women making up 56% of the victims.

  Under the case of *State of Tamil Nadu v Suhas Katti*[36], the accused created a fictitious email account under her name and sent emails to the victim, a divorced woman, asking for information. Because she was receiving obnoxious phone calls in the brief that was soliciting, the victim experienced mental harassment as a result of the posting of messages. As a result, in February 2004, she filed a complaint at the Egmore Court, and the accused was taken into custody by the Chennai police cyber unit. He was charged under section 67 of the IT Act of 2000 and 469/509 of the IPC. He was booked under the aforementioned sections after charges were proven against him.

- **Cyberbullying:** Cyberbullying is the practice of harassing, degrading, or intimidating women, especially young girls, through the use of technology. This includes sharing embarrassing images, making offensive posts, and circulating misinformation. In India, women make up about 40% of victims of cyberbullying.

- **Revenge pornography:** The distribution of sexually explicit photos or movies of

[35] Mr. Shashikiran V, Dr. Bharat J K, "A comprehensive analysis of crimes against women In India: An examination of NCRB Data" < https://ijcrt.org/papers/IJCRT2409238.pdf> accessed on 4 July 2025
[36] *State of Tamil Nadu v Suhas Katti*, CC No. 4680/2004, Additional Chief Metropolitan Magistrate Court, Egmore (5 November 2004)

women without their knowledge, frequently as a form of blackmail or retaliation, is known as revenge pornography. With 227 recorded cases in 2020 alone, this crime has increased by 148% in India. It harms women's reputations and results in significant emotional suffering[37].

A mechanical engineer in Assam[38] was arrested for creating pornographic content using AI software. The act began as a personal grudge but quickly escalated into a plot to make money for the accused, who made around ₹10 lakh by hiding the content behind a subscription wall. The victim filed a complaint, alleging that her manipulated photos were used to disparage her. The accused used AI software for personal reasons and had a former acquaintance.

- **Cyber Financial Fraud:** Phishing, credit card fraud, and other online frauds that target women. Women are now more susceptible to these types of scams due to the increase in internet transactions. India reported more than 205,000 incidences of internet banking fraud in 2020[39].

  The Harshad Mehta Securities Scam of 1992[40] was a large financial fraud in India, involving an estimated ₹5,000 crore. Harshad Mehta, a stockbroker, used systemic flaws in the banking and securities industries to manipulate stock prices. Mehta stole more than ₹1,000 crores and invested the money in a few equities on the Bombay Stock Exchange using faked stamp documents, fraudulent bank receipts, and illegal transactions. The scam showed a lack of regulatory monitoring and prompted reforms in Indian financial markets, including SEBI empowerment and higher compliance standards.

- **Morphing and Defamation:** Deepfake morphing is the practice of using women's images or videos to produce phony sexually explicit content and disseminating

[37] Government of India, Ministry of Home Affairs, < https://www.mha.gov.in/MHA1/Par2017/pdfs/par2025-pdfs/LS18032025/2944.pdf > accessed on 10 July 2025
[38] Hindustan Times, HT News Desk (13 July 2025) <https://www.hindustantimes.com/india-news/assam-engineer-made-rs-10-lakh-from-morphing-image-of-woman-to-defame-her-police-101752414971537.html> accessed on 14 July 2025
[39] Vishi Aggarwal, Ms. Shruti, "Cybercrime Victims: A comprehensive study" < https://ijcrt.org/papers/IJCRT1807078.pdf> accessed on 7 July 2025
[40] Tanushree Jaiswal, "Scam 1992- Harshad Mehta Scam Story" (25 February 2025) < https://www.5paisa.com/blog/scam-1992-harshad-mehta-scam-story> accessed on 11 July 2025

misleading information to disparage women online.

- **Cyber blackmail and threats:** Threatening to reveal private information or photos in order to coerce or threaten women.

- **Fake Profile Creation:** Creating false accounts or impersonating women in order to harass or swindle them. Because of a lack of knowledge about legal rights and a lack of faith in law enforcement, many cybercrimes frequently go unreported. Although India's judicial system is developing, it still has difficulties dealing with these offenses.

  In this case of *Manish Kathuria v Ritu Kohli*[41], Manish Kathuria was taken into custody by Delhi Police's crime branch for unlawfully using her name to communicate on the website "MIRC" to stalk an Indian woman named Ms. Ritu Kohli. He disseminated her home phone numbers and used foul and offensive language, asking people to call and talk to her. Because of this, Ritu continued to get pornographic calls from all directions and was subjected to filthy conversations. She reported the incident to Delhi police while in a condition of shock. The police acted quickly, found the offender, and filed a criminal complaint against him for insulting Ritu Kohli's modesty under sections 67 of the IT Act and 509 of the IPC[42].

VIII. Cyber Criminals

An offender or criminal is any individual who commits a crime or illegal conduct with the purpose of committing a crime. Any individual who engages in cybercrime is referred to as a cybercriminal in this sense. The majority of amateur hackers and cybercriminals are teenagers between the ages of 9 and 16, which may seem hard to accept but is true[43].

Hacking into a website or computer system is a source of pride for kids, who have just recently started to comprehend what seems to be a lot about computers. These young insurgents could also engage in cybercrimes without being fully aware of their actions. Hacktivists are people who hack websites for political reasons. Pakistani Cyber Warriors have attacked 200 Indian

[41] *Manish Kathuria v Ritu Kohli*, C.C. No. 14616/2014, Delhi High Court
[42] Prachi Shah, "Cyber stalking & the impact of its legislative provisions in India" <https://www.legalindia.com/cyber-stalking-the-impact-of-its-legislative-provisions-in-india/> accessed on 10 July 2025
[43] Dr. Meenu Sharma, "Risk of Cybersecurity Threats, Cyberterrorism and Cyber Warfare" < https://download.ssrn.com/2024/12/21/5066911.pdf> accessed on 10 July 2025

websites, exemplifying political hacktivists[44]. Increased computer independence and automation have made it easier for irate workers to commit computer-related crimes, causing significant financial losses. Businesses now store information electronically, making it easier for competitors to steal trade secrets. Professional hackers are hired for industrial espionage, as it eliminates the need for physical presence to retrieve vital documents[45].

In 2019, cybercriminals targeted Paytm users through phishing attacks by pretending to be Paytm representatives. They deceived users into sharing their login details, resulting in unauthorized account access and financial losses. This case underscored the importance of user vigilance and stronger cybersecurity measures to protect digital payment platforms[46].

IX. Factors Contributing to the Surge of Cybercrime in India

One of the primary causes is the nation's swift digital transition. Over the past ten years, internet usage in India has significantly increased, greatly increasing the potential victim pool for cybercriminals. Cybercriminals now have more ways to take advantage of weaknesses in online platforms because of the growing digital economy, which is fuelled by e-commerce, online banking, and digital transactions. Furthermore, new security issues have emerged as a result of the move to cloud-based services. The dangers of improperly configured or insufficiently secured cloud resources are highlighted by the fact that 68% of organizations say that cloud account takeovers are one of the biggest security risks[47].

The rise in cybercrime is also fuelled by people's and businesses' lack of awareness about cybersecurity[48]. Many people are easy targets because they lack the knowledge necessary to recognize possible risks or implement efficient preventive measures. Furthermore, as internet access grows quickly, inequalities in digital literacy imply that more people are using technology without the required cybersecurity training, making them more vulnerable to

[44] Times of India (TOI), "Pakistani hackers claim to have breached many Indian defence sites" (6 May 2025) <https://timesofindia.indiatimes.com/india/pakistani-hackers-claim-to-have-breached-many-indian-defence-sites/articleshow/120912212.cms > accessed on 11 July 2025

[45] G. Rathinasabapathy and L. Rajendran, "Cybercrime and Information Frauds" <https://www.academia.edu/2821473/Capacity_Building_in_the_Knowledge_Environment_A_Human_Resource_Development_Approach> accessed on 10 July 2025

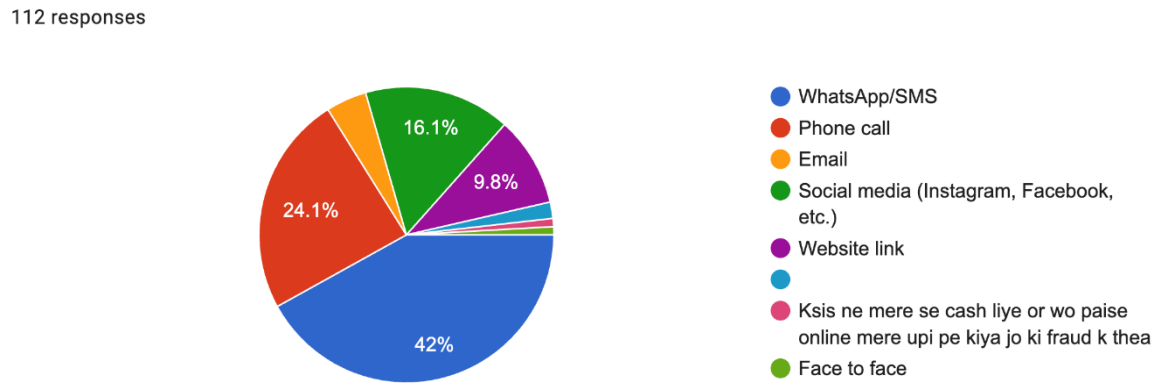
[46] Times of India (TOI), "Paytm offers cyber fraud covers of up to Rs 10,000 at Rs 30" (20 December 2022) < https://timesofindia.indiatimes.com/city/mumbai/paytm-offers-cyber-fraud-cover-of-up-to-10000-at-30/articleshow/96357846 >

[47] SentineIOne, "50+ Cloud Security Statistics in 2025" < https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-security-statistics/> accessed on 20 August 2025

[48] Shambhavi Tripathi, "Cybercrime and Cybersecurity" < https://blog.ipleaders.in/cyber-crime-and-cyber-security-an-overview/> accessed on 10 July 2025

assaults. India's cybersecurity infrastructure is struggling to keep up with evolving hacking strategies due to lack of investment, antiquated systems, and lack of coordination between public and private entities. Legal and jurisdictional obstacles complicate investigations, leading to stalled crimes[49].

Chart 1: Different ways in which individuals are exposed to cyberfraud.



This survey was conducted to understand how individuals come into contact with cyberfraud. According to the results, 42% of respondents encountered fraud through WhatsApp or SMS, 24.1% via phone calls, 16.1% through social media platforms, 9.8% through website links, and smaller percentages through email, face-to-face interactions, or other sources.

X. Repercussions of Cyber Offenses

Crimes affect victims and their loved ones in a number of ways, including behaviourally, physically, emotionally, physiologically, financially, cognitively, spiritually, and socially. Everyone is impacted by cybercrimes, whether directly or indirectly, and they can lead to anxiety and financial hardship. Secondary victims, such as friends and relatives, might not get the attention they need, and helping groups and cultures can be difficult, even when the primary victims are simple to identify[50]. Hacking, cyberbullying, cyberstalking, harassment, pornography, fraud, and defamation are examples of cybercrimes that can cause mental shock

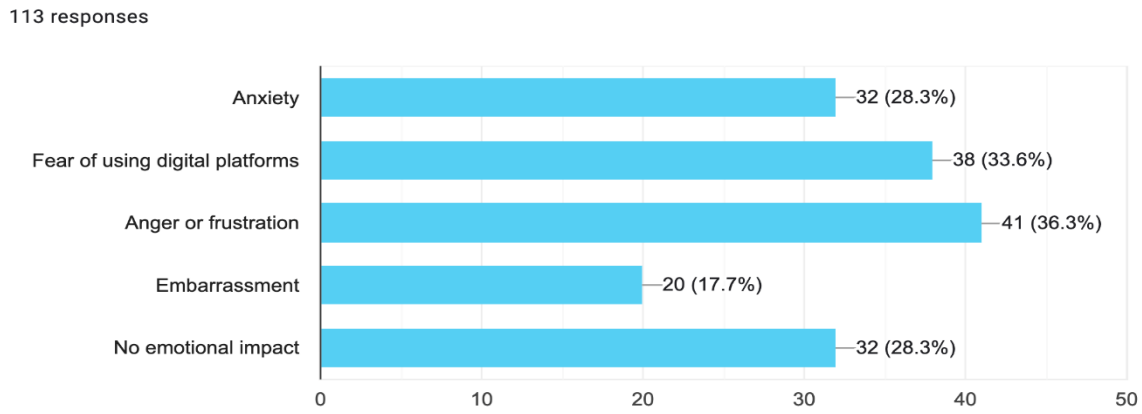
[49] Times of India(TOI), "Cybersecurity is a matter of national importance" (15 July 2025) < https://timesofindia.indiatimes.com/city/bengaluru/cybersecurity-is-a-matter-of-national-importance-says-mp-yaduveer-at-bsides-bangalore-2025/articleshow/122436217.cms > accessed on 24 July 2025

[50] Swapnali V Jadhav, Mayuri Kumar, Swaroop S S., Mahipal S. S., "Psychological Influences of Cybercrime on Human Mind and Behaviour" < https://www.researchgate.net/publication/380402545_Psychological_Influences_of_Cyber_Crimes_on_Human_Mind_and_Behaviour> accessed on 11 July 2025

or trauma. This can lead to psychological issues like despair, suicidal thoughts, substance abuse, anxiety disorders, and a higher chance of experiencing more abuse.

Even after the crime has been committed, victims may have emotional consequences like PTSD, despair, rage, terror, and lack of sleep[51]. Cybercrimes can also result in financial losses, psychological distress, and victim-blaming, which can seriously impair the victim's mental health. Anxiety, bodily pain, heart attack, stroke, decreased sex drive, and other health issues are among the physical effects of cybercrimes.

Graph 2: Types of Mental Stress Experienced by Individuals



The survey emphasizes the mental stress that people endure as a result of cybercrime, underscoring the pressing need for knowledge and help.

XI. Initiatives to Mitigate Cybercrime Threats

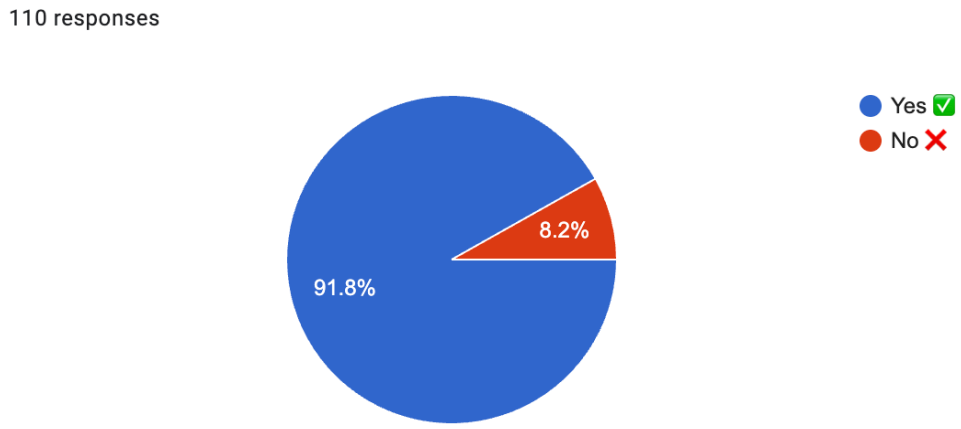
The adage *"prevention is better than cure"* applies to computers as much as to human health. Preventing cybercrimes by taking the appropriate measures is always preferable. Although total internet security and the eradication of cybercrime may not be achievable, businesses can lessen their vulnerability to it by implementing a defined in-depth approach to system, network, and data protection as part of a successful cybersecurity strategy[52]. The following actions can help lower the risk of cybercrime:

[51] Deepanjali Mishra, "Impact on Mental Health of Women Victims of Cyberviolence" < https://www.indianjournals.com/ijor.aspx?target=ijor:ijphrd&volume=10&issue=9&article=021&type=pdf> accessed on 11 July 2025

[52] Akash Kori,"Critical Analysis of Cyber Laws in India" < https://blog.ipleaders.in/cyber-laws-in-india/ > accessed on 11 July 2025

Establishing clear regulations, developing incident response plans, and putting robust cybersecurity measures in place are all necessary for businesses to maintain a secure digital environment. Verifying odd email requests, updating systems often, and storing up data to guard against loss during cyberattacks are all part of this. Workers should be continuously trained on security procedures and breach response techniques. They should not share passwords or sensitive information online, limit social media access to trustworthy connections, and post cautiously. Furthermore, installing software only from reputable sources is critical to avoiding security threats[53].

Chart 2: Percentage of individuals who understand the cybercrime portal in India



This chart is specifically designed to help people understand how they use the cybercrime portal in India. In our study, 91.8% of participants said they knew how to use the cybercrime portal, compared to 8.2% who didn't. This high level of awareness is a good sign because it indicates that the majority of people understand how to access and use a critical platform for reporting cybercrimes. In an era of growing digital risks, such understanding is critical for guaranteeing timely reporting, reducing harm, and promoting digital safety.

XII. Pivotal Cybercrime Incidents Exposing India's Digital Vulnerabilities

- The ***Vijay Mallya and Kingfisher Airlines scam***[54] entailed the theft of ₹9,000 crore for Kingfisher Airlines from 17 Indian banks. Mallya secured the loans using false financial

[53] Mrs. Renuka P. D., Mrs. Preeti B., "Impact of cybercrime on mental health" < https://www.iesrj.com/upload/2.%20Mrs.%20Renuka%20Polly%20Dass,%20Mrs.%20Preeti%20Bahuguna%20-%20Online.pdf> accessed on 11 July 2025

[54] Advocate Misha Deb, "An analysis of the Vijay Mallya case" < https://blog.ipleaders.in/analysis-vijay-mallya-case/ > accessed on 11 July 2025

documents, but the monies were later diverted to personal accounts, enterprises, and unrelated ventures. Kingfisher Airlines shut down in 2012, and Mallya fled India in 2016, becoming a fugitive economic offender. Reforms and more stringent due diligence for high-value loans resulted from the scam, which also revealed problems with financial monitoring.

- In August 2018, one of the biggest and most advanced cyberattacks on an Indian bank occurred at ***Cosmos Bank***[55]**.** Hackers gained access to the bank's ATM switch and SWIFT systems, allowing them to make over 12,000 fraudulent ATM withdrawals and 2,800 transactions in seven hours. The attackers cloned debit cards and exploited the bank's transaction messaging system, enabling large cash withdrawals without real-time verification. Eleven of the eighteen people detained have been found guilty.

XIII. CONCLUSION & SUGGESTIONS

India's rapid embrace of technology has fuelled innovation and economic growth but also exposed the nation to new and evolving threats in the form of cybercrime. The research highlights a significant rise in cyber offenses from financial fraud and phishing to digital harassment and identity theft with a disproportionate impact on vulnerable groups such as women and youth.

While the Information Technology Act, 2000, offers a foundational legal framework to combat these threats, its limitations are evident. The absence of a comprehensive data protection law, vague enforcement mechanisms, and outdated infrastructure continue to undermine the effectiveness of cybersecurity measures. High-profile cases like the Cosmos Bank cyberattack and financial frauds involving figures like Vijay Mallya have further revealed deep systemic flaws and the urgent need for digital reforms.

Addressing this crisis requires a multi-pronged, proactive strategy. India must update and strengthen its cybersecurity and data protection laws, improve coordination between law enforcement and the judiciary, and invest in advanced digital infrastructure. Digital literacy and awareness campaigns especially targeting youth, women, and rural users are vital for building

[55]Dhaarani S. & Aaliya Ameer A, "A case study on cybersecurity threat to Cosmo Bank" < https://ijirl.com/wp-content/uploads/2023/12/A-CASE-STUDY-ON-CYBER-SECURITY-THREAT-TO-COSMOS-BANK.pdf> accessed on 12 July 2025

resilience against online threats. Moreover, streamlined grievance redressal mechanisms and robust victim support services are essential for fostering public trust and timely reporting. India now stands at a critical juncture. It must leverage its technological strengths not just for development but also to ensure safety, privacy, and trust in the digital ecosystem. Only through a comprehensive, inclusive, and forward-looking approach can India secure its digital future for all.