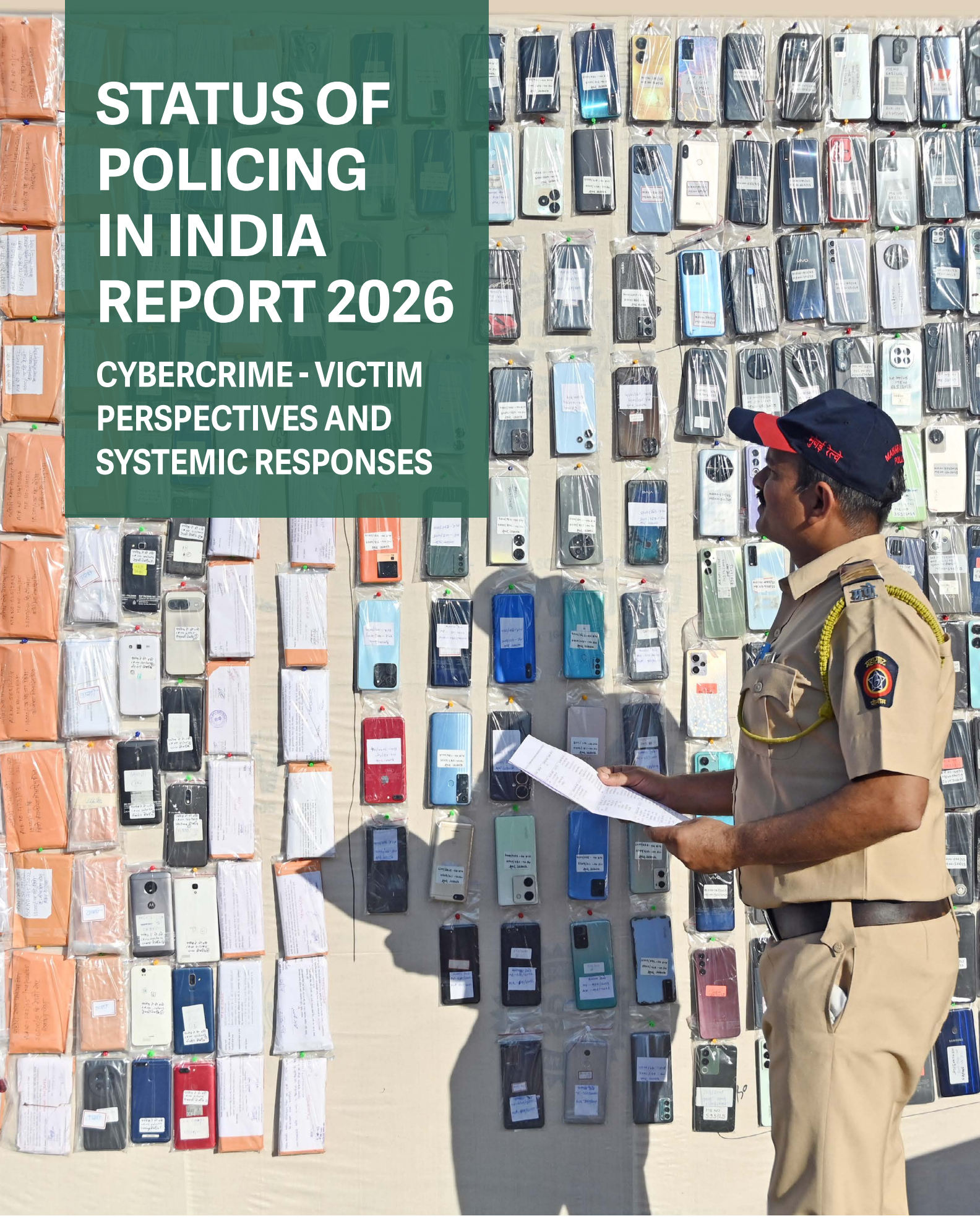
STATUS OF POLICING IN INDIA REPORT 2026

CYBERCRIME - VICTIM PERSPECTIVES AND SYSTEMIC RESPONSES



COMMON CAUSE
A ROMANCE WITH PUBLIC CAUSES SINCE 1980

लोकनीति
Programme for Comparative Democracy

LAL FAMILY FOUNDATION

CSDS
centre for the study of developing societies

STATUS OF POLICING IN INDIA REPORT 2026

Cybercrime - Victim Perspectives and Systemic Responses

COMMON CAUSE
A ROMANCE WITH PUBLIC CAUSES SINCE 1980

लोकनीति
Programme for Comparative Democracy

LAL FAMILY FOUNDATION

CSDS
centre for the study of developing societies

For limited circulation, not for sale.

Common Cause, Common Cause House, 5, Institutional Area,
Nelson Mandela Road, Vasant Kunj, New Delhi 110 070
Phone: +91-11-45152796
E-mail: commoncauseindia@gmail.com
Website: www.commoncause.in

Lokniti, 29, Rajpur Road, Civil Lines, Delhi 110 054
Phone: +91-11-45789412
Email: csdsmain@csds.in; lokniti@csds.in
Website: www.csds.in; www.lokniti.org

Published by

Common Cause & Lokniti – Centre for the Study of Developing Societies (CSDS)

Usage of information

Cover image: Government Railway Police GRP recovered over a thousand stolen mobile phones in Ghatkopar (Mumbai, Maharashtra - December 10, 2025).

Credits: Raju Shinde/Hindustan Times

Note: The pictures in this report are for representational purposes only.

Designed & Printed by

FACET Design
D-9, Defence Colony, New Delhi - 110024
+91-11-24616720, 41553497

Team Members

Team Advisory Committee

Vipul Mudgal
Sanjay Kumar
Suhas Palshikar
Sandeep Shastri

Research Team/Authors

Vibha Attri
Divya Singh Chauhan
Rishikesh Kumar
Mohd. Aasif
Krishangi Sinha
Kirti Sharma
Manmitha
Athulya T. Anilkumar

Data Support

Himanshu Bhattacharya
Himanshu Kapoor

Lead Researchers and Authors

Radhika Jha
Vinson Prakash
Priyanka Mittal
Devesh Kumar

Research Support

Dhruv Pandey
Nikita Jha
Divyanshoo Singh
Dhananjay Kumar Singh
Rishikesh Yadav

Interns

Chhavi Mishra
Kiera Potineni
Lavanya Mittal
Nadiya

State Coordinators & Supervisors

Assam: Dhruba Pratim Sharma and Suman Kumar Das
Bihar: Rakesh Ranjan and Vijay Kumar Singh
Delhi: Rishikesh Yadav
Gujarat: Bhanukumar Parmar and Vithalbhai Chimanbhai Talpada
Haryana: Chanchal Kumar Sharma and Sweta Raj
Jharkhand: Harishwar Dayal and Amit Kumar
Karnataka: Veena Devi and Nagesh K.L.
Kerala: Nitya Neelakandan Radha and P.S. Abhishek
Madhya Pradesh: Yatindra Singh Sisodia and Manish Gyani
Maharashtra: Nitin Birmal and Shivaji Girirao Motegaonkar
Odisha: Gyana Ranjan Swain and Ushakanta Sahoo
Rajasthan: Sanjay Lodha and Manoj Rajguru
Tamil Nadu: P. Ramajayam
Telangana: Vageeshan Harathi and T. Venkatesh
Uttar Pradesh: Shashikant Pandey and Ranjana Upadhyay
West Bengal: Suprio Basu and Rima Ghosh

Contents

List of Figures

List of Tables

Kolkata Police Bust a Fake Call Centre in a raid (Kolkata, India – April 23, 2026).

Photo by Kolkata Police FB Page.

Cybercrime: Introduction and Context

Cybercrime: Introduction and Context

Digital technology has transformed our lives faster than any innovation in human history. If used sensibly, it can make our futures fairer, brighter and more peaceful. Its potential to empower individuals, support inclusion, and improve access to public services makes it a powerful equaliser in an unequal world. Sensible use matters because our experience has been that, without citizen-centric guardrails, the same technology can be used to cheat and manipulate us or exploit our data for mass surveillance.

As the digital revolution reshapes our work, investments and relationships, its harmful aspects also evolve almost in tandem. We can make payments or trade stocks in a flash, but can also lose our savings within seconds. Fame and glory can be earned spontaneously, but reputations can be ruined as quickly. We have got used to remote work, video conferencing and digital workplaces. So, if citizens turn into netizens, can criminals be stopped from shifting online? Crimes or illegal actions committed in the cyber sphere, using a networked device, are broadly defined as cybercrimes.

We are also learning a new vocabulary with terms like hacking, phishing, deepfakes, ransomware, identity theft, morphing, and many more. We should be alarmed that things are going far beyond the personal sphere. Unregulated technology use is polarising our world by weaponising anxieties and making hate speeches viral. Citizens globally are also learning that its illegal and malicious use poses grave threats to free speech and electoral integrity (OHCHR, 2025). We hope to take up some of these issues in the future. However, the Status of Policing in India Report (SPIR 2026) takes up a small part of illegal digital activities: cybercrimes committed against ordinary citizens and the state of our preparedness to tackle them.

For this study, we have mainly dealt with three types of cybercrimes: (a) where someone impersonates a victim or illegally breaks into her device without her knowledge, (b) when someone uses "social engineering" to manipulate a victim psychologically, tricks her into disclosing confidential information or making a digital arrest, and (c) when someone is made a target of trolling, cyberbullying, online sexual abuse or harassment. The study is based on all-India surveys, in-depth interviews and focus group discussions (FGDs) with domain experts.

As an early mover in digital technology adoption, India has had more than its share of cyber-attacks and security breaches. We face the twin challenge of a profusion of cybercrimes and a lack of preparedness among the police and the courts. The rapid expansion has also commodified data and made it vulnerable to theft and attacks. Our impressive adoption to the Internet of Things (IoT) is inadvertently making us prime targets (and gullible enablers) of cybercrime. Obviously, police and courts have a lot of catching up to do in the new scheme of things.

The data points to a new shift in criminal activities from offline to online. In 2024, registered cases of cybercrime surged by over 17 per cent while traditional cognisable crimes fell by six per cent, according to the National Crime Records Bureau (NCRB). Between 2020 and 2024, the rate of cybercrimes nearly doubled. The scale outpaces conventional crimes because a single criminal can target hundreds of victims, using simple devices. The payouts can also be huge and quick, but the rates of arrest and resolution are slow. Then there are barriers of jurisdiction between states, regions and countries. No wonder that cybercrimes are the lowest-risk and highest-reward activities in the world of crime today. A UNODC study on

cybercrimes noted as early as 2013 that soon it would be hard to imagine any crime without the involvement of an electronic device or the internet (Malby et al., 2013).

Perceptions and Experiences

Cybercrime is also an under-researched subject because its fast-changing nature makes it difficult to study trends and patterns or time-series data. The SPIR 2026 tries to fill that gap by studying the perceptions and perspectives of ordinary victims and systemic preparedness.

SPIR 2026 is the seventh report on policing and the rule of law. It is supported by our philanthropic partner, the Lal Family Foundation. Jointly prepared by Common Cause and Lokniti-Centre for the Study of Developing Societies (CSDS), it delves into the victims' experiences with reporting, investigation and disposal of these crimes in light of the preparedness of the police, banks, courts and other institutions. The report also documents the prevalence and the resolution of common cybercrimes. It taps into the wisdom of domain experts to complement the findings of the all-India survey.

The citizen survey involved over 8,306 ordinary citizens in five districts each in 16 states of India, including 1,085 victims and 814 respondents who assisted victims. The qualitative analysis is based on interactions with 37 in-depth interviewees and FGD participants. The surveys cover the lower, middle and higher-income localities in selected urban and rural areas. The study focused on the nature and experiences of victims across offences such as online fraud, digital arrests, trolling, bullying, identity theft, and online sexual harassment.

The victims feel particularly helpless because of the anonymity and sophistication of attackers. Cybercrime shatters their sense of control over their privacy, personal devices and bank accounts. Many are overcome by shame and guilt, often blaming themselves for not securing their data well enough or for falling for the scams so easily. Sometimes, they avoid sharing their experiences with friends and relatives, fearing that their lack of judgment would be ridiculed. Many victims have very low expectations of recovery, and they end up not reporting the matter to the police or not following up on the case.

Several victims confided that they were facing stress, trauma and depression not only because of the cybercrime but also due to the cumbersome procedures that need to be followed. One of the victims was so impacted that she had a miscarriage. Another had to leave her profession and move to a different country, unable to overcome the fear and the trauma. A senior citizen reported having gone into a state of severe depression after losing his entire life's savings and retirement benefits.

The sheer impact and scale of the activity are scary and alarming. Portals and systems operated by the Indian Cyber Crime Coordination Centre (I4C) show that between 2021 and 2025, nearly two lakh FIRs were registered in more than 65 lakh financial fraud complaints involving a whopping Rs 55,000 crore (*The Hindu*, 2026). For the criminals, these activities are like a picnic when compared to the risks associated with conventional crimes, such as endangering their lives while stealing or robbing physical assets and monetising them. Cybercriminals, even after being caught, can get away with penalties and short-term imprisonment. Some crimes are common but invisible because of grave under-reporting. These include sextortion, blackmail with intimate images, and cyberstalking to cause fear or distress.

Women and Digital Spaces

Women are frequent targets of cyberstalking, digital voyeurism, revenge porn, and picture morphing (superimposing a person's face onto explicit images) for blackmail or slander. SPIR 2026 found women to be more fearful of cybercrimes than men. Following reports of suicides by women victims in Kerala after being harassed online, a group of feminists, educators, lawyers and government officials held a consultation recently. Anita Gurumurthy and Niveditha Menon of Bangalore-based IT for Change, who participated in the consultation, have warned that policy choices need to avoid

narratives of fear around new technologies that can constrain women's freedom to use digital spaces.

A Parliamentary Standing Committee on the Empowerment of Women quoted NCRB data to highlight that in the five years between 2017 and 2022, cybercrimes against women increased by 239 per cent and there was a "multi-fold rise" in the cases involving children (PRS, 2026). The Committee was particularly concerned about the inadequacy of cyber safety awareness among women and children in rural areas. It recommended training of Asha and Anganwadi workers in cybersecurity; age-appropriate social media regulations for young adults and higher accountability standards for digital platforms.

Replying to a question in Parliament, the Home Ministry said that between 2021 and 2025, online and social media crimes, including cyberstalking, impersonation, identity theft and harassment, surged 140 per cent. This period has also recorded a nearly five-fold increase in complaints regarding child sexual abuse material (Basu, 2026). Crimes against senior citizens have also increased considerably. Over 70 per cent of all registered cybercrimes were online financial frauds.

The elderly are particularly vulnerable as criminals exploit their sense of fear, urgency, loneliness or lack of ease with digital technologies. This makes them key targets for impersonation and digital arrests. Scammers also use deepfakes pretending to be their friends or grandchildren, or bank officials asking for KYC updates. Even overtly cautious senior citizens sometimes fall for clickbaits faking charities or miracle cures. Retired professionals and businessmen are also perceived as high-value targets because of better financial standing, regular pensions, savings and other assets built over a lifetime.

As police and public order are state subjects under the Indian Constitution, the primary responsibility for the prevention, detection and investigation of crimes, including cybercrimes against women and children, lies with the state or UT governments. The Central Government supplements this with awareness campaigns, provides advisories and occasional financial assistance under various schemes. It has also created an 'Indian Cyber Crime Coordination Centre' (I4C), which runs a toll-free helpline number (1930) and a national Cyber Crime Reporting Portal (NCRP) with special focus on cybercrimes against women and children (PIB, 2026).

Social Engineering Syndrome

A common element in a large number of cybercrimes is the psychological manipulation of victims to lure them into sharing private data or granting access to personal devices or credentials. Unlike breaking firewalls or hacking security codes, social engineering perpetrators "hack" human minds by winning trust through emotional manipulation, raising fear about a loved one being in crisis, or invoking urgency about a delivery or pending action. They also follow the target's routine or anxieties, or collect information through fake emails, infected downloads or with the help of compromised bank officials.

The SPIR 2026 also found that, except in odd cases, cybercriminals run fairly well-organised networks. Some of them deal directly with victims and others sell leaked sensitive information about potential victims or "kits" comprising mule accounts and fake SIM cards. Many cases go unreported because of a lack of trust in the police and other authorities and a lack of awareness. It is also concerning that most of the victims who recovered the lost money fully or partially were those who were able to use personal influence. Victims who paid a bribe to the police were three times more likely to recover the money.

The response of the banks was found problematic by both the victims and experts of financial cybercrimes. They strongly felt that the banks refused to take responsibility or failed to assist victims through the recovery process. The banks almost always maintained that the victims "collaborated" with the fraudster. Nearly a quarter of the victims were highly dissatisfied with the banks' role in recovering the lost money. While the victims were mostly kept in the dark

about the progress in the investigation, the police often cited problems of jurisdiction and lack of coordination between state police departments. Many respondents found the complaint registration process quite cumbersome.

The domain experts also corroborated that most cases of online gender-based violence and non-consensual image abuse go unreported. They agreed with the victims that the online police complaint mechanism was difficult to understand, cumbersome to navigate and unclear about the investigation to be followed. Many did not receive any communication from the police other than an automated acknowledgement number. The experts also highlighted the police apathy towards online gender-based crimes and their tendency to blame the victims. The focus of the police is often on "settling" the cases between victims and perpetrators through compromise.

The SPIR 2026 also confirmed at least one finding of the earlier SPIRs that police are particularly harsh on victims from poor and underprivileged backgrounds. However, most other victims who visited cyber police stations or units felt that the staff was polite and helpful. The poor, on the contrary, complained that the police were rude, abusive, dismissive and unwilling to register FIRs. A quarter of the victims surveyed said they had to visit the police stations five times or more, particularly those from rural areas. The poorer victims were nearly four times more likely to pay a bribe to the police. Those who paid a bribe were more likely to recover their loss.

This study aims to understand people's perceptions and experiences with cybercrimes and the system's preparedness to tackle them. The qualitative insights from victims and domain experts are contained in the first two chapters, and the rest of the chapters are on the findings of the nationwide survey. Chapter 1 contains insights from interviews with cybercrime victims and their experiences with the reporting process and case outcomes. Chapter 2 further highlights these victims' experiences with institutions like the police, banks, courts and civil society organisations.

Chapter 3 contains citizens' perspectives about exposure to digital attacks like scam calls and messages, etc., as well as their anxieties about digital safety and vulnerability. Chapter 4 presents the data on the penetration and nature of various cybercrimes faced by the survey respondents. Chapter 5 focuses on the victims' experiences during complaint redressal processes with the police as well as courts. Chapter 6 brings out victims' experiences with the banks, while Chapter 7 covers the respondents' online payment and banking behaviours, and their use of social media or digital apps/ platforms. Chapter 8 discusses the security measures deployed by citizens to safeguard themselves against cyber vulnerability. Chapter 9 reports the public's assessment and perceptions of the institutions dealing with cybercrimes—police, banks and courts.

We are aware that SPIR 2026 covers only a slice of a rapidly expanding landscape. Nonetheless, it is part of our attempt to assess the impact of policing on the ground and to identify need gaps. We also see it more as a building block for more policy-oriented research in the future. We firmly believe in bridging the gap between computer science and behavioural science by keeping humans in the loop. The caution is that techno-managerial solutions must not come at the cost of citizens' dignity, privacy or civil liberties.

As always, the SPIR teams at Common Cause and Lokniti-CSDS look forward to your feedback, comments or suggestions.

Vipul Mudgal
Director, Common Cause

References

- Basu, V. (2026, March 23). *Cybercrimes against women go up in 5 years.* The New Indian Express. https://www.newindianexpress.com/india/2026/Mar/23/cybercrimes-against-women-go-up-in-5-years
- Gurumurthy, A., & Menon, N. (2009). Violence against Women via Cyberspace. *Economic & Political Weekly, 44*(40). https://www.epw.in/journal/2009/40/commentary/violence-against-women-cyberspace.html
- Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S., & Ignatuschtschenko, E. (2013, February). *Comprehensive study on cybercrime.* United Nations Office on Drugs and Crime. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
- Ministry of Home Affairs, Government of India (2025, July 29). *Cyber-crime Targeting Children* [Press release]. Press Information Bureau. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2149788&reg=48&lang=2
- PRS Legislative Research. (2026, April 1). *Cyber Crimes and Cyber Security of Women.* https://prsindia.org/policy/report-summaries/cyber-crimes-and-cyber-security-of-women
- The Hindu Bureau. (2026, June 10). *NHRC flags ₹ 52,976 crore cyber fraud losses, seeks urgent action against "digital arrest" scams.* The Hindu. https://www.thehindu.com/sci-tech/technology/nhrc-flags-52976-crore-cyber-fraud-losses-seeks-urgent-action-against-digital-arrest-scams/article71081619.ece
- UN Special Rapporteur on freedom of opinion and expression. (2025, July 4). *Elections at risk in the Digital Age.* The Office of the High Commissioner for Human Rights. https://www.ohchr.org/en/stories/2025/07/elections-risk-digital-age

CHAPTER

01

Gurugram cyber police tableau during the 77th Republic Day celebrations at Tau Devi Lal Stadium (Gurugram, Haryana - January 26, 2026).

Photo by Parveen Kumar/Hindustan Times.

The Landscape of Cybercrime and Victim Experiences

Key Findings

- Cybercrime perpetrators rely heavily on “social engineering” to commit crimes, using deception, manipulation, coercion and threats to gain access to sensitive information or personal devices.
- There are organized networks running both the financial and non-financial cybercrimes. Databases of leaked sensitive information are available for easy purchase, along with “kits” selling mule accounts and fake SIM cards.
- Many cases of cybercrimes go unreported because of the social stigma and fear of public embarrassment, lack of trust in the authorities, lack of awareness about the redressal mechanisms and the feeling that the case will not be taken seriously by the authorities. According to experts, most cases of online gender-based violence and non-consensual image abuse go unreported.
- Victims and experts noted that the online police complaint mechanism was cumbersome to navigate and lack of clarity regarding the investigation that followed. Many did not receive any communication from the police other than an automated acknowledgement number.
- Of the ten respondents who lost money through financial frauds and filed a complaint, five were able to recover a partial amount. One was able to recover the full amount. Three out of the six people had to use personal connections with people of influence to recover their money.
- Several victims described facing stress, trauma and depression due to the cybercrime and the complaints procedure that followed. One of the victims had a miscarriage. Another had to leave her profession and move to a different country. Another reported being in severe depression after losing his entire life savings post-retirement.

The Landscape of Cybercrime and Victim Experiences

Over the last decade, cybercrimes have disrupted conventional patterns of crime and the institutional responses designed to address them, traversing jurisdictions, affecting multiple institutions and communities, and evolving into a highly organised ecosystem. The crisis has compounded with limited checks in the face of inadequate technical expertise and institutional preparedness. The constantly evolving forms and increasing sophistication of cybercrimes further strain the capacity of institutions to respond effectively. Often, by the time a particular cybercrime is legally defined and public awareness begins to develop, newer variants are likely to have already emerged. While these crimes rely heavily on exploiting technological vulnerabilities, they fundamentally target the human mind—through manipulation, deception, intimidation, or coercion.

In this context, it becomes imperative to look beyond crime statistics and examine people's lived experiences, both of victimisation and of navigating institutional responses. To understand the nature and prevalence of cybercrimes and the preparedness of institutions to respond to them, this study combines a large-scale survey of the general public (reported in **Chapters 3 to 9**) with in-depth interviews with cybercrime victims and domain experts (reported in **Chapters 1 and 2**).

This chapter is based on qualitative insights gathered from detailed one-on-one dialogues and a focus group discussion (FGD). It presents findings from open-ended conversations with 37 respondents who were domain experts, cybercrime victims and those who closely assisted them, and kin of individuals charged with cybercrime. One-on-one in-depth interviews (IDIs) were conducted with 10 cybercrime specialists, serving and former police officers dealing with cybercrime investigations, senior banking officials, journalists and experts working on online gender-based violence, and 16 victims, along with two close family members who assisted them. Interviews were also conducted with family members of two persons accused of cybercrimes, and two respondents whose bank accounts were frozen due to on-going cybercrime investigations. Aside from this, a focus group discussion was conducted with five of India's well-known experts in digital rights and cybersecurity. All the qualitative insights have been analysed together.

The chapter examines victims' experiences across the trajectory of cybercrime—from the modus operandi of the crime and the reporting process, to the outcomes of their cases, the support systems available to them, and the broader personal and social impacts of victimisation. It also includes the experiences of family members of individuals accused of cybercrime and those whose bank accounts were frozen during ongoing investigations. Insights from the expert interviews and FGD are presented alongside victims' accounts to provide a more comprehensive understanding of both individual experiences and systemic responses. To protect the anonymity and confidentiality of respondents, all names have been changed, and pseudonyms are used for the victims throughout the chapter. The names of the domain experts have also not been given.

A detailed methodology for the in-depth interviews is provided in **Appendix 4.**

1.1 *Modus Operandi:* Mapping Forms of Cybercrime and its Networks

It began with a phone call to a stationery shop owner. A close friend urgently needed money to pay for medical treatment. The voice sounded familiar, the UPI payment screenshot looked genuine and messages claimed that money had already been returned. The call, screenshots and messages all turned out to be fake and the caller, though he sounded exactly like the friend that he claimed to be, was, in fact, a fraudster.

A retired senior executive from a Public Sector Undertaking (PSU) was trapped in a digital arrest for about 10 days on allegations of taking a bribe of Rs. 26 lakhs. He lost all of his life savings of nearly Rs. 66 lakhs.

In East Delhi, two sisters and their mother found themselves at the centre of an organised online hate campaign; their photographs were circulated by an organised group of cyberbullies running social media pages called "Bhagwa Love Trap", where pictures and videos of Muslim women seen with non-Muslim men were targeted for online abuse and real-life threats.

A then-minor son of a domestic worker mistakenly visited an explicit content website and was then blackmailed into paying Rs. 37,000 against threats of police complaints for visiting the website.

These are just a few of the varying cybercrime cases for which interviews were conducted. An underlying theme is the use of psychological tactics. Even as many associate the term *"cybercrimes"* with the misuse and manipulation of sophisticated technology, it is essentially, a manipulation of the mind in most cases. As noted by a renowned cybercrime expert who regularly assists police and intelligence departments with the investigation of cybercrimes, most of the cyberattacks are through *"social engineering"*. The term 'social engineering' in the context of cybercrime refers to a cybercriminal convincing the victim to provide personal information or transfer money to the criminals through fraud, deception, threat, manipulation, etc. The interviews with victims reveal a similar pattern, where cybercriminals employ carefully designed psychological, technological and organisational strategies that exploit trust, fear and urgency rather than technical vulnerabilities alone.

The most frequently reported type of cybercrime is financial cybercrime. Notably, however, non-financial cybercrimes might be just as, or sometimes even more prevalent than financial cybercrimes, but the rate of reporting for these cases is much lower. In this study, of the 16 victims that were interviewed, two were cases of cyberbullying, and one was a case of hacking. The remaining 13 cases were all different types of financial cybercrimes—digital arrests, sextortion, fraudulent investment applications, and other cyber frauds. Of the 13 financial cybercrime victims who were interviewed, only two claimed that their accounts were accessed/hacked without them sharing any information with a third party or without any known sources of data leaks. Across all other forms of cybercrimes, the perpetrators demonstrated a sophisticated understanding of human behaviour and institutional processes.

1.1.1 Building trust with the victim

Perpetrators of financial frauds used inventive ways of building trust with the victims. A victim of digital arrest explained how the caller, allegedly an officer of the Mumbai Crime Branch, informed him that his Aadhaar card may have been misappropriated and misused for illegal activities. The caller suggested to the victim that he should get a masked Aadhaar card for future purposes, which hides its first eight digits along with other personally identifiable information, while still being a valid ID card. She even guided him through the procedure to get a masked Aadhaar card from the Unique Identification Authority of India (UIDAI) website. This advice worked to further establish trust between the victim and the perpetrator and increased her legitimacy in the eyes of the victim.

Among victims of digital arrest scams, the first point of contact was typically an unsolicited phone call from an unknown number. Victims described receiving automated recorded messages alleging that their mobile number had been linked to illegal activities. They were then seamlessly transferred to individuals impersonating police or other law enforcement officials. The transition from an automated message to a seemingly professional conversation enhanced the credibility of the scam and created an immediate sense of panic. Once contact was established, the perpetrators gradually collected personal information under the pretext of verifying the victim's identity. Rather than possessing detailed prior knowledge, the fraudsters elicited information during the conversation and subsequently used publicly available information, including internet searches, to strengthen their impersonation and convince victims that they had conducted extensive background checks.

1.1.2 The leaked data economy

In many other cases, however, the perpetrators have a ready database of the details of potential victims. A cybercrime expert explained the highly organised nature of these crimes, where different groups provide different kinds of services to cybercriminals. Some groups operate only to source data. They access leaked personal data and sell it to others who use it for cyber fraud. The data includes all personally identifiable information, such as name, age, Aadhaar number, passport number, etc., which can then be used to con people. Another group sells pre-activated SIM cards and bank accounts to fraudsters, which can be used to commit crimes.

One of the experts cited a case in Odisha, where a group of people set up a unit to distribute subsidised rice. To appear legitimate, they used government logos and photos of the President of India. They distributed two kilograms of rice to each of the beneficiaries and used their personal information collected through the drive to open bank accounts in their name and activate three SIMs per person, without their knowledge. These pre-activated SIM cards and mule accounts[i] are then sold as kits, available for Rs. 10,000-20,000 each. Every week, he said, about 25,000 SIM cards are supplied only in the Mewat region, located across Haryana, Rajasthan and Uttar Pradesh, which is a well-known cybercrime hub.

There is another market for stolen phones in India. Recently, perpetrators have started sourcing stolen phones from neighbouring countries like Nepal and China since there is stricter blocking of stolen mobile phones in India, according to the expert. Perpetrators also exploit weak security systems to easily access sensitive personal information. One victim reported that perpetrators first managed to change the mobile number linked to their bank account, thereby ensuring that one-time passwords (OTPs) and transaction alerts were redirected before unauthorised transactions took place. Victims therefore remained unaware of the fraudulent activity until substantial financial losses had already occurred. The interviews suggest that attackers exploited weakness in both account verification processes and victims' susceptibility to share sensitive information.

1.1.3 From victims to unwitting accomplices

The interviews also highlight the evolving nature of fraudulent investment and betting app scams. A victim described being persuaded to install a mobile application that promised unusually high daily returns on modest investments. Initially, he received regular pay-outs, reinforcing confidence in the legitimacy of the scheme. As trust increased, victims were encouraged to deposit progressively larger sums under different investment *"cycles",* while also being incentivised to recruit additional participants through commission-based rewards. By recruiting others around him to invest in the app, the victim became an accessory to the fraud, which inhibited him from reporting it to the police and other authorities. The structure closely resembled a multi-level marketing scheme, where early gains encouraged continued participation until victims had invested substantial amounts.

The apps were gamified, which kept the participants hooked for constant *"rewards"*. Further, withdrawing from the scheme before completing a cycle would result in the loss of all invested funds, creating pressure to continue investing despite growing suspicions. Even the withdrawal of existing amounts required investments, which kept increasing progressively. The operators also maintained anonymity by frequently changing payment links and avoiding identifiable contact details.

The recruitment of victims to further perpetuate the cycle of crimes, whether knowingly or unknowingly (as in the case mentioned above), happens across different types of cybercrime categories. A cybercrime expert gave an example of a location between Thailand and Myanmar, known as KK Park, which has become an international cybercrime hub. Most of the people who work in these scam *"call centres"* are, in fact, themselves fraud and trafficking victims who are then kept in inhumane conditions, tortured and forced to work there in these scam operations. In a recent raid, 1300 people were rescued from these centres, of which about 250 were Indians.

1.1.4 Identity-based targeting

Various other types of cybercrimes, such as cyberbullying, also function in a similarly organised setup, though with different agendas and outcomes. The interviews indicate that cyberbullying was often organised rather than spontaneous, and transcended not just jurisdictions but also various other categories of crimes, such as stalking, doxing[ii], criminal intimidation, etc. The victims described coordinated networks operating multiple fake social media accounts to target individuals, particularly Muslim women who were in inter-faith relationships. A network, running by the handle *"Bhagwa Love Trap",* worked to *"expose"* such women by posting their private pictures and videos online without their consent, with captions and abusive messages. While some of these photos/videos were taken from their personal social media handles, others were recorded by persons associated with this network, without the knowledge or consent of the victims. It must be mentioned that in the course of this study we came across only one such group. However, we are not aware if similar vigilante groups are operating on 'behalf' of other communities as well.

One of the victims, a Delhi-based journalist, was informed by the police that these networks functioned across jurisdictions, with perpetrators believed to be operating from outside India. A sting operation conducted by the victim and her colleagues for a news report found that the network relied on multiple *"sleeper cells"* operating across various locations, where members associated with the network would provide on-ground information by following the women, recording videos and photos without consent, acquiring their personal information, and passing on this information to the people running the social media handles. As in this case, they also target other family members or close associates of the victims based on the information received from the sleeper cells. What began as a cyberbullying case against a Muslim woman who, at the time, was dating a Sikh man, eventually also targeted her elder sister and her mother.

In cases of Non-Consensual Intimate Image (NCII) abuse, such as revenge porn, morphed images and deepfakes, in most cases the perpetrator is someone known to the victim. As explained by an expert who works on online gender-based violence, usually women between the ages of 18 and 35 years are targeted by a former or current intimate partner. There are, however, increasing cases involving minors and older women, as well as professional women with public visibility, like journalists and politicians, activists and content creators. These images/videos, once uploaded on the internet, spread across various platforms and are hard to track or take down.

Across cybercrime categories, a common pattern emerges: perpetrators combined social engineering with careful exploitation of institutional authority, digital platforms and payment systems. Rather than relying

primarily on advanced technical hacking, most incidents relied on manipulating victims' emotions, exploiting procedural weaknesses and maintaining anonymity through digital infrastructures. The FGD with experts corroborated these findings, emphasising that contemporary cybercrime increasingly depends on psychological persuasion, organised criminal networks and the strategic misuse of legitimate communication technologies.

1.2 Reporting of Cybercrimes to Different Authorities

1.2.1 Non-reporting and underreporting: Factors & trends

Reporting of cybercrimes to different authorities depends on various factors, some of which came out during the interviews. A victim of a betting app fraud, who lost about Rs. 2.5 lakhs, did not report the case to the police or any other authority since he had invited his friends and relatives to invest in the app, unaware that it was a fraud. He was afraid that he would also be implicated if he reached out to the authorities. He said that at least three more people who had fallen victim to the scam had also not reported their cases and that many such cases go unreported. He was also of the view that the police lack training and awareness about such crimes and wouldn't be able to help, which further inhibited him and others from reporting their cases.

A cybercrime expert further corroborated this, stating that the official data on financial cybercrimes is actually just a fraction of overall cases that are actually occurring. The official figure of money lost due to cybercrimes, as reported by the National Crime Records Bureau (NCRB) was about Rs. 22,000 crores in the previous year, but in his estimate the actual scale of the loss would be closer to Rs. 1,00,000 crores.

Cybercrime experts noted that underreporting is significantly more common in cases of non-financial cybercrimes, even though they are more pervasive. Cases of defamation, sextortion, impersonation, cyberbullying and non-consensual intimate image (NCII) abuse are very rarely reported because of the reputational harm to the victim, the anonymity of the perpetrator and lack of adequate redressal. While recognising the difficulties faced by women in the reporting of online sexual crimes, an expert noted even the male victims of sextortion are apprehensive about coming forward due to fear of being shamed and ridiculed.

A journalist who has covered the issue extensively and has done ground reporting of interviews with perpetrators believed that sextortion is one of the most common cybercrime cases, though they are rarely reported. The shock of the crime and the fear of public embarrassment inhibit most victims from reporting these cases. Many victims have attempted suicide because of these crimes. He notes that there is a need for public awareness about such crimes.

1.2.2 Reporting of online gender-based violence and child sexual abuse

For women, in many cases, the crimes are so normalised that the victims do not report the cases at all, for the fear of not being taken seriously. An expert on online gender-based violence recounted an incident where more than 600 women from Mumbai reported cyber flashing, wherein women got unsolicited video calls from unknown numbers with explicit content. As isolated incidents, women were wary of reporting these cases because the police blamed them for answering video calls from unknown numbers. But when it started happening to multiple women from the same localities, many more victims came forward, and police took cognizance of the cases, and with assistance from the cyber profiling expert, they were able to narrow down the suspect.

In cases of cyberbullying and non-consensual intimate image (NCII) abuse, one of the victim's primary concerns is to take down the offensive content from online platforms and get the

accounts circulating the content deactivated. To do so, social media platforms play an important role. However, as shared by a cyberbullying victim, these platforms are often not very responsive to such complaints. On popular social media platforms such as Instagram or Facebook, the victims have to complain multiple times from multiple accounts to get an account deactivated. And being an organised group, numerous such accounts are targeting the victim. Even after one gets taken down, many other new accounts replace them and continue to target the victims.

It becomes even more difficult to get offensive media taken down from the platforms and block troll accounts. A cyberbullying victim shared, *"As laypersons, we cannot do anything. The videos will not be removed... When we block one account, they create a hundred more accounts. How can we keep blocking so many accounts?"* [Translated from original in Hindi]

Experts who work with victims of cyberbullying and NCII also noted that platforms are not very responsive, and the responsiveness varies by platform. Adequate internal guardrails against online gender-based violence are missing in a majority of the social media platforms. One expert cited a study by the Internet Freedom Foundation which found that the response of social media platforms to misogynistic hate speech is 'very poor'.[iii] Victims need to provide evidence for reporting to the platforms, but despite the evidence, the platform responses remain inadequate.

Inhibitions against reporting to law enforcement agencies become even more pronounced in cases involving minors. An expert noted that cases of cyber-grooming and cyberbullying involving minors are much less likely to be reported, as the parents do not want to put their children through the psychological toll of the police reporting process. Another expert, who works on online gender-based violence, pointed out the difficulties that minors face while reporting non-consensual intimate image abuse. Not only are the police attitudes rude, dismissive and conservative, but the fact that minors are required to be accompanied by a parent or caregiver inhibits them from reporting accurate details of the case because of the shame associated with it.

1.2.3 Reporting cases on the cybercrime portal and cybercrime helpline

In 2020, the Indian Cybercrime Coordination Centre (I4C) officially launched the National Cybercrime Reporting Portal (NCRP)[iv] to ease the process of reporting all forms of cybercrimes. This, along with the helpline number 1930, was envisaged as an integrated reporting portal for all types of cybercrimes occurring anywhere across the country, through which all relevant authorities such as banks, law enforcement agencies, RBI, etc. can work in tandem on cases of financial and non-financial cybercrimes.

However, victims who have reported the cases on the portal and helpline number have mixed opinions on the ease of use of these forums. The victims who pursued their cases reported that the domain or the helpline number does not act as a one-stop avenue for reporting cases, from where the case will automatically be transferred to the relevant authorities. Instead, the victims are expected to take three different steps for reporting: make the call on the helpline number, register a complaint on the online portal, and visit the cybercrime police station of their jurisdiction.

Further, many victims did not find the portal easy to navigate. An expert noted that the portal is not very user-friendly, and many victims, particularly those with language barriers, face difficulty navigating the portal. However, she highlighted the importance of reporting the cases, particularly those of non-financial cybercrimes, for better official statistics even if the victims choose not to pursue the case legally. Thus, when victims are unable to complain, the expert's organisation steps in and hand-holds the victim through the reporting process.

In almost all of the interviews where victims reported complaining on the portal, they had to take assistance from a friend, family member or

an acquaintance to fill out the online form. As recounted by one of the victims of a financial fraud, *"I filled in the form on the* [cybercrime] *portal. And I can tell you that it is not easy. It is not user-friendly at all...It was a nightmare filling that form."*

Victims also do not have clarity on the steps that should be taken by law enforcement after a complaint has been made on the portal. Of the 16 victims of cybercrimes that were interviewed, about half (9) reported their case using the online portal or the centralised helpline number. While a majority of these victims got a call back after complaining online, in at least four of these cases, the victims did not receive any call back or update on their cases even after months, and in some cases, years, and are unaware of the status of their cases. In two cases, the victims also visited the cyber police unit multiple times after the online complaint, but their cases never progressed. Even amongst those who received a call back after the online complaint, further action was taken by the police only in two cases where the respondent physically visited the cybercrime police station and pursued the case with the help of others in their network.

As recalled by a victim of hacking from Chennai, after filing the online complaint, he immediately got an acknowledgement mail. After two days, he received a call from the local cybercrime unit asking about the details of his case. The police officer advised him not to click on any suspicious links and to keep changing his passwords, and after that, there was no further communication from the police.

An investigating officer (IO) from a cybercrime police station in Delhi informed the research team that of the approximately 15,000 cybercrime complaints registered in their jurisdiction in the previous year, just about 250 cases were converted into FIRs. He highlighted the lack of human resources and the non-investigative load on IOs as the primary reasons for the low conversion rate. Each IO, according to him, has a workload of about 500 cases for investigation.

1.3 Case Outcomes

1.3.1 Outcome of digital arrest cases

Amongst the three digital arrest victims, only one suffered an actual financial loss, while the other two were able to avert the transfer of money altogether because of intervention from someone outside the formal redressal system.

Sanjeeb lost over Rs. 65 lakhs to the fraudsters before recognising the fraud. An FIR was registered immediately, but the victim was only able to recover Rs. 5 lakhs. A court order for the return of Rs. 22 lakhs was passed in his favour, but its release is still pending as the bank works through a queue of other defrauded customers awaiting reimbursement. Police reportedly arrested 11-12 mule account holders linked to the racket, but the victim's case did not progress beyond that.

In the other two cases, the fraud was interrupted through informal interventions from friends of the victims before any money changed hands. Both interventions came right before the transfer of money when the victims had already gone through the ordeal of breaking their structured investments and collating all their money to be later transferred to the fraudster. Once formally reported, however, both cases received only cursory institutional attention. One victim assumed the police would not act on a case where no money had actually been lost, and did not follow up by himself. The police also did not update him about the case until it was closed, and the closure was the only communication to the victim seven months later. The victim felt strongly about *"the lack of policing"*. The other victim fared similarly, where the bank confirmed that no funds had left the account, and the police did not follow up again after the complaint was lodged on the cybercrime portal.

1.3.2 Outcome of other financial fraud cases

Amongst the ten financial fraud victims, three approached the police, the bank, and the court for redressal; five approached the police and

their bank, one approached only the bank, and one did not pursue any method of redressal.

Of the nine respondents who lost money through financial frauds (other than digital arrest) and complained to the police or the banks, five were able to recover a partial amount at either the bank level, or through court or RBI orders, and one was able to recover the full amount through their bank.

Marie was defrauded for about Rs. 2 lakhs while her account was dormant for several months and found the police indifferent to her case, remarking that they *"got much more pressing issues for them to take care of…so I don't think they were able to, you know, concentrate on this and proceed with it"*. Her relationship with the bank fared no better, and she rated her satisfaction as 0 out of 5 with the bank. The RBI Ombudsman never responded to her complaint. She was able to recover Rs. 1 lakh before going to the court but was ultimately unsuccessful in recovering the rest of her money through the court.

A victim who lost about Rs. 20 lakhs across two accounts approached the bank, then the police, then the RBI Ombudsman once recovery stalled, and finally the court. Favourable orders were received from the court and the RBI Ombudsman in this case. The court secured recovery on one account and the Ombudsman on the other, returning around Rs. 18 lakhs of the total loss.

Another victim lost a little over Rs. 14 lakhs, and his bank refused to register a complaint until an FIR was filed. Once the FIR was filed the banks shifted the onus of the fraud onto the victim and tried to absolve themselves of any responsibility to act. Thirty days passed without any action from the bank, which prompted the victim to approach the RBI Ombudsman. Recovery only began after a magistrate's order compelled it, and a consumer court claim for the remaining Rs. 4.9 lakhs was still pending at the time of the interview.

In line with our findings from the survey (**Chapter 5**), three of the victims were able to harness their personal connections to sustain momentum and aid better recovery in their cases. While another victim, who had no equivalent access, recovered only half her loss through a process she described as long, arduous, and physically and mentally taxing.

Victims who were able to recover even a partial amount reported having to follow up extensively with the institutions involved. A retired NRI victim who lost over 14 lakhs, stayed back in the country for several months following the incident so that he could closely follow up the investigation. He managed to recover a little over 9 lakhs, while the recovery of the remaining amount is pending.

For victims who had lost relatively smaller amounts, which, however, formed a significant portion of their income, the outcomes were less than satisfactory. Two victims who lost Rs. 25,000 and Rs. 19,000, respectively, encountered a more uniform indifference. Neither of them has recovered any money so far.

Read together, the financial fraud outcomes suggest that formal escalation, such as filing an FIR, approaching the Ombudsman, or going to court, did not reliably determine whether there was a chance to recover the money. What varied more consistently was the victim's own leverage, either through a personal contact in a position of authority or a valued banking relationship.

1.3.3 Outcome of cyberbullying

Both victims interviewed here were Muslim women who underwent prolonged online gender-based violence and were targeted because of their religion and gender. We tried contacting similar victims from other communities but were not successful in that due to the sensitivity involved.

Both victims had to endure a targeted campaign of hate where they were stalked and abused on their social media accounts, and such abuse even extended to their other family members. They would take the help of their friends and other social connections to get an account reported and banned, but there was not much action that could be taken by the social media platform to mitigate the abuse, as the perpetrator would just create a new

account and continue the abuse. They note that some accounts which were reported kept reappearing, as Instagram (as reported by the victim) does not permanently ban an account but rather places a time-bound restriction on it. *Nadiyah* felt that social media platforms should take on more responsibility to prevent online gender-based violence, and it should not be as easy as this case to take someone's videos and photos and circulate them online to monger hate. Another victim noted the caveat with social media content guidelines: that even after reporting, the photos and videos would not be taken down – the reason being that they do not contravene the platform's policies.

The victims reported the case to the police and the offensive content was taken down. The police also actively followed up with the victim, but ultimately the scale of the abuse was reported by the victim as too much for the police to handle as well. It felt like a racket and that there were *"too many IDs"*.

In contrast to the financial fraud and digital arrest cases, which were largely defined by whether money was recovered, the cyberbullying cases point to a different measure of outcome altogether: personal safety and the ability to resume ordinary life. On that measure, neither case got resolved. Even sustained police engagement, an exception against this study's broader institutional pattern, could not fully contain harassment that was distributed across multiple platforms, replicated through new accounts, and, in both cases, based outside Indian jurisdiction altogether. The social media platforms involved emerge here as a redressal actor distinct in kind from the police, courts and banks discussed so far. One whose content-moderation policies, rather than any lack of institutional will, structurally permitted the abuse to continue.

1.4 Impact of Cybercrimes: Mental, Financial and Social

In 2013, *Marie,* a resident of Chennai, was on bed rest due to her pregnancy. On complaining about the fraud to the police, she was asked by them to visit the police station in person several times. She also acted as a liaison between the police and the bank. During an unsuccessful investigation by the police and a long-winded court case that followed, *Marie* had a miscarriage.

"More than the financial burden, it was the mental trauma and the physical trauma that we had to undergo. Right now I cannot even think about it because there's so much that we underwent... I was already on bed rest and that itself was a lot of stress. But ultimately, I lost my child also", Marie shared.

Marie's loss was incomparable; the stress and trauma caused by the loss of money and the gruelling complaint and recovery process that followed were echoed by many other victims more than a decade later. For a then-minor victim of sextortion, the trauma stems not only from the cybercrime incident, but also from the police's rude behaviour towards him and his family.

Several victims of financial fraud reported undergoing depression for months following the cybercrime incident. The *"mental shock"* and *"trauma"* following the incident were more than the monetary loss alone. The *"stigma and embarrassment"* from being defrauded led several victims to lose their confidence and financial autonomy. A 75-year-old victim from Delhi stopped using online banking systems entirely following the cybercrime and now relies on her adult children to withdraw cash, which she uses for her daily transactions.

The loss of significant amounts of money, in one case a victim's entire life savings, also caused major financial, mental and social repercussions. As a retired person, he does not even have the option of earning the money again. He describes himself as a "*living dead person,* [whose] *body is working but the mind has totally shut down*".

In the case of a victim who inadvertently introduced others to the fraudulent app, his personal financial loss is overshadowed by the overwhelming social and emotional distress due to the losses suffered by others and the fear for his safety. He is constantly being threatened with legal action and went into *"depression and trauma"*.

The cyberbullying victims interviewed in this study faced lasting reputational, professional and mental harms due to their targeting. One of the victims, a former social media influencer, had to change her profession and moved abroad following the incident. The fear of being recognised and targeted again is carried by her several months after the incident, and she remains wary of strangers looking at her or trying to approach her. Distant family members and acquaintances reached out to the victim's family, questioning her character. Both the victims reported suffering intense social and psychological distress following the incident.

1.5 Cybercrime Perpetrators: Accounts of Families of Accused

This research includes interviews with family members of two persons who have been accused in separate cases of cybercrimes. There is another category of respondents included in this study, who are neither perpetrators nor victims of cybercrimes, but have nonetheless been impacted by it. These are persons whose bank accounts have been frozen, allegedly due to ongoing cybercrime investigations, though the account-holders are unaware of which case they are linked to. A common thread across all these interviews suggests that these are persons whose bank accounts have allegedly been used as "mule accounts" for cybercrimes.

Understanding the operation of mule accounts is essential to examining the wider ecosystem of cyber financial fraud. Fraudsters use mule accounts to conceal the movement of stolen funds, complicating investigation and recovery efforts. This section explores the experiences of individuals whose bank accounts were allegedly used for this purpose.

The RBI defines 'Money Mules' (mule account holders) as third parties that are recruited by fraudsters to gain illegal access to deposit accounts. These third parties may be innocent, while in others they may be colluding with the criminals (RBI, 2014). Routing the defrauded money through a mule account shields the fraudster from leaving traces of their own identity, impedes the traceability of the money and causes jurisdictional problems for investigating officers.

Jamal, a small business owner, was approached by a bank employee shortly after obtaining a GST number for his business and offered a low-interest loan on the condition that his account show a pattern of high-value transactions. The same employee volunteered to arrange these transactions, persuading *Jamal* to share OTPs for transfers moving through his account. He was later arrested following a police notice and spent 58 days in jail before securing bail. In the meantime, his business came to a standstill, and his family faced financial strain, on top of the emotional and social strain of his detention. His uncle, the interview respondent, had to travel from Uttar Pradesh to Delhi for repeated hearings.

Zakir was 18 when a co-worker persuaded him to open a mule account, handing over his SIM card in exchange for a promised Rs. 5,000 *"now and then."* He too was arrested, has now remained in jail for four months and has been denied bail twice. His mother reports him injured and struggling to walk while in custody and describes waiting in court in the hope of securing his release. The co-worker who recruited him was, by her account, neither questioned nor arrested.

In both cases, the money mules were deceived into operating as one and had to bear the full weight of the criminal justice system, with the actual criminal not even being questioned or investigated in one of the cases. Both these cases point towards the system targeting the most visible and replaceable link in the chain while the recruiter, the organiser, or the mastermind behind the scheme goes untouched.

Another respondent's case illustrates the same problem but from a different angle. Someone who had done nothing wrong knowingly, nor had any contact with a recruiter/fraudster. When he attempted to withdraw money from his account for his wife's urgent medical care, he realised that his entire money had been frozen, with an additional Rs. 17,000 shown as

a *"negative balance in lien"*. The bank's only information was that the funds were tied to a series of complaints, and its only guidance was procedural — visit the cybercrime cell, obtain the recipient bank's location from them, then secure a no-objection letter from that bank before the freeze could be lifted. Being a delivery driver, his work was impacted in the pursuit of redressal, leading to financial loss, compounding a period already strained by his spouse's illness.

Two other cases, whose money in their bank accounts was put *"in lien"*, allegedly due to ongoing investigations, follow a similar pattern, with the account holders running between banks and the police, without getting sufficient answers or recourse. One such person was himself a victim of a digital fraud, but instead of being able to recover his lost money, the police mistakenly froze more money from his account. All three respondents whose bank accounts were frozen and the two accused persons were Muslim. Both the accused were in prison at the time of the interviews. The interviews were conducted with their family members outside court premises.

Across all cases, the redressal machinery responded to the account and its holder rather than the person orchestrating the crime. How the person came to be implicated seems to have made little difference to the institutions, and the burden of proving their innocence and working with the system fell entirely on the individual and his family, rather than the one who had schemed the operation.

1.6 Conclusion

This chapter highlights how cybercrimes are not simply a problem of technological vulnerability but one that exploits trust, fear, social relationships and institutional weaknesses. Across different forms of cybercrimes, perpetrators increasingly operate through organised networks that combine social engineering, access to personal data, digital platforms and financial infrastructures, while victims are often left to navigate fragmented and difficult systems of redressal.

The findings show that reporting does not always result in meaningful institutional action and that recovery or resolution is frequently dependent on a victim's ability to persist, mobilise personal connections, or gain institutional leverage. Victims of non-financial cybercrimes face even greater barriers, with stigma, fear, inadequate platform responses, and the difficulty of containing abuse that can be replicated across jurisdictions limiting both reporting and redressal.

The experiences of accused individuals and those whose accounts have been frozen highlight the consequences of a system that can respond to the most visible or accessible link in a criminal network while failing to reach those who organise or profit from it. Cybercrime, therefore, needs to be understood not only through the scale of financial losses or number of complaints but also through the human and institutional costs it produces. A meaningful response necessitates that institutions become more accessible, coordinated, and accountable, while also acknowledging that effective cybercrime prevention and redressal must address the social, psychological, and organisational dimensions of these crimes, in addition to their technological infrastructure.

Endnotes

i The RBI defines 'Money Mules' (mule account holders) as third parties that are recruited by fraudsters to gain illegal access to deposit accounts. These third parties may be innocent, while in others they may be colluding with the criminals (RBI, 2014).

ii Doxing is the act of exposing private or identifying information on the internet about an individual or group without the person's or group's consent, usually with malicious intent. Source: https://www.britannica.com/topic/doxing

iii Internet Freedom Foundation. (2024, February 1). *Letting hate flourish: YouTube and Koo's lax response to the reporting of hate speech against women in India and the US*. https://internetfreedom.in/report-misogynistic-hate-speech/

iv National Cyber Crime Reporting Portal. www.cybercrime.gov.in

References

- Hadnagy, C. (2011). Social engineering: The art of human hacking. Wiley.
- Menon, S. (2023, November 23). Bhagwa love trap: A new Indian online trend causing real-world harm. BBC. https://www.bbc.com/news/world-asia-india-67101250
- Reserve Bank of India. (2014, July 1). *Master circular on customer service*. https://rbidocs.rbi.org.in/rdocs/notification/PDFs/70MK010714FL.PDF

CHAPTER

02

Maharashtra Cyber Security Command Centre (Navi Mumbai, Maharashtra- October 11, 2024).

Photo by Maharashtra Cyber Police.

Institutional Response and Experiences

Key Findings

- Most of the victims who visited cyber police stations or units felt that the staff was polite and helpful. However, with victims from poor backgrounds, the police were reportedly rude, dismissive and abusive.
- FIRs are not commonly registered in cybercrime cases. Of the 15 victims who complained to the police either online or in person, an FIR was registered in six cases. Two of these were automatic FIRs, and in at least two other cases, the victims reached out to persons of influence to get the FIR registered.
- In most cases, the victims had no information about any investigation into the crime being done by the police. The police often cited jurisdiction problems and lack of coordination between state police departments as the primary deterrents against conclusive investigations.
- In cases of online gender-based violence, experts highlighted the police apathy towards such crimes and their tendency to blame the victims. The focus of the police is often on "*settling*" the cases, urging victims to come to a compromise with the perpetrators.
- Victims of financial cybercrimes and experts overwhelmingly felt that the banks refused to take accountability, or assist the victim through the recovery process. Barring one case, in all other interviews with financial fraud victims, the banks maintained that the victims *"collaborated"* with the fraudster.
- Amongst the ten respondents who rated their experience with the police, the average rating given to the police was 2.4 out of five. Amongst the six victims who rated their experience with the banks, the overall rating was a poor one out of five.

Institutional Response and Experiences

This chapter examines the institutional response to cybercrime, focusing on victims' experiences with the police, banks, courts and other legal services, as well as the informal and semi-formal support structures available to them. Alongside the police, particular attention is also given to the role of the banking sector, including both public and private banks and oversight mechanisms such as the RBI Ombudsman, given its central role in responding to financial cybercrimes.

While the previous chapter highlighted victims' experiences with cybercrimes, the reporting process and the impact of the crime and the investigation, this chapter examines the role of the police, the banks and other authorities. It also includes victims' experiences and satisfaction with the responses they received. The chapter concludes with recommendations and policy suggestions drawn from the experiences and perspectives of both victims and experts.

As in **Chapter 1**, the findings in this chapter are also drawn from qualitative interviews with 37 respondents. These include 16 in-depth interviews with cybercrime victims, interviews with two close family members who assisted victims, 10 in-depth interviews with cybercrime experts and a focus group discussion (FGD) with five cybercrime experts and police officers. Family members of two persons accused of cybercrimes in separate cases and two other respondents whose bank accounts had been frozen due to on-going cybercrime investigations were also interviewed. The detailed methodology for these interviews is provided in **Appendix 4.**

To protect the anonymity and confidentiality of respondents, all names have been changed. Domain experts and professionals have been identified with their professional identities.

2.1 Police Responses to Cybercrimes

2.1.1 First-contact with the police

Of the 16 victims of cybercrimes interviewed for this study, 10 of them had visited the relevant police stations/units. Many of the victims reported visiting the cyber police stations multiple times. Particularly, those who visited cyber police stations or units largely recalled the staff as being polite and helpful. Many victims were also sympathetic towards the police, considering the volume of cases that they have to handle with strained resources.

Victims noted the stark difference between their previous interactions with the regular police compared to the behaviour of the staff at cyber police stations. As one victim described, *"Usually what happens if you go to a normal police station, these cops, a hundred percent, they are not cooperative. They are abusive. They misguide you, and they mislead you. They give dodgy answers…But this was very unusual, how these people* [the cyber police station staff] *helped me. I could not believe it at first."*

There was, however, a noteworthy difference in the attitude of the cyber police staff towards the complainants from a lower socio-economic stratum compared to the more elite, English-speaking complainants. Two victims pointed out the dismissive and rude attitude of the police towards other complainants who were evidently from a poor background and had lost smaller amounts of money. One of the victims, a son of a domestic worker from Noida, talked about the police's rudeness towards him and his family when they went to file a complaint against sextortion. He noted that the police would only talk to his mother's employers who were accompanying him and not to him directly

as the complainant. Instead, they asked him, *"Tu kaun hai? Tujhe kyun lekar aaye hein?* [Who are you? Why do they get you here?]" The police refused to believe that he was at that time a minor (16 years of age), called him a liar and blamed him for the crime. At the local police station that they went to before being redirected to the cyber police station, he claimed that the police were abusive towards him and his family. The police were extremely uncooperative and finally registered an FIR on the fourth visit, after a lot of pressure from his mother's employers.

As for bribes sought by the police, only one digital arrest victim suspected that the police-appointed lawyer and the police pocketed Rs. 55,000 paid by him for a court order towards partial release of the lost money. Rest of the victims did not report having to pay any bribe to the police.

2.1.2 Registration of FIRs

Despite the relatively positive police attitudes in most cases, several victims reported lack of clarity on what type of complaint had been registered by the police, whether an FIR was registered, and the process of the complaint and investigation. On being asked why her complaint was not converted into an FIR despite multiple visits to the police station, a victim stated, *"You know how the police are. They don't give us reasons"*. Similar sentiments were echoed by many victims, with some not even being told if the FIR had been registered at all or given any updates on their case.

One of the victims highlighted the lack of coordination between different police departments. *Kamala,* a 90-year-old retired professor, found out late one evening that about Rs. 11 lakhs had been debited from her account. With the help of her relatives, she called her bank and the cybercrime helpline number. She visited the cyber police station the next day, but they did not have any records of a case with her acknowledgement number. She was asked to file another complaint on the cybercrime portal, which she did with the help of an accompanying relative. Soon, she received a call from the regional cyber department, asking if she had made the same complaint twice. She explained that the staff at the police station asked her to do so, but the officer continued to berate her. An FIR was filed only during the second visit, after she had approached a top police official through her personal network.

Many others, however, failed to even get an FIR registered. Of the 15 victims who complained to the police either online or in person, an FIR was registered in six cases. Two of these were automatic FIRs because the e-Zero FIR initiative mandates automatic conversion of all financial cybercrime complaints to FIRs in Delhi for crimes above the threshold limit of Rs. 10 lakhs.[i] In at least two other cases from outside Delhi, the victims reached out to persons of influence to get the FIR registered.

2.1.3 Investigation of cybercrime cases by the police

Even after the registration of FIRs, for most victims the contact with the police was limited to tracing the money lost due to the financial fraud or taking the offensive content and accounts down in cases of cyberbullying. Rarely were the victims privy to any criminal investigation of the fraud or cybercrime. In one case of digital arrest in Kolkata, the victim claimed that the police had arrested several mule account holders. In another case of financial fraud from Faridabad, the victim took assistance from his contacts at the bank to trace the mule accounts into which the money had been transferred and gave the details to the police. Due to the alleged inaction of the police, he approached the consumer forum and banking Ombudsman and was able to get a partial refund after more than three years of the incident.

In most other cases, however, the victims had no information about any investigation into the crime being done by the police. The police often cited jurisdiction problems and lack of coordination between state police departments as the primary deterrents against conclusive investigations. Upon enquiring, a victim from Delhi got this response from a staff member at a cyber-police station: *"Ma'am, how can I trace*

these people? [The money] *is probably divided up among three or four people. These people—one may be in Muzaffarpur, one may be in Myanmar, and one may be in China. I can't help you with that."*

A victim of cyberbullying elaborated on her disappointment at the lack of criminal investigation by the police: *"We wanted the police to arrest the perpetrators, which was not done… Because the police has not been able to arrest them, they are still doing the same thing. Girls are continuing to become their targets"* [translated from Hindi]. Over a period of six months, the police assisted the victim in taking down the offensive accounts. However, on independent verification by the research team, we found that several pages titled *"Bhagwa Love Trap"* (of which the respondent was a victim) or related names are active on popular social media platforms and continue to target Muslim women in inter-faith relationships.

2.1.4 Visits to the police station

Several victims recounted having to visit the cyber police station many times for follow-ups on their case but were not always successful in getting a satisfactory response or outcome. As recounted by *Ahmed,* who lost Rs. 19,000 - a significant portion of his income as a small shop owner in Delhi - he visited the cyber police station 7-8 times, but without any resolution. Instead, the police mistakenly seized his account and blocked Rs. 19,000 more from his account. An acquaintance of the victim, who is a journalist, had to intervene and reach out to higher authorities to get the seized amount unblocked.

2.1.5 Lack of coordination between the banks and the police

Victims of financial cybercrimes overwhelmingly felt that there was a lack of proper communication and coordination between the banks and the police. Several victims reported having to act as a liaison between the banks and the police and pass on relevant information from one institution to the other for timely action on their cases.

The process was even more complicated in cases where the fraudsters transferred the amount to a cloud bank. As one victim recalled, the police were trying to get in touch with a cloud bank where part of the money was transferred, but did not have any information about the concerned authorities from the bank whom they could contact.

2.1.6 Responses to online gender-based violence

In cases of online gender-based violence, experts who have been working with such victims highlighted the police's apathy towards such crimes and their tendency to blame the victims. The focus of the police is often on "*settling*" the cases, urging victims to come to a compromise with the perpetrators. On the other hand, they also noted the lack of coordination between the police and the social media platforms. One of the experts said that the police often rely on NGOs that work on online gender-based violence to get offensive content removed from the internet. She stated, *"…we would like to be of aid to the police more, but not in such a haphazard, incomprehensible manner where no standard operating procedures are made clear."* She mentioned the lack of effective training, lack of human resources and the absence of dedicated staff working on such issues as some of the reasons for poor police responses.

Overall, while many of the respondents felt that the police were cooperative and polite, most respondents felt that the action taken by the police in their case was inadequate. Respondents were sceptical of the police's competency to deal with cybercrime cases. Victims who went through the drawn-out process of recovering their money felt that the police were *"not competent enough to be able to deal with these cases"*. Several victims were left with a sense that the police are constantly dealing with more important cases and that their cases were not as important. As stated by a hacking victim, *"I'm not their priority, right?"*.

Amongst the ten respondents who rated their experience with the police, the average rating given to the police was 2.4 out of five.

2.2 Bank Responses to Cybercrimes

2.2.1 Shifting liability and weak security systems

As an institution, banks play a central role in both the execution of financial cybercrime as well as the redressal of it. Yet, as evidenced by the interviews with victims and experts, the response from this institution leaves much to be desired. Barring one case, in all other cases of financial frauds that were interviewed in this study, the banks maintained that the victims *"collaborated"* with the fraudster even in cases where there is no evidence of negligence on the part of the victim. An expert shared that banks have a standard reply with different variations, all essentially shifting the entire liability of the fraud to the victim. Notably, the case in which the banking officials proactively assisted the victim through the recovery process without a court order was that of a high net-worth individual who had a long-standing relationship with the bank. In most other cases, victims were of the opinion that the banks were unwilling to take any responsibility or action to redress the cybercrime incident.

The banking guidelines, on the other hand, specify that banks should be liable for a loss incurred due to a third-party breach. As per a 2017 RBI guideline, when a customer loses money due to a third-party breach where the deficiency lies neither with the bank nor with the customer, and the customer notifies the bank within three working days, s/he is entitled to zero liability, and the loss must be borne by the bank (RBI, 2017). This guideline was further extended in 2026 on a pilot basis to entitle those victims who have been tricked or coerced into a fraudulent scam payment to limited liability (*The Hindu,* 2026). The ground reality, however, suggests minimal accountability by the banks, even in cases of third-party breaches where the victim has not shared any information, knowingly or unknowingly, with the fraudsters. In one of the cases, the victim had not made any financial transactions for several months and had neither clicked on any links nor shared information with a caller. Yet, the bank insisted that the customer was liable for the fraud, as in many other cases.

As experts point out, the banks have a higher liability in many such cases because of weak security systems and frequent data leakages. Even in cases where the victim may have unwittingly shared some information with a fraudster, if the perpetrators are already aware of the banking details of the victim before the fraud, such as account number, name of the bank in which the victim has an account, etc., it suggests loopholes in the banking systems for which the institution should be held responsible. Most digital transactions require multi-factor authentication, which is now also mandated by the RBI rules (RBI, 2025). Even in cases where the victim has, under threat or coercion, shared one layer of authentication, the second layer of authentication is often breached at the level of the banks, despite the fact that they have the resources to build more secure infrastructure.

Banks often have sufficient training and technical know-how to be able to prevent financial cybercrimes to a great extent but often evade responsibility for this, as was highlighted by the law enforcement, cybersecurity and banking experts during the FGD. They stressed the need for mandatory accountability and criminal action against bank officials who fail to comply. An expert cited the example of the United Kingdom, which recently passed a law making banks fully liable for frauds up to £85,000 and requiring them to reimburse the victims for digital frauds within five days. Following this, banks in the UK have proactively started safeguarding their technical infrastructure.

2.2.2 Delays in bank response

Vipin, a journalist based in Gurgaon, got a call from Airtel on a Saturday asking if he wanted his SIM to be upgraded. When he refused, the caller shared some of his personal information, including his name, date of birth, and Aadhaar card number as well as his debit card number.

The next day, he lost Rs. 5,000. He immediately blocked his number and emailed his bank, since it was closed on Sunday. However, by the time he reached the bank physically the following day, his account had still not been blocked, and the fraudsters had taken a loan of Rs. 5 lakhs against his credit card, half of which they had already withdrawn. The bank, however, took *"zero accountability"* for this loss and was *"apathetic"* to the complaint. He has not recovered any of the money lost, and his case is being investigated by the police.

Vipin's case is not an isolated one. Another victim stated that more money had been withdrawn even after they had apprised the bank of the fraud. In another case, the victim's Fixed Deposit (FD) was withdrawn without her consent on a Sunday, and even though the money was deducted on the same day, the *"slip"* showed the date as the following Monday. Several other victims mentioned that the fraudsters already had their personal banking details, which led them to trust the caller.

The above cases suggest negligence on the part of the bank, causing further financial loss to the victims. A digital arrest victim also pointed out the failure of the banks to alert the victims of possible frauds. When he went to the bank to withdraw his high-value FDs, the bank staff did not say anything to him, even though they seemed suspicious. He echoed the opinions of other experts, stating that banks have a bigger role in making the customer aware of frauds such as digital arrests. If any banking staff step in at such times to inform the victims about digital arrests and similar frauds, such cases can be prevented.

2.2.3 Bank complicity

The lapses in banking response, the lack of security regarding personal banking information and the specific targeting of vulnerable accounts led several victims to believe that the banks' officials, whether directly or indirectly, were complicit in the cybercrime. Five of the financial cybercrime victims held this opinion. A few others also pointed to the lack of vigilance by the banks when, for instance, *"big-ticket amounts are being transferred to suspicious current accounts with fishy names"*. One of the victims was told by the investigating police officer in her case that the bank must be complicit, though no action was taken against them because of lack of evidence.

The interviewed cybercrime experts, retired and serving police officers, were also strongly of this opinion. On the one hand, they pointed out the common data leaks in the banks which are not sufficiently addressed—both due to inadequate security systems and the direct complicity of some banking officials. Secondly, the banking institutions enable the cybercrime infrastructure by their failure to do due diligence in the opening of bank accounts and lax KYC processes. *"People like you and me will lose access to our accounts due to KYC procedures, but these accounts* [the cyber criminals'] *will never be closed",* stated a former police officer. While focusing simply on the opening of new accounts, banks are failing to take necessary preventive measures against financial cybercrimes.

2.2.4 Responses from RBI Ombudsman and satisfaction with the banking experience

Five of the interviewed victims of financial cybercrimes escalated their cases to the level of the RBI Integrated Ombudsman Scheme. Of these cases, three victims (who, notably, had personal connections in RBI) managed to get a positive outcome and were able to recover a partial amount. In the other two cases, the Ombudsman agreed with the bank response and placed the liability of the scam entirely with the victim.

Overall, victims were largely dissatisfied with their experiences with the bank, even in cases where they were able to recover some of their money. The levels of dissatisfaction with the banks were higher than those with the police. Experiences were similar across private and public banks. Amongst the six victims who rated their experience with the banks, the overall rating was poor, at one out of five.

2.3 Interactions with Courts and Legal Services

2.3.1 Approaching the courts

Victims' experiences of courts and legal services were very diverse. Few were ultimately able to obtain favourable outcomes. Most described litigation as a long and uncertain process that requires significant time, financial resources and persistence. Out of the 16 cybercrime victims, only four victims employed legal representation and pursued litigation through the courts.

Most victims who approached the courts did so only after concluding that other mechanisms would not resolve their grievances. Litigation emerged as a last resort rather than the natural starting point for seeking justice. As explained by a victim, after exhausting other avenues, *"only the option left was to go to the court."* Victims did not view litigation as an accessible first response to cybercrime.

Not every victim considered litigation worthwhile. Several deliberately remained outside the court system because of their arduous experiences with the police and banks, which led them to deliberate whether the investment required to pursue litigation was worth the outcome. A victim explained that pursuing a court case would involve paying lawyers, attending repeated hearings and spending additional money without any certainty of recovery. Access to legal advice did not automatically translate into court proceedings.

2.3.2 Delays in procedures

Victims who entered the judicial process consistently spoke about delays. Their frustration stemmed not simply from the passage of time, but from the absence of visible progress despite repeated hearings. *Vinod* offered the clearest illustration: *"The best part of our court is, judges are famous for giving the dates... from the last three years, they go on giving the dates."* The narrative reflects the feeling that litigation had become an ongoing process without hope for resolution. Each hearing required continued investment of time and energy while offering little indication that the dispute was moving closer to conclusion.

The experts' accounts provide further insight into why these experiences recur across cases. A serving police officer explained that each investigating officer in their cyber cell is responsible for managing investigations simultaneously while also attending court hearings related to those cases. Such operational demands inevitably slow the progress of investigations and judicial proceedings.

An expert pointed out that in cases involving intimate images or online abuse, authorities may eventually succeed in removing content, but *"the question is the time, when do they do it"*, because by then the material may already have spread across multiple platforms. This observation reflects a wider challenge within cybercrime. Digital harm often escalates far more quickly than formal legal processes.

2.3.3 Legal assistance

Some victims judged lawyers primarily by whether they helped move the case forward. One victim explained that after employing a lawyer, the matter eventually proceeded before the court and resulted in a favourable outcome. Legal representation therefore became valuable because it translated procedural requirements into practical progress.

Not every victim expressed the same confidence. A financial cybercrime victim had to switch lawyers after becoming dissatisfied with the advice he received, saying that his lawyer preferred settlement over adjudication. Another pointed to the nexus between the police, prosecution and legal-aid lawyers.

Age also appeared to shape some victims' interactions with legal processes. *Sanjeeb,* a senior citizen, described considerable difficulty navigating legal procedures and assessing the reliability of legal assistance. This suggests that older victims may experience additional vulnerabilities when engaging with complex legal and institutional systems following cybercrime.

2.3.4 Cost of legal proceedings

Cost emerged as another important consideration. Victims repeatedly assessed whether the financial and emotional investment required to pursue litigation remained proportionate to the amount lost. Some victims who already suffered financial loss saw little value in committing further resources to a process in which the outcome remained uncertain. An expert notes that even though legal aid provisions are in place, they are severely overstressed. Access to justice therefore depends not only upon legal rights but also upon victims' ability to sustain prolonged legal proceedings after suffering financial harm.

The data does not present an entirely bleak picture of judicial engagement, although victims encountered considerable challenges throughout the process. For some, the courts ultimately facilitated the recovery of losses. The findings suggest that litigation primarily functioned as the final procedural step required to authorise the release of recovered funds.

A banking expert explained that banks cannot independently release frozen funds because *"the stolen property is returned by a court order"*. However, notably, some victims reported recovering money at the level of the banks, without a court order.

2.4 Interactions with Informal Support Networks and Civil Society Organisations

2.4.1 Role of people of influence

Only a small number of victims explicitly discussed the role of people of influence, but their accounts reveal that such individuals often became important when formal institutional processes appeared slow, uncertain or ineffective. Victims turned to people in positions of authority or professional credibility to help them communicate with institutions, get clarification, create pressure and encourage quicker action on their cases. Victims linked these interventions to improved responsiveness from institutions at crucial stages of the redressal process.

Several victims believed that influential individuals help sustain the progress of cybercrime cases. For them, access to influential individuals increased confidence that the complaint would continue to receive attention.

A similar perception emerges from the account of a cyberbullying victim. As a Muslim woman, the victim believed that access to influential professional networks shaped how seriously the complaint was received by the police. Being a journalist, they were able to draw upon professional contacts who facilitated direct access to senior officers within the cybercrime unit. Her account suggests that they viewed these connections as instrumental in securing institutional attention that she believed might otherwise have been more difficult to obtain.

Victim accounts suggest that personal connections impact the case at several stages--whether or not an FIR is registered, whether or not the victim is able to recover any of the lost money, whether or not the victim is able to secure a favourable ruling from the court or RBI ombudsman. Of the six cases in which an FIR was registered, in two of the cases the victim used personal connections to get the FIR registered. Amongst the six victims of digital financial frauds who were able to recover their money partially or fully, three used personal connections at several levels.

These accounts illustrate that access to influential networks was perceived not merely as a means of expediting administrative procedures but as a mechanism for overcoming anticipated barriers to institutional responsiveness.

However, the experiences of some victims demonstrate that access to people of influence was not equally distributed. While some victims could approach senior police officers, media professionals or civil servants, others described navigating the aftermath of cybercrime without any comparable networks. Sextortion victim *Rohit* notes this disparity most clearly when reflecting on his experience: *"Hamare paas koi upper hand nahi tha... Humne jo bhi kiya tha, khud se kiya tha."* [We did not have any *"upper hand"*. We did everything on our own].

It is important to note that there is an overlap between victims who relied on influential contacts and those who ultimately engaged with the courts, suggesting that access to powerful social networks functioned as a mechanism for accessing formal justice. Those without such resources were more likely to abandon formal legal action or navigate complex institutional processes without additional support.

2.4.2 Support from family, friends and close associates

Victim experiences reveal that the process of recovery from cybercrime extends far beyond their contact with formal institutions. Many relied on informal support networks (family members, friends, neighbours, teachers, doctors and civil society organisations) as well as the police, banks, legal services and courts. These people often acted as first responders immediately after victimisation, helping victims to identify the cybercrime, stop the ongoing crime, make decisions and deal with emotional distress.

For many victims, family members provided the earliest and most consistent source of emotional support. Their role extended to actively assisting victims in managing the crisis. This support, however, was not always expressed only in terms of sympathy but co-existed with anger, concern, shame and attempts to prevent further victimisation, as a sextortion victim described.

In many cases, friends contributed both emotional support and practical assistance. Beyond emotional reassurance, friends also acted as important sources of specialised knowledge. When a victim found out that his email account had been hacked, he immediately called a classmate who works in the IT sector who suggested that he check his Google account activity. Instead of going through official channels, the victim first contacted a personal acquaintance who had the technical expertise, which he believed was needed.

Several accounts illustrate how support emerged from individuals who happened to be present during the offence rather than from pre-existing support structures. *Ganga* sought assistance from neighbours after becoming increasingly suspicious during a fraudulent phone call. The neighbour immediately instructed her to disconnect the call and helped terminate the conversation despite the fraudster's repeated attempts to prevent her from ending it. Similarly, *Fatima* described calling a doctor to her residence while experiencing a digital arrest scam. The doctor arrived immediately, instructed her to block further communication with the offenders and advised her to contact her auditor before any money was transferred. These interventions were significant because they occurred while the offences were still unfolding and prevented monetary loss.

However, family and other informal networks were not uniformly experienced as sources of support. For victims of gendered cybercrimes, disclosure sometimes carried the risk of blame, humiliation and social judgement rather than understanding. An expert explained that women experiencing NCII or online gender-based violence may be reluctant to seek support from their own families because of concerns about *"shame and honour"*. The expert noted that victims often fear how parents and relatives will respond, particularly where intimate images are involved, and therefore choose not to disclose the abuse at all. This observation suggests that the availability of family support cannot be assumed. For some victims, anticipated stigma itself becomes a barrier to seeking help.

2.4.3 Support from civil society organisations

Beyond these relationships, the experts spoke about organisations that provide counselling, legal guidance, referrals and practical support throughout victims' recovery. An expert on online gender-based violence explained that her organisation offers different forms of assistance, including counsellors and legal service providers. Cases are referred to organisations according to their particular expertise, enabling victims to receive specialised support appropriate to their circumstances. Similarly, another expert talked

about providing extensive *"handholding"* to victims and their families. That meant explaining how to report; supporting victims when dealing with police; helping parents manage children's distress; and connecting victims with vetted professionals such as cyber lawyers, investigators and journalists.

The experts also highlighted the importance of psychological support, particularly for victims experiencing image-based abuse, online harassment and other highly personal cybercrimes. However, both experts emphasised that existing support remains inadequate.

The findings demonstrate that informal support networks constituted an important component of victims' pathways to recovery. Family members, friends, teachers, neighbours and trusted professionals frequently helped victims make informed decisions and cope with emotional distress. Civil society organisations complemented these informal networks by providing specialised psychological, legal and practical assistance that formal state institutions often lacked. However, access to such support was uneven.

The findings suggest that informal support networks can occupy an ambivalent position within victims' recovery in cases of gendered cybercrimes. For victims of image-based abuse and online harassment, concerns about blame and reputational damage could therefore discourage disclosure and limit access to support at precisely the moment when it was most needed. The findings also suggest that recovery from cybercrime depends not only upon the effectiveness of formal institutions but also upon the availability and accessibility of supportive social relationships and victim-centred civil society services.

2.5 Recommendations

The recommendations presented below are drawn directly from the in-depth interviews with cybercrime victims and experts, as well as the FGD. Victims' accounts pointed to the need for greater institutional responsiveness, accessibility and accountability after a cybercrime occurs, while experts, including police personnel, banking professionals and civil society representatives, emphasised reforms required to strengthen prevention, investigation and coordination across institutions.

2.5.1 Improving reporting and access to justice

Accessing institutional support remained a significant challenge for many victims because of the complexity of the reporting process itself. One victim of financial cyber fraud criticised the design of the National Cybercrime Reporting Portal (NCRP), observing that it should function more like other government digital services by guiding users through each stage of reporting, preventing incomplete submissions and allowing complaints to be saved and completed later. Victims also suggested that the portal should more clearly distinguish different categories of cybercrime and provide contextual guidance throughout the reporting process. Such improvements were considered particularly important because complaints are often submitted when victims have already suffered considerable financial loss and are experiencing emotional distress.

Victims also highlighted the lack of transparency once complaints had been registered. Victims of financial cyber fraud described receiving little to no communication regarding the progress of their complaints, leaving them uncertain about whether any action had been initiated. One victim suggested that complainants should receive immediate confirmation that *"your details are now with such and such agency",* followed by regular updates on the case's status. Another recommended a tracking mechanism similar to the Right to Information process, enabling complainants to monitor each stage of the investigation rather than repeatedly contacting different agencies. Victims also proposed that online complaints should remain editable so that additional information or evidence can be submitted without requiring repeated visits to police stations. These narratives point to the need for a more transparent and victim-centred

complaint management system that keeps victims informed throughout the investigative process.

Experts working on gendered cybercrimes also highlighted the need to improve access to justice through dedicated reporting mechanisms, specialised support units and safeguards against coercive settlements for victims of gender-based cybercrimes.

2.5.2 Strengthening institutional response and investigation

Across interviews with victims of financial cyber fraud, the timeliness of institutional responses emerged as one of the most consistent concerns. Victims described delays in registering FIRs, assigning investigating officers, and initiating recovery measures as factors that not only reduced the likelihood of recovering stolen funds but also prolonged emotional distress. One victim recommended that authorities should *"take action very quickly"* and complete essential action *"within a month",* explaining that prolonged delays leave victims struggling with persistent anxiety. Another victim, who had lost Rs. 2.7 lakhs in a cyber fraud, recalled being informed that the investigating officer was unavailable because of VIP duty, questioning why an urgent complaint should *"take a backseat"* to other responsibilities. Other victims similarly described having to approach police officials repeatedly to ensure that complaints progressed. These accounts suggest the need for clearly defined timelines for complaint registration and investigation, routine review of pending cases and stronger accountability mechanisms to ensure that cybercrime complaints receive timely attention.

The victims also pointed to the fragmented nature of the current institutional response. Several victims said they had to separately visit police stations, banks, payment service providers, telecommunication companies and regulatory authorities after an incident of cyber fraud. To address this, victims recommended establishing a single-window mechanism capable of coordinating action across relevant institutions. One victim proposed *"a system and a single window",* connecting banks, the Reserve Bank of India and telecommunications providers to facilitate simultaneous action. At the same time, another suggested that the RBI Banking Ombudsman should serve as the central coordinating authority. Such a mechanism, victims argued, would reduce procedural delays, improve inter-agency coordination and minimise the burden currently placed on victims in navigating multiple institutions.

Across interviews, experts emphasised that the rapid growth and increasing sophistication of cybercrime have outpaced existing institutional capacity. Experts recommended expanding dedicated cybercrime police stations, strengthening cyberforensic laboratories and investing in technological infrastructure to support digital investigations. Policing experts from the FGD also highlighted the need to recruit investigators with engineering and cybersecurity expertise and recommended revisiting provisions of the Information Technology Act, 2000 that restrict the investigation of certain cyber offences to particular police ranks. According to these experts, broadening investigative powers and enhancing technical capacity would enable a more effective and timely response to cybercrime.

Civil society representatives recommended developing standard operating procedures that clearly define institutional responsibilities and improve coordination between police, regulators and victim support organisations. Experts also proposed establishing a dedicated 24-hour cybercrime helpline capable of providing immediate guidance, directing victims to the appropriate reporting mechanisms and ensuring that timely action is initiated during the critical period immediately following a cybercrime incident.

2.5.3 Accountability of financial institutions and digital platforms

The responsibility of financial institutions emerged as a major theme across interviews with victims of financial cyber fraud. While victims acknowledged the importance of individual

vigilance, they argued that fraud prevention should not depend solely on users. One victim suggested that banks should monitor unusual transaction patterns, explaining that if an individual who had never withdrawn more than Rs. 1 lakh suddenly attempted to transfer Rs. 10 lakhs, the transaction should automatically trigger additional verification. Victims also proposed allowing customers to determine transaction limits when opening bank accounts and introducing additional safeguards for vulnerable users. One victim recommended that transactions above a specified amount from a minor's account should require parental approval before completion.

Victims further argued that banks themselves should be held accountable for preventing cyber fraud. One victim recommended that banks periodically publish fraud statistics so that customers can compare institutions based on their cybercrime records. According to the victim, public disclosure would keep banks *"on their toes"* by encouraging stronger fraud prevention measures and greater institutional responsibility. Another questioned why banks continue to rely on security mechanisms that major technology companies have already abandoned, recommending that authentication systems should be reviewed and updated regularly to respond to emerging threats.

Shortcomings within digital payment systems were also highlighted. Victims recommended that account holders should receive immediate notifications whenever accounts are flagged for suspected fraud, or funds are placed under a *lien*, similar to the alerts currently generated after incorrect PIN entries. Strengthening payment systems and improving communication between financial institutions and customers were viewed as important preventive measures.

Experts also highlighted the need to redistribute responsibility for cybercrime prevention across institutions rather than placing the burden primarily on victims and law enforcement agencies. Banking experts, police personnel and civil society representatives argued that financial institutions, payment service providers and telecommunications companies should assume greater responsibility for preventing cyber-enabled fraud. Drawing on international practice, one expert observed that *"as soon as we start giving accountability, people will react",* referring to regulatory approaches that make banks financially liable for reimbursing victims of authorised push payment fraud.

The expert argued that such measures encourage financial institutions to invest in stronger fraud prevention systems because institutional failures carry tangible consequences. Experts therefore recommended strengthening regulatory oversight of banks, payment intermediaries and telecommunications providers, particularly in relation to mule accounts, fraudulent SIM card issuance and other institutional vulnerabilities that facilitate cybercrime.

2.5.4 Strengthening responses to gender-based cybercrimes

Victims of gender-based cybercrimes, including NCII abuse, bullying and sextortion, highlighted the need for responses that recognise the distinct nature of these harms. Victims described the psychological impact of image-based abuse as extending well beyond the initial incident, emphasising that dismissive attitudes and victim-blaming responses by authorities can further compound trauma. They therefore recommended that police personnel should ensure that complaints are handled with empathy, confidentiality and respect for victims' dignity. Victims also stressed that quicker intervention is critical in cases where harmful content, abusive messages and intimate images can spread rapidly across digital platforms. They recommended stronger coordination between police, social media platforms and other intermediaries to facilitate the immediate removal of such content and prevent further circulation.

Experts working on gendered cybercrimes argued that responses to these offences should recognise the distinct nature of the harm suffered by victims. They observed that existing legal and institutional approaches frequently treat such cases through the lens of obscenity rather than acknowledging

violations of privacy, dignity and bodily integrity. Experts recommended reforms that place greater emphasis on protecting victims' rights and reducing secondary victimisation during the reporting and investigation process. They also advocated for specialised gender-sensitive training for police officers and judicial personnel, noting that victim-blaming attitudes continue to discourage reporting and undermine confidence in the justice system.

2.5.5 Expanding cyber safety awareness and prevention

Awareness and digital literacy featured prominently across interviews with victims. Many expressed concern that existing awareness initiatives are failing to reach those most vulnerable to cyber-enabled fraud. Victims recommended practical awareness campaigns that explain common fraud techniques, safe digital banking practices, reporting procedures and the responsible use of digital payment applications, particularly for older adults, rural communities and first-time users.

The importance of strengthening public awareness initiatives was emphasised across interviews with experts. A banking expert stated that cyber safety campaigns should be delivered in regional and vernacular languages rather than relying primarily on Hindi and English. He said that effective communication must be in tune with India's linguistic diversity. Another expert argued that cyber safety messaging should receive far greater visibility across *"electronic media, print media, social media",* noting that existing initiatives do not match the pace of the increasing prevalence of cybercrime. One expert noted that *"a lot of things are not solved only by law"* and emphasised that cyber safety interventions are required *"at every level"*. This included strengthening cyber safety education in schools, supporting parents and communities, and encouraging greater responsibility among technology companies.

Endnotes

i Press Information Bureau. (2025, May 19). *Union Home Minister Shri Amit Shah says MHA's Indian Cybercrime Coordination Centre (I4C) has introduced the new e-Zero FIR initiative to nab any criminal with unprecedented speed*. Government of India. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2129715&reg=48&lang=2

References

- Reserve Bank of India. (2017, December 14). *Customer protection: Limiting liability of customers of co-operative banks in unauthorised electronic banking transactions*. https://www.rbi.org.in/commonman/english/scripts/Notification.aspx?Id=2623
- Reserve Bank of India. (2025, September 25). *Reserve Bank of India (Authentication mechanisms for digital payment transactions) Directions, 2025*. https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12898&Mode=0
- Smith, C., & Meierhans, J. (2024, September 25). *Banks must refund fraud up to £85,000 in five days*. BBC News. https://www.bbc.com/news/articles/cy94vz4zd7zo
- The Hindu. *(2026, June 25). RBI's digital scam compensation pilot explained.* https://www.thehindu.com/business/Economy/rbis-digital-scam-compensation-pilot-explained/article71145018.ece#google_vignette

CHAPTER

03

Punjab Feminist Union of Students protesting against MMS scandal in Chandigarh University (Chandigarh, Punjab - September 19, 2022).

Photo by Ravi Kumar/Hindustan Times.

Threats to Digital Safety: Perceptions and Experiences

Key Findings

- A third of the respondents frequently receive fake delivery or high-return investment scam calls; nearly a quarter have frequently received bank impersonation calls, phone calls linked to illegal activities, and unknown numbers claiming to be a friend.
- Data shows that greater usage of online payment methods is associated with higher exposure to fraudulent calls. Among the respondents who have higher online usage, nearly half (46%) have reported exposure to fraudulent calls.
- Victims of cybercrimes are more likely to receive frequent scam calls or messages.
- More than half of the respondents (55%) are very scared of losing money through online fraud or scams. Fifty-seven percent respondents also feel that incidents of online scams and frauds have increased a lot in the last two years.
- Women are relatively more fearful of different types of cybercrimes than men.

Threats to Digital Safety: Perceptions and Experiences

Digital expansion has transformed everyday life, transcending vital aspects of modern life – communication, finance, governance, and social interaction, to name a few. From digital payments and e-commerce to social media engagement and online public services, individuals increasingly rely on digital platforms. This growing dependence has created new opportunities for efficiency, connectivity, and participation in the digital economy. However, the rapid pace of digitalisation has outpaced the development of adequate safeguards and public awareness, exposing users to a range of emerging risks and vulnerabilities.

As digital systems become more central to everyday transactions and communication, concerns about online safety, privacy, and fraud have also intensified. Cybercrime has evolved in both scale and sophistication, targeting individuals through phishing, identity theft, financial scams, and other deceptive practices. These developments raise important questions about how citizens experience and interpret security in an increasingly digitised environment.

Against this backdrop, this chapter examines how citizens perceive security in the digital environment, how frequently they encounter fraud attempts, what kinds of harms they fear most, whether they believe their social identities make them more likely to be targeted, and whether they perceive cybercrimes to be increasing over the years. The findings reveal a public that is deeply integrated into the digital ecosystem but increasingly cautious, alert, and anxious about the risks that accompany it.

3.1 Routine Exposure to Scam Calls and Messages

Digital scams in India are proliferating at an unprecedented rate and are embedded within routine digital activity. To understand how normalised such exposure has become, it is essential to first examine how frequently citizens encounter different types of fraudulent calls and messages.

The survey with the general public reveals that one in three respondents receives fake calls about delivery of the products they never ordered (33% - combining both “many times” and “sometimes”) (**Table 3.1**). A similar proportion (31% - combining both “many times” and “sometimes”) also encounters high-return investment scams. More than one in four respondents (27% - combining both “many times” and “sometimes”) reported having received calls from individuals posing as bank officials seeking personal or account details. Also, about a quarter of the respondents reported having received calls telling them that their phone number has been linked to illegal activities (23% - combining both “many times” and “sometimes”) or calls from unknown numbers claiming to be a friend or relative who urgently needs money (23% - combining both “many times” and “sometimes”). One in five respondents also reported frequently receiving calls from someone impersonating an authority figure, claiming that their friend or relative is in danger or has committed a crime. Delivery scams draw on the rapid growth of e-commerce, investment scams tap into rising financial aspirations, bank impersonation exploits institutional credibility and fake calls from the police leverage fear of legal authorities. However, it is also interesting to see that a majority of respondents, ranging from roughly half to nearly six in ten across different scam types, reported that they have never encountered such calls or messages (**Table 3.1**). Overall, cyber fraud evolves in parallel with patterns of digital adoption, continuously adapting to everyday digital practices.

Table 3.1: High-return investment and fake delivery scams are among the most frequently reported fraud attempts

Received a call/ text message for	Many times	Sometimes	Rarely	Never
Investment opportunity, guaranteeing a high return	10	21	20	45
Delivery of a product you never ordered	8	25	20	44
Bank official asking for personal or account details	7	20	21	49
The phone number has been linked to illegal activities	6	17	16	56
An unknown number claiming to be your friend/ relative who is in urgent need of money	6	17	19	54
Call from police or someone in authority claiming that your friend/ relative is in danger or has committed some crime	5	15	18	59

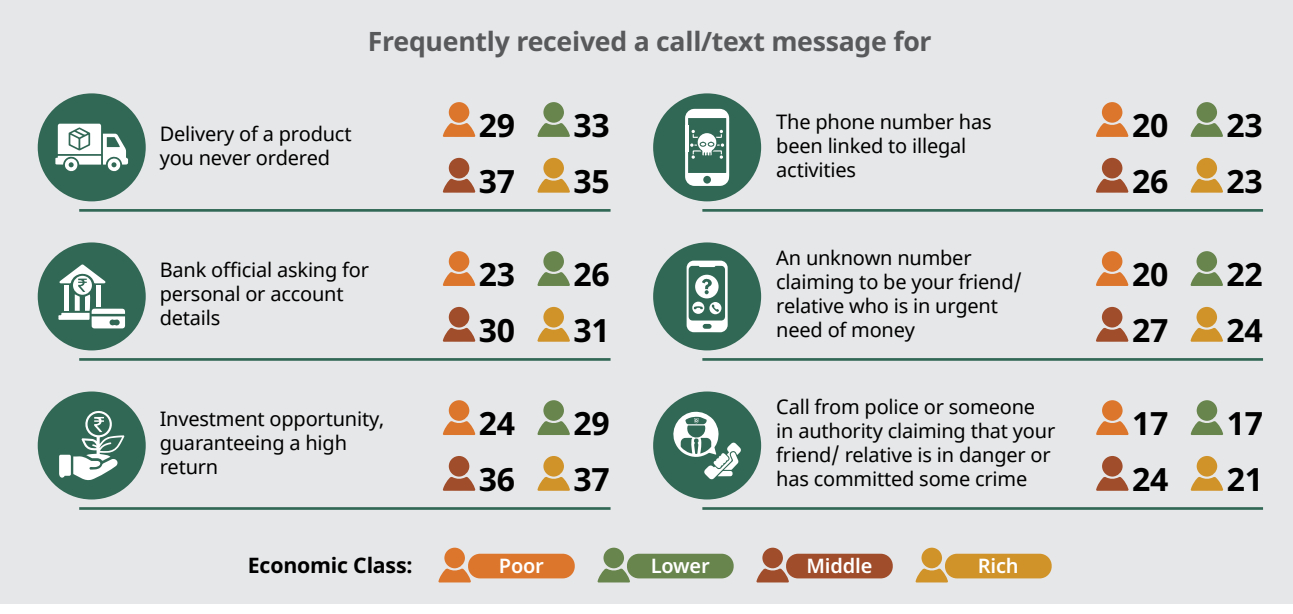
Note: All figures are in percentages. Rest did not respond.

Question asked: "How often do you receive a call/text message – Delivery of a product you never ordered/ Phone number has been linked to illegal activities/ Bank official asking for personal or account details/ Unknown number claiming to be your friend/relative who is in urgent need for money/ Police or an authority claiming a friend or relative is in danger or committed a crime – many times, sometimes, rarely, or never?"

Digital exposure is rarely socially neutral. Patterns of access, consumption and financial participation differ across economic groups, potentially shaping both opportunity and vulnerability. Examining scam exposure across economic classes, therefore, helps clarify whether fraud risk is evenly distributed or concentrated across various income groups.

Figure 3.1 shows that respondents belonging to middle and high-income groups report higher levels of frequent scam calls than respondents from economically disadvantaged sections. For instance, 37 percent of those belonging to the middle class and 35 percent of those from rich backgrounds frequently receive fake delivery scam calls, compared to 29 percent among those

Figure 3.1: Middle and high-income groups report higher exposure to frequent scam calls



Note: All figures are in percentages. The categories of "many times" and "sometimes" have been combined as "frequently". Some figures might not add up to 100 as they represent only the respondents who received a call/text message "frequently".

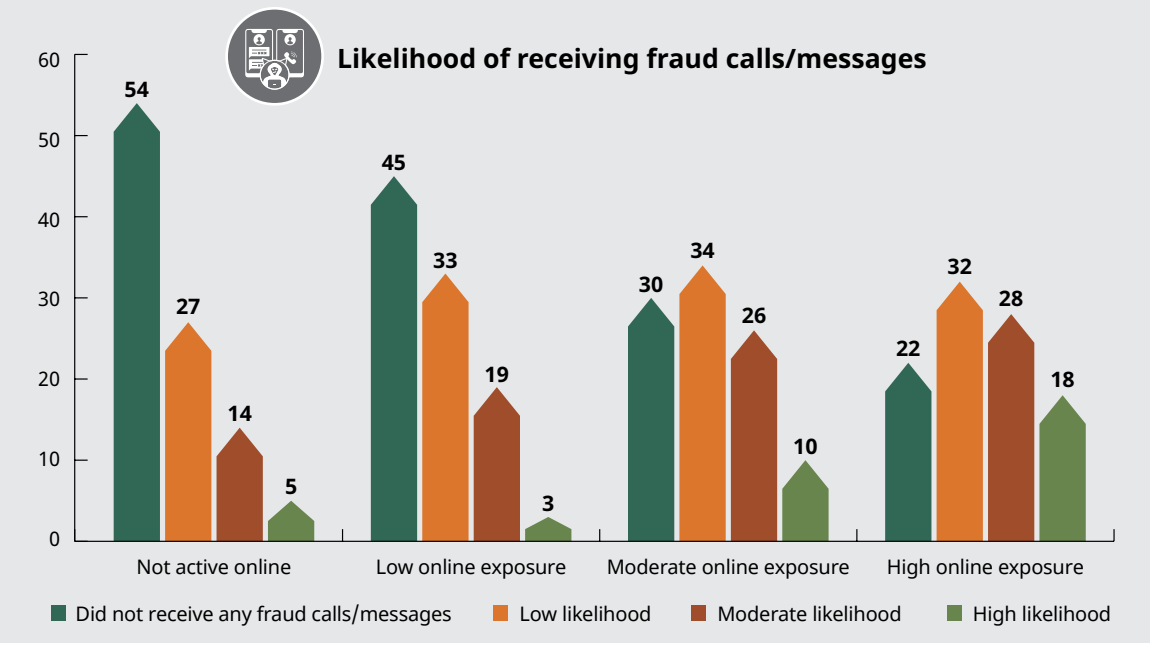
who are economically the weakest. Similarly, 36 percent and 37 percent of those belonging to the middle economic class and the most affluent class respectively encounter high-return investment scams, compared to 24 percent among economically disadvantaged respondents.

Recent news reports further reinforce that cyber fraud often involves disproportionately large financial losses, suggesting that individuals with greater financial resources are more actively targeted. For instance, an elderly man in Bengaluru reportedly lost Rs. 76.65 lakh in a cyber scam (*The Hindu,* 2026), while in another case a woman lost Rs. 3.75 crore after being misled by an AI-generated video of *Sadhguru,* a religious preacher (Bopanna, 2025). Similarly, reports detail cases such as an elderly man in Kolkata losing Rs. 1.8 crore (Ghosh, 2025), and a retired supervisor in Bhopal losing Rs. 68 lakh to "digital arrest" scams (*Times News Network, 2025*).

This variation across income groups may be attributed to two main reasons: higher income groups may engage more actively in online transactions, investments and e-commerce, while economically disadvantaged groups may interact differently with digital platforms. This could make the former more vulnerable to cyber scams because of higher digital exposure. Secondly, more sophisticated forms of cyber scams involve profiling victims through access to bank account details and other personal information, thus rendering those with better economic corpus as more vulnerable.

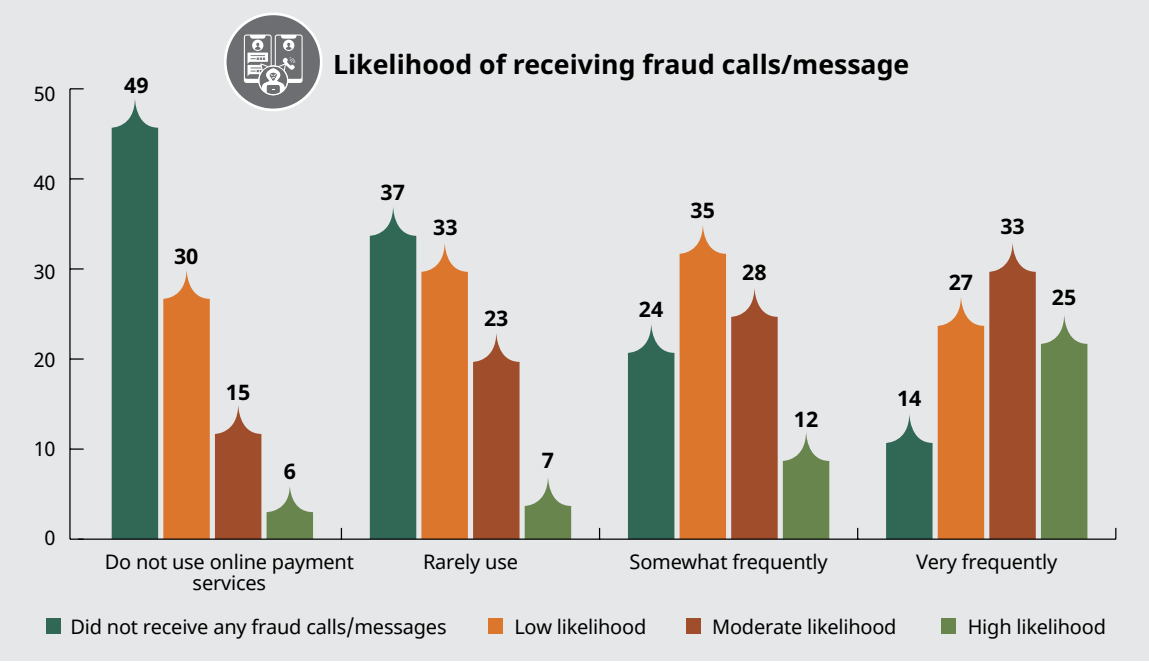
Individuals who spend more time online or rely heavily on digital payment systems leave larger digital footprints and interact more frequently with unknown digital actors. This raises an important question: does deeper digital integration increase exposure to fraudulent communication? **Figure 3.2** reveals a clear pattern between internet usage and exposure to fraudulent calls and messages. Among the respondents with high online usage, 18 percent fall in the high scam-exposure category and 28 percent fall in the moderate scam-exposure category; together – 46 percent report scam exposure. In contrast, among those who do not use the internet, only five percent report high exposure and 14 percent report moderate exposure. Conversely, a majority of those who did

Figure 3.2: Those who are more active on the internet are more likely to be exposed to fraud calls/messages



Note: All figures are in percentages. This is an index created using a battery of questions. They include a question on the frequency of use of social media, mobile banking apps and UPI and another question on the frequency of receiving suspicious/fraud-related calls or messages, including fake deliveries, bank scams, emergency money requests, illegal activity claims, and fraudulent investment offers. Please refer to Appendix 3 to see how the index was created.

Figure 3.3: Those who use online payment services very frequently are very likely to receive fraud calls/messages



Note: All figures are in percentages. This is an index created using a battery of questions. These include questions on the frequency of using different modes of online payment, including UPI, NEFT/RTGS, cards, and payment wallets and another question on the frequency of receiving suspicious/fraud-related calls or messages, including fake deliveries, bank scams, emergency money requests, illegal activity claims, and fraudulent investment offers. Please refer to Appendix 3 to see how the index was created.

not use internet (54%) reported not receiving any suspicious or fraud calls/messages, compared to only 22 percent among those who are very active online. These findings suggest that digital engagement significantly raises exposure to suspicious or fraudulent communication.

A similar pattern emerges with the use of online payment services. Among respondents who use digital payment platforms very regularly, 25 percent report high exposure to fraudulent calls and messages, while another 33 percent report moderate exposure. In contrast, only six percent of those who do not use online payment services report high scam exposure. At the same time, a majority of those who do not use online payment services (49%) did not report receiving fraud calls/messages, compared to just 14 percent among those who use online payments very frequently (**Figure 3.3**). The findings indicate that deeper participation in digital financial systems increases visibility to potential fraudsters, making frequent users more likely to encounter scam attempts.

These findings draw attention to an important trend: User integration into digital systems – whether through frequent internet use or reliance on online payments – increases susceptibility to scam attempts. Digital participation expands convenience and inclusion, but it simultaneously increases visibility within networks where fraudulent actors operate. In this sense, digital immersion not only enables opportunity; it also structurally heightens exposure to cyber risk.

Experience with cybercrime may alter patterns of future exposure. Victimhood can sometimes lead to greater caution, but it may also result in compromised data circulation, making individuals more visible to fraud networks. To understand whether prior victimisation reduces or intensifies subsequent scam exposure, it is important to compare those who have experienced cybercrime directly or indirectly with the broader sample.

As **Table 3.2** reflects, cybercrime victims report substantially higher exposure to all forms of scam calls and messages than non-victims. More than half (53%) of victims frequently receive fake delivery scam calls, compared to

Table 3.2: Cybercrime victims report substantially higher exposure to frequent scam calls and messages

Received a call/text message for...	Overall	Victims	Non-victims
Delivery of a product you never ordered	**33**	53	29
The phone number has been linked to illegal activities	**23**	38	20
Bank official asking for personal or account details	**27**	46	23
An unknown number claiming to be your friend/ relative who is in urgent need of money	**23**	44	19
Investment opportunity, guaranteeing a high return	**31**	50	27
Call from police or someone in authority claiming that your friend/relative is in danger or has committed some crime	**19**	37	16

Note: All figures are in percentages. The figures here represent the combined responses of "many times" and "sometimes" categories. The categories of "many times" and "sometimes" have been combined as "frequently".

only 29 percent among non-victims. Similarly, half of the victims (50%) frequently encounter high-return investment scams, whereas the figure drops to 27 percent among non-victims. Victims are also nearly twice as likely to report bank impersonation attempts in contrast to non-victims (46% versus 23%), calls from unknown relatives seeking money (44% versus 19%), and digital arrest-related scams (38% versus 20%).

In contrast, non-victims consistently report much lower levels of exposure across all scam categories, suggesting that they are either less frequently targeted or less aware of fraudulent attempts. The findings indicate that cybercrime victimization does not necessarily reduce future exposure; rather, victims appear to remain significantly more vulnerable to continued targeting. This may reflect the circulation of compromised personal data among fraud networks or heightened awareness among victims that enables them to recognise scam attempts more readily.

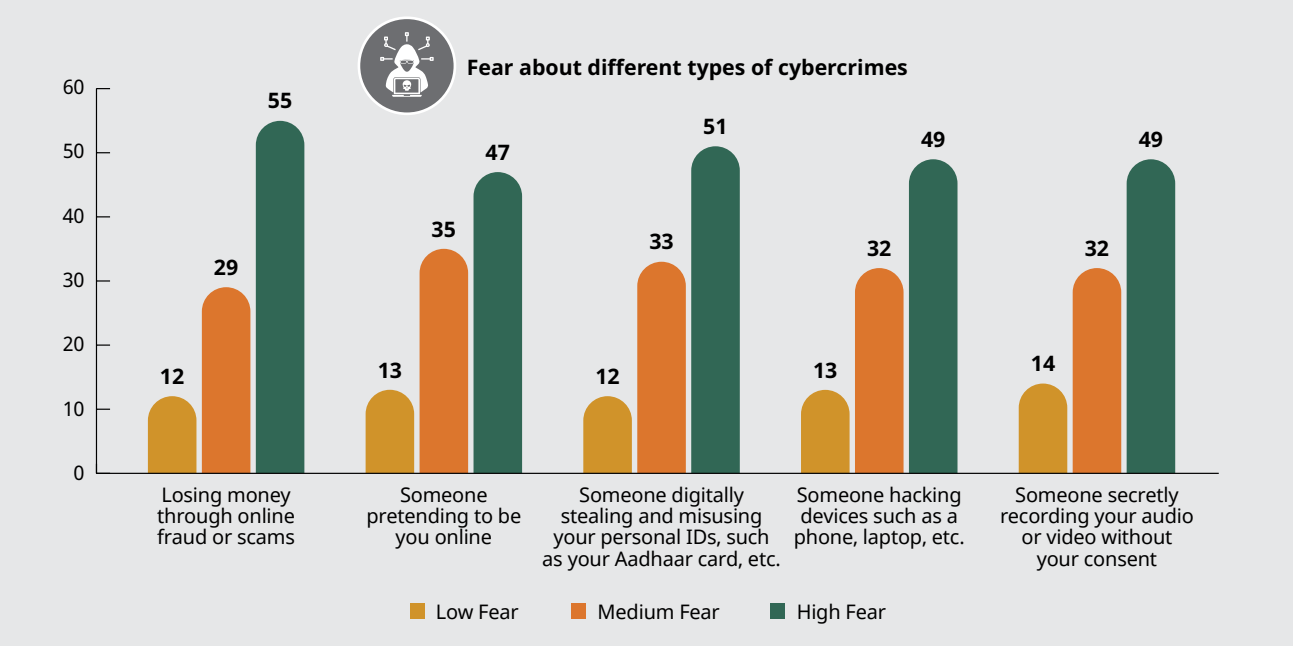
3.2 The Emotional Architecture of Digital Fear

Exposure alone does not fully capture digital vulnerability. Perceptions and emotions play a crucial role in shaping how secure citizens feel within digital environments. It is thus important to assess how scared people feel of different forms of cybercrimes.

As shown in **Figure 3.4,** financial fraud sits at the centre of digital anxiety. More than one in every two respondents (55%) reports a high fear of losing money through online scams. The fear of misuse of personal information follows closely behind. A slim majority (51%) expresses high fear of misuse of personal identification documents such as Aadhaar, signalling deep concern about identity theft and data misuse. Close to half report high fear of device hacking (49%) and secret recording without consent (49%). Even impersonation, someone pretending to be them online, generates high fear among nearly half of the respondents (47%). The clustering of these figures around the 50 percent mark indicates that digital fear is not marginal; it is widespread and structurally embedded. Economic harm appears to be the most immediate and tangible threat, but concerns about surveillance, hacking and misuse of personal data are nearly as powerful.

Digital spaces are embedded within broader social hierarchies, and offline inequalities often extend into online environments.

Figure 3.4: People are most afraid of losing money through online fraud or scams



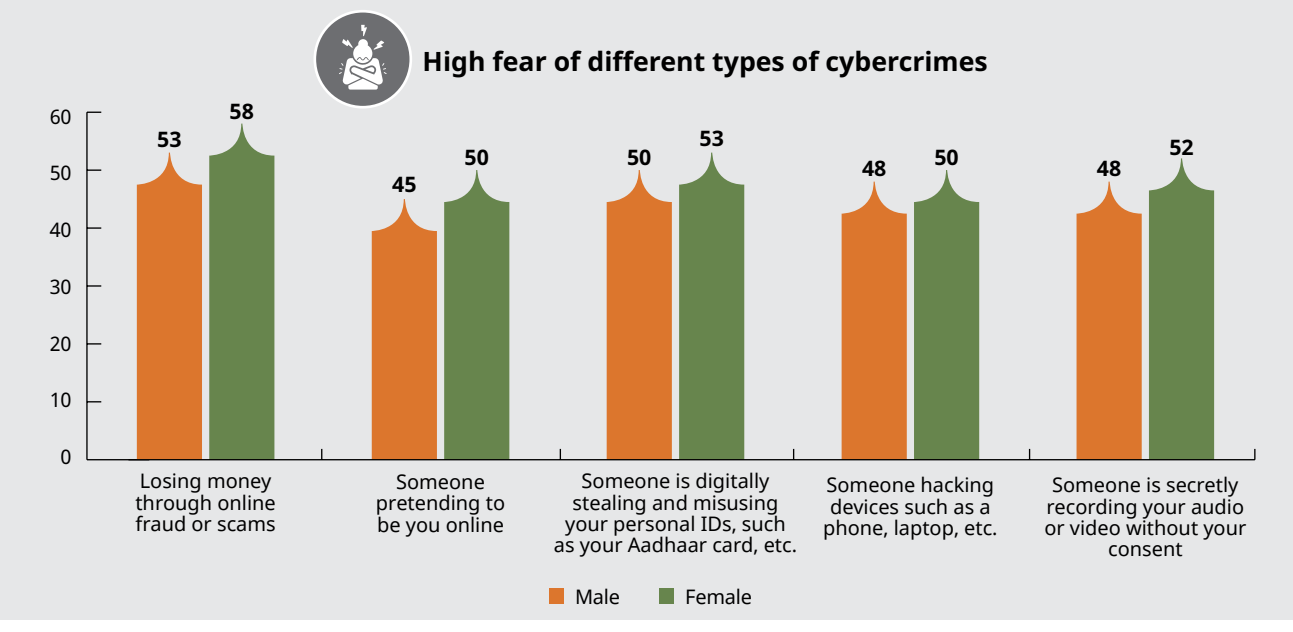
Note: All figures are in percentages. The rest did not respond. The categories of fear have been combined. 'Not at all scared' and 'Category 2' as "Low Fear", Category 3 and Category 4 as "Medium Fear", Very scared as "High Fear".

Question asked: "On a scale of 1 to 5, where 1 means 'not at all scared' and 5 means 'very scared', how scared are you – Losing money through online frauds or scams/ Someone pretending to be you online/ Someone digitally stealing and misusing your personal IDs such as Aadhaar card, etc./ Someone hacking your devices such as phone, laptop, etc./ Someone secretly recording your audio or video without your consent?"

Gender, in particular, shapes experiences of harassment, impersonation and privacy violations. Understanding gender differences in cyber-related fear helps illuminate how digital insecurity intersects with existing patterns of vulnerability.

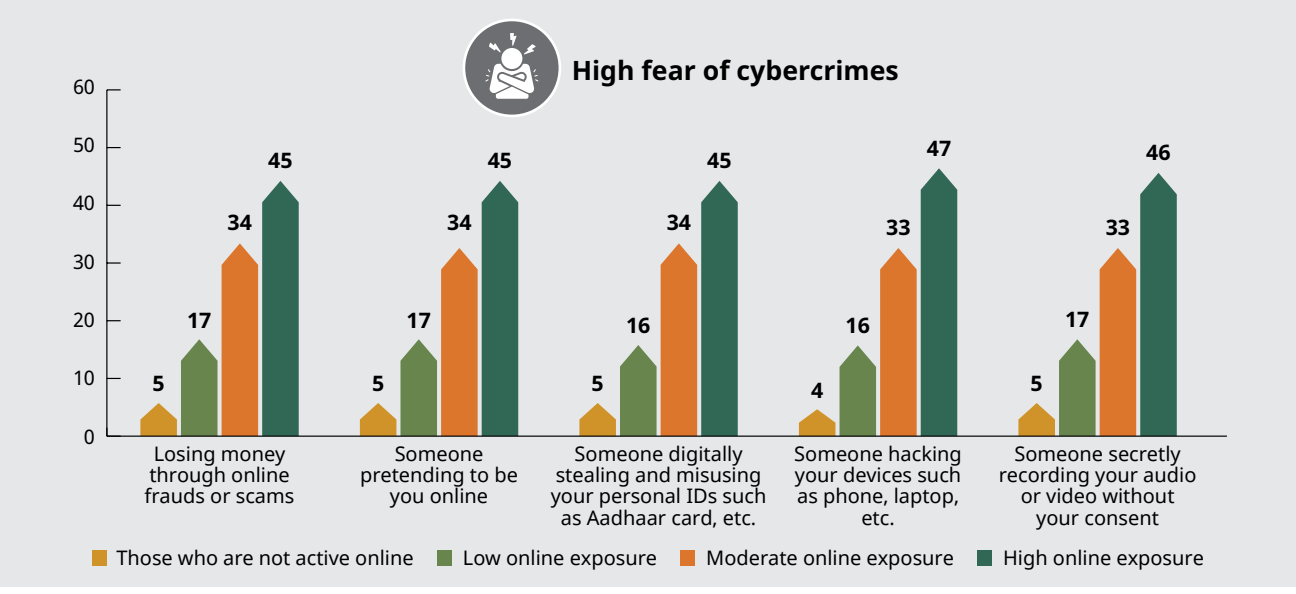
Figure 3.5 shows that women report slightly higher levels of fear across all cyber-risk scenarios. Nearly six in ten women (58%) express high fear of financial fraud, compared to 53 percent of men. Women are also more likely to report high fear of impersonation (50% versus

Figure 3.5: Women consistently report higher levels of fear of different types of cybercrimes



Note: All figures are in percentages. The figures represent only those respondents who said "high fear".

Figure 3.6: Those who have high online exposure are the most likely to have high fear of cybercrimes

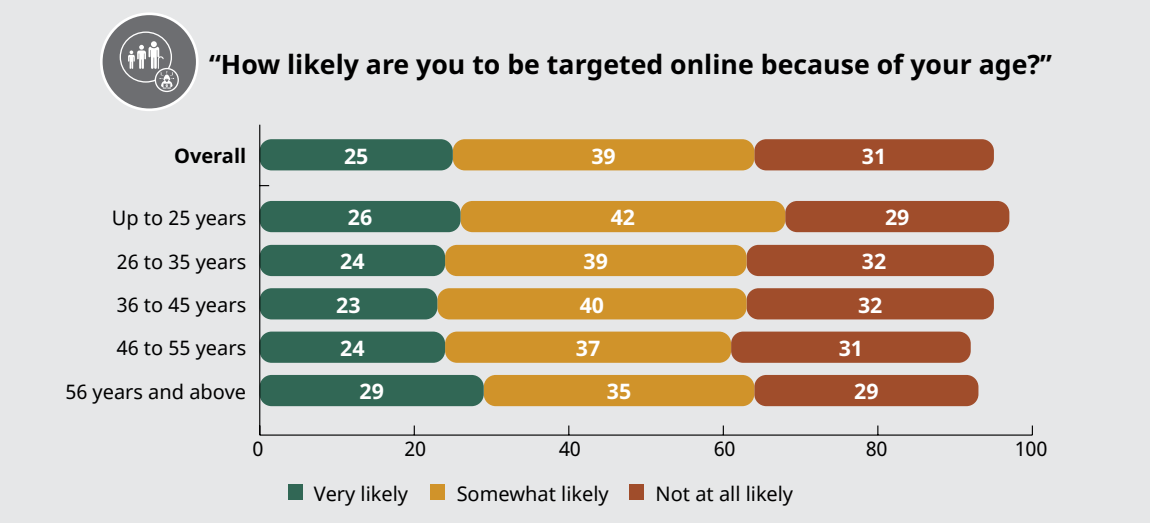


Note: All figures are in percentages. The figures may not add up to 100 as numbers are rounded off. The figures represent only those respondents who had a "high fear" level.

45%), identity misuse (53% versus 50%), device hacking (50% versus 48%), and secret recording without consent (52% versus 48%). These differences reflect how digital vulnerability intersects with broader gendered patterns of insecurity, particularly in relation to harassment and non-consensual content misuse.

There is an inherent paradox in the use of digital services; those who rely most heavily on digital systems for communication, work and financial transactions may simultaneously feel the most vulnerable within them. **Figure 3.6** demonstrates that high-frequency online users dominate the "high fear" category across every risk dimension. Roughly 45-47 percent of those expressing high fear of financial fraud, impersonation, identity theft, hacking or secret recording are frequent online users. By contrast, only a negligible four to five percent

Figure 3.7: Respondents of all age groups feel that they are vulnerable to cybercrimes because of their age



Note: All figures are in percentages. Rest did not respond.
Question asked: "Compared to others, how likely are you to be targeted online because of your age?"

of those with high fear report not using online platforms at all.

3.3 Social Profile of Vulnerability

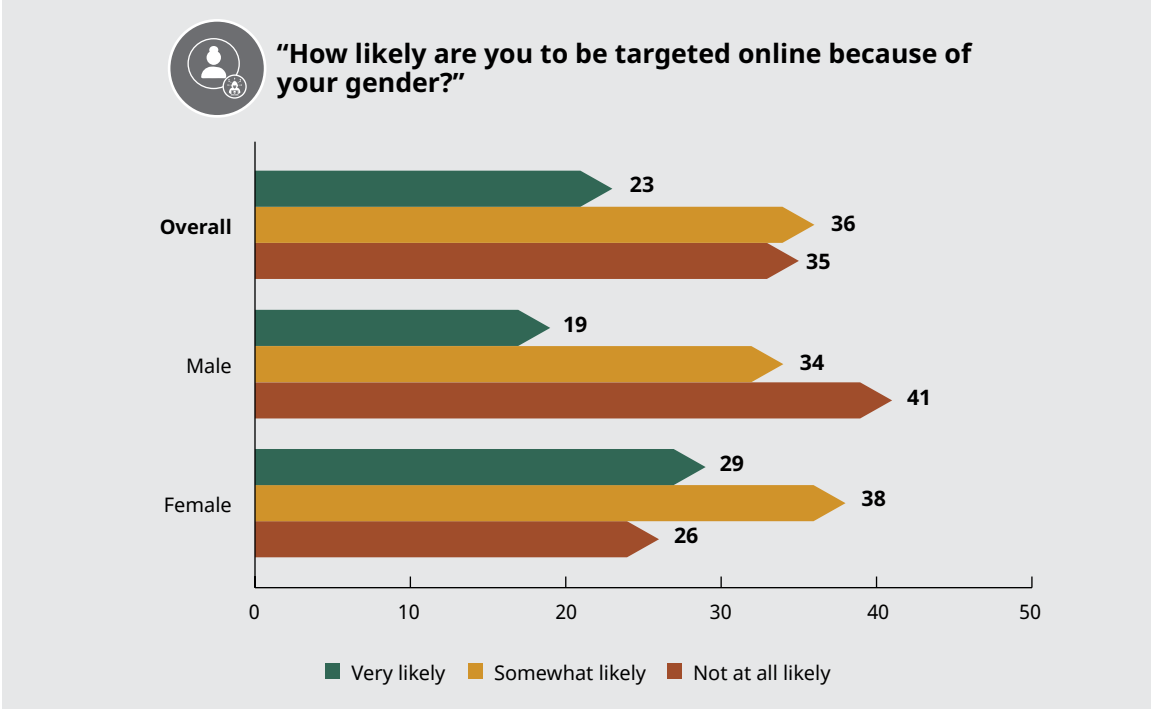
Cyber vulnerability is not experienced purely as a technological issue; it is often interpreted through social identity. Age, gender, religion, caste, profession and other identity markers may influence how individuals perceive their likelihood of being targeted online. Understanding which social characteristics are most commonly associated with perceived targeting helps reveal whether digital risk is understood primarily as behavioural or socially structured.

The patterns in **Figure 3.7** show that people's perceptions of age-based targeting are remarkably consistent across all age groups. Overall, 64 percent of the respondents believe that age increases their likelihood of being targeted online, including 25 percent who say "yes, very much" and 39 percent who say "yes, somewhat". Across age categories, combined perceptions of vulnerability remain consistently high, ranging between 61 and 68 percent. Even among those aged 56 years and above, 64 percent (29% "very much" and 35% "somewhat") feel their age makes them vulnerable to cybercrimes.

Gender differences, however, are sharper and more pronounced. Women are significantly more likely to feel vulnerable to cybercrimes, compared to men. As shown in **Figure 3.8,** over two-thirds of women (67%) believe they are likely to be targeted because of their gender. Most strikingly, 29 percent of women say they are "very much" at risk compared to only 19 percent of men, a ten-point gap in strong perception of vulnerability. On the other hand, 41 percent of men feel that they are not at all likely to be targeted online because of their gender in comparison to only 26 percent of women.

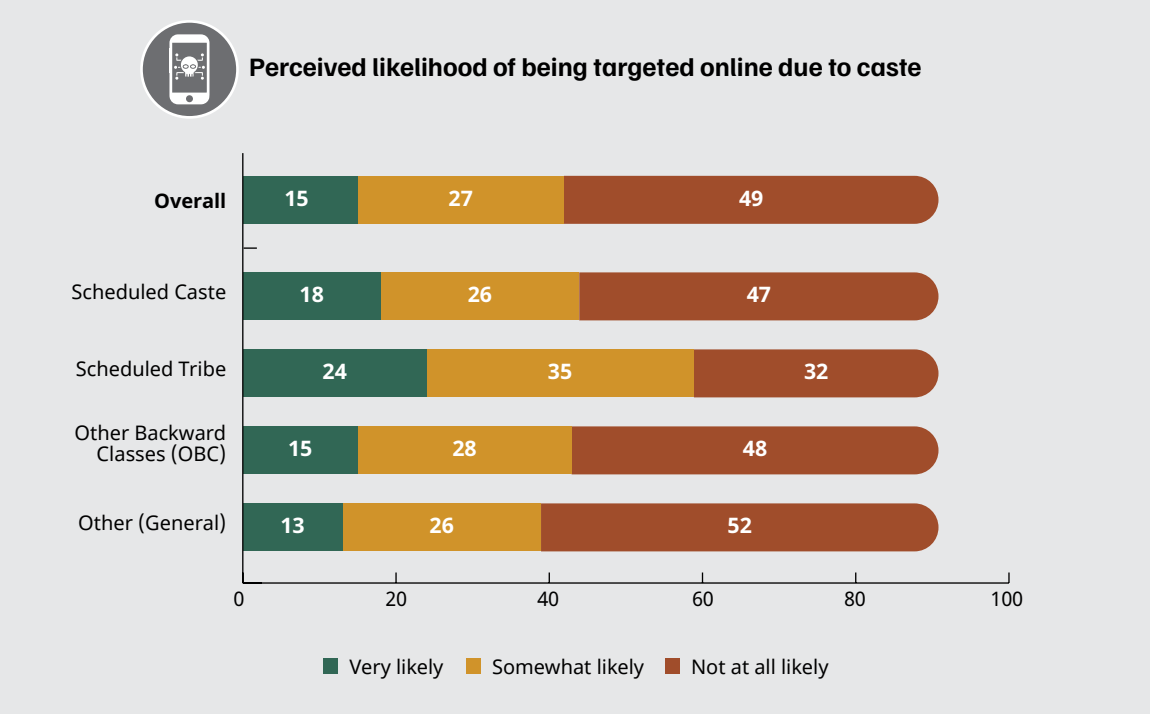
There are increasing trends of identity-based cybercrimes, particularly non-financial cybercrimes such as cyberbullying and hate speech in the recent years. To capture this, respondents were asked whether they felt vulnerable to being targeted online due to their religion or caste.

Figure 3.8: Women feel significantly more vulnerable to gender-based online targeting than men



Note: All figures are in percentages. Rest did not respond.
Question asked: "Compared to others, how likely are you to be targeted online because of your gender?"

Figure 3.9: Scheduled Tribes report being most vulnerable to caste-based online targeting



Note: All figures are in percentages. Rest did not respond.
Question asked: "Compared to others, how likely are you to be targeted online because of your caste?"

Religion does not appear to be widely perceived as a major basis for online targeting. Across religions, nearly half of the respondents feel that they are "not at all" likely to be targeted because of their religion, while about one in seven (15%) feel strongly vulnerable. Patterns remain broadly similar across religious categories, with relatively limited variation between groups.

Similarly, there is not a lot of variation across caste categories on the question of whether they feel vulnerable to being attacked online due to their caste. About half of all respondents or roughly one in two, feel that they are not at all likely to be targeted because of their caste identity (**Figure 3.9**). However, an outlier to this trend are respondents from Scheduled Tribes background. Among this group, 35 percent felt at least somewhat targeted, and about one-fourth (24%) felt very likely to be targeted online because of their caste identity. Scheduled Castes also show elevated concern (18% said "very likely") as compared to the general category respondents (13% said "very likely").

At the national level, being targeted on the basis of regional identity appears relatively low (**Table 3.3**). About half of the respondents (47%) say they are not at all likely to be targeted because of their regional identity. The most prominent finding emerges from Tamil Nadu, where perceptions are dramatically higher: 40 percent of the respondents report feeling at least somewhat targeted, and over one in three (34%) feel this very strongly. A similar, though less extreme pattern is visible in Bihar and Gujarat, where a sizable proportion of the respondents report some level of perceived targeting (71% and 57% - 'very likely' and 'somewhat likely' combined). In contrast, respondents from Delhi, Haryana and West Bengal are considerably less likely to perceive such risks, with roughly two-thirds reporting that they are "not at all" likely to be targeted online because of their regional identity (68%, 67% and 65% - 'very likely' and 'somewhat likely' combined).

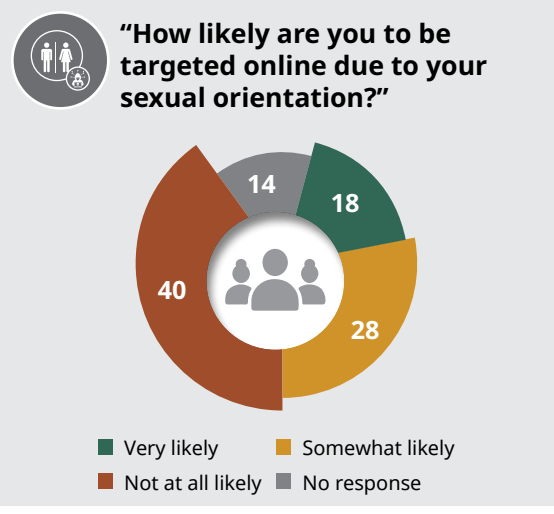
As highlighted in **Figure 3.10,** about four in ten respondents feel that they are "not at all likely"

Table 3.3: Tamil Nadu stands out with the highest perceived online regional targeting

State	Perceived likelihood of being targeted online due to regional identity		
	Very likely	Somewhat likely	Not at all likely
Overall	**13**	**30**	**47**
Tamil Nadu	34	40	24
Bihar	27	44	25
Rajasthan	19	24	48
Madhya Pradesh	18	25	49
Gujarat	17	40	19
Jharkhand	16	37	43
Karnataka	12	44	35
Uttar Pradesh	12	35	42
Haryana	9	19	67
Kerala	9	27	61
Telangana	9	14	48
Delhi	7	20	68
Odisha	6	46	42
Assam	5	16	63
Maharashtra	5	30	55
West Bengal	5	18	65

Note: All figures are in percentages. Rest did not respond.
Question asked: "Compared to others, how likely are you to be targeted online because of your regional identity?"

Figure 3.10: Nearly one in five respondents feel they are very likely to be targeted online due to their sexual orientation



Note: All figures are in percentages.
Question asked: "Compared to others, how likely are you to be targeted online because of your sexual orientation?"

to be targeted based on sexual orientation. Nearly one in five respondents (18%) said that they are "very likely" to be targeted online due to their sexual orientation, while another 28 percent felt that they are "somewhat likely" to be targeted.

3.4 The Perception of Rising Cybercrime

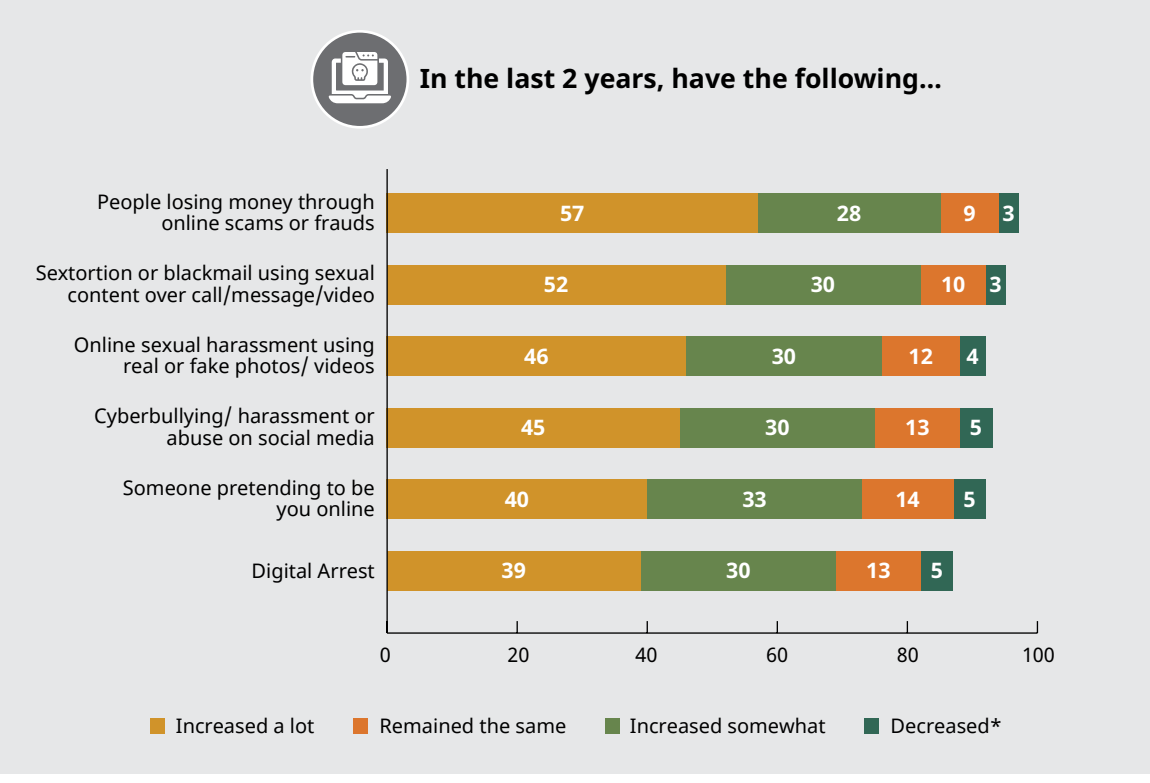
Trust in digital systems is shaped not only by personal experiences but also by the perceived threat posed by cybercrimes. Even individuals who have not directly experienced cybercrime victimisation may exhibit lower levels of trust if they believe cybercrimes are becoming more prevalent. Understanding whether the public perceives digital threats as increasing, decreasing or stabilising provides insight into the broader climate of digital confidence.

As highlighted in **Figure 3.11,** a majority of people perceive that digital threats have rapidly increased. Financial fraud stands out as the clearest example, with close to six in every ten respondents (57%) believing that people losing money through online scams has increased "a lot." Other forms of cyber harm are also widely seen as rising. More than half (52%) believe sextortion or blackmail using sexual content has increased "a lot". Around four in ten respondents report sharp increases in digital arrest scams (39%) and impersonation (40%). Similarly, nearly half perceive significant growth in online sexual harassment (46%) and cyberbullying (45%). Although these figures vary slightly across categories, the broader pattern is clear: substantial portions of the population see multiple forms of cyber harm expanding simultaneously. This pattern is consistent across both victims of cybercrimes as well as the overall respondents. Thus, actual experience with cybercrimes predictably reinforces the feeling that these crimes have increased significantly.

3.5 Conclusion

In sum, while digital technologies expand inclusion and opportunity, they also produce a pervasive sense of fragility. Trust in the digital environment appears conditional and cautious. Taken together, the findings reveal a layered crisis of digital trust. Exposure to scams is widespread and frequent; fear of financial and identity-related harms is high; many perceive that their age or gender increases their vulnerability; and a strong majority believe cyber threats are escalating. Digital participation, especially heavy online usage and use of digital payments, both empowers and unsettles citizens.

Figure 3.11: Online scams and sextortion or blackmailing cases are seen as rapidly growing threats



Note: All figures are in percentages. Rest did not respond.

**Option "Decreased" was a silent option.*

Question asked: "In your opinion, have the following increased a lot, increased somewhat, or remained the same, in the last two years – people losing money through online scams or frauds/ sextortion or blackmail using sexual content over call/message/ video/ online sexual harassment using real or fake photos/videos/ cyberbullying/harassment or abuse on social media/ someone pretending to be you online/ digital arrest?"

The digital ecosystem today is not experienced as uniformly secure. For many, routine exposure to fraudulent calls and messages has normalised the expectation of risk. Financial fraud, identity theft and privacy violations are viewed not as distant possibilities but recurring concerns embedded in everyday digital interaction. The emotional landscape of the digital sphere is therefore marked by vigilance: individuals remain connected and active, yet alert to the possibility of harm.

At the same time, respondents widely perceive cybercrimes to have increased in recent years. When citizens perceive threats as growing rather than stabilising, trust in digital systems becomes even more tentative. Digital inclusion has expanded opportunities, but it has also exposed individuals to new forms of insecurity. The challenge ahead lies not only in technological innovation but in rebuilding a sense of safety that matches the scale of digital transformation.

References

- Bopanna, D. (2025, September 12). Bengaluru woman loses ₹3.75 crore after falling for AI video of Sadhguru. *NDTV*. https://www.ndtv.com/bangalore-news/bengaluru-woman-loses-rs-3-75-crore-after-falling-for-ai-video-of-sadhguru-9262185
- Ghosh, D. (2025, September 13). Elderly man loses retirement savings of ₹1.8 crore in digital arrest fraud. *The Times of India*. https://timesofindia.indiatimes.com/city/kolkata/elderly-man-loses-retirement-savings-of-1-8-crore-in-digital-arrest-fraud/articleshow/123873890.cms
- The Hindu. (2026, February 28). Elderly man loses ₹76.65 lakh to cyber fraud. *The Hindu*. https://www.thehindu.com/news/national/karnataka/elderly-man-loses-7665-lakh-to-cyber-fraud/article70687435.ece
- Times News Network. (2025, September 13). Digital arrest scam: Retired BHEL supervisor loses ₹68 lakh. *The Times of India*. https://timesofindia.indiatimes.com/city/bhopal/digital-arrest-scam-retd-bhel-supervisor-loses-rs-68-lakh/articleshow/123858988.cms

CHAPTER

04

Eighteen people arrested for running fake call center (Noida, Uttar Pradesh - August 1, 2025).

Photo by Sunil Ghosh/Hindustan Times.

Mapping Cybercrime Experiences in India

Key Findings

- Thirteen percent of the respondents have been victims of cybercrimes in the last 2-3 years. Less educated and younger respondents are more likely to be victims of cybercrimes.
- More than half of all cybercrimes reported involve digital financial frauds. Eleven percent of the victims faced personal data theft, seven percent faced cyberbullying and four percent faced online sexual abuse. Respondents from upper class backgrounds and those who are more educated are more likely to face digital financial frauds.
- Almost a quarter of the digital financial fraud victims (23%) lost more than Rs. 20,000
- Nearly a third of the victims of digital financial fraud (31%) believe their personal financial data was leaked by a bank insider. Victims from a poor economic background are more likely to believe so.

Mapping Cybercrime Experiences in India

Cybercrime has emerged as one of the fastest-growing security challenges for the police. As digital payments, online banking, social media and e-governance continue to expand, so do opportunities for cybercriminal activities. Cybercrime is no longer limited to hacking and data theft; it has now broadened into diverse and more complicated offences like phishing, identity fraud, financial scams, ransomware, cyberstalking and even targeted attacks on other critical infrastructure. Reflecting on this evolving nature of cybercrime, the National Cybercrime Reporting Portal (NCRP) classified as many as 24 distinct types of cybercrime, as of April 2026 (Ministry of Home Affairs, n.d.).

This rapid expansion must also be understood alongside the increasing digital footprint of Indian citizens (refer to **chapter 7**). While greater access to smartphones and the internet has enabled crores of people to participate in the digital economy, it has also heightened the associated risk. For many users, as discussed in the previous chapter, their interactions with fraudulent calls, suspicious links, and scam messages have become increasingly normalised. Over time, this repeated exposure has contributed to a broader erosion of digital trust, where a sense of risk appears to have become a routine part of everyday online experiences. However, despite this widespread sense of vulnerability, the actual intensity and scale of cybercrime remain difficult to fully capture.

Available data, however, provides important insights into the extent of the problem. The National Crime Records Bureau's (NCRB) report, *Crime in India 2024,* shows a sharp and consistent rise in registered cybercrime cases over recent years. Registered cybercrime cases increased from 27,248 in 2018 to 44,735 in 2019, and from 50,035 cases in 2020 to 64,420 in 2023. In 2024, the number peaked at 1,01,928 cases. In the same report, fraud-related offences accounted for nearly 72.6 percent of all cybercrime cases (Manral, 2025; Singh, 2026). At the same time, broader estimates suggest that the true scale of the problem is even larger. Government data shows that cybersecurity incidents rose from 10.29 lakh in 2022 to 22.64 lakh in 2024 (Press Information Bureau, 2025). Another report emphasises that financial losses are mounting, with cyber fraud cases amounting to ₹36.45 lakh crore reported on the National Cybercrime Reporting Portal (NCRP) as of 28 February 2025 (Ministry of Home Affairs, 2025).

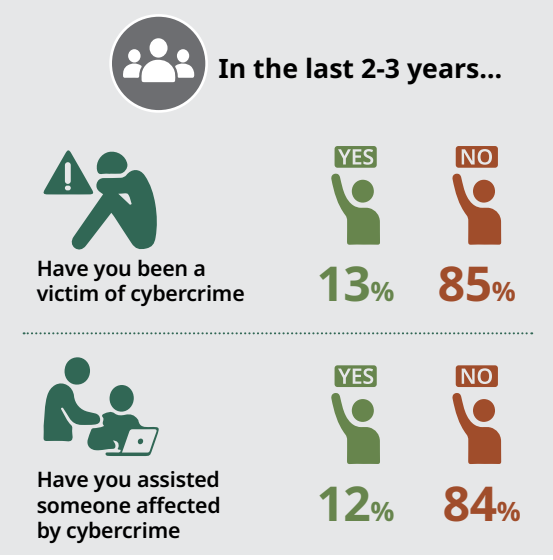
Given the scale and complexity of the issue, cybercrime in India demands closer and more systematic examination. With this background, this chapter seeks to assess the prevalence of cybercrime and examine how it affects different social groups. It also analyses various types of cyber offences and their occurrences, while examining the financial consequences faced by victims.

4.1 Understanding the Penetration of Cybercrime

While cybercrime has become increasingly pervasive, we need to look beyond reported cases to examine how frequently people encounter these threats in their everyday lives. To understand the experiences of victims of cybercrime, it is important to first understand the scale of its prevalence.

To examine this, the respondents were asked whether they had been a victim of cybercrime or had helped someone else who was a victim. The data shows that 13 percent of the respondents had been a victim of a cybercrime in the last two to three years (**Figure 4.1**). Among those who had not been victims, about 12 percent said they had helped someone deal with a cybercrime incident. Using the total number of victims and those who have assisted cybercrime victims, an index was created (for details, please refer to **index 7, Appendix 3**). The data from the index suggests that nearly one in four respondents (23%) have had some form of exposure to cybercrime.

Figure 4.1: Thirteen percent of the respondents have been victims of cybercrimes in the last 2-3 years



(N) cybercrime victims = 1085, and those who assisted cybercrime victims = 814

Note: The rest did not respond. All figures are in percentages.

Question asked: Have you been a victim of a cybercrime in the last 2-3 years? Did you help the victim closely in registering the cyber complaint or in handling the overall issue?

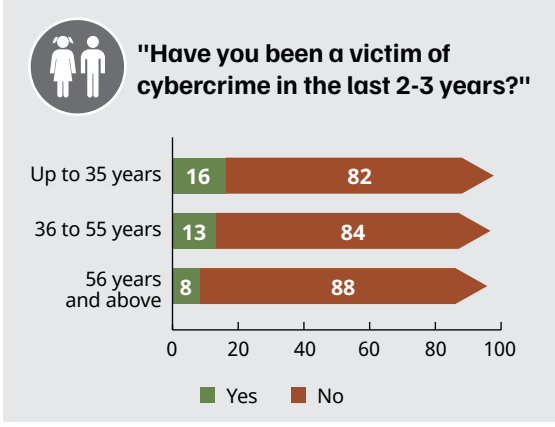
In the analysis of questions about experiences with the police, banks and courts, the responses of the victims, as well as those who have assisted victims of cybercrimes, have been merged, except where specified. This is because those who have assisted victims are also often familiar with the intimate details of the cybercrime incident.

Figure 4.2: Respondents without formal education are more likely to be the victims of cybercrime

Note: The rest did not respond. All figures are in percentages. Data presented is based solely on victim's responses.

An analysis across social demographics allows for a closer understanding of vulnerability to cybercrime. The data, as reflected in **Figure 4.2,** indicates only a marginal difference across different levels of education. It shows that respondents without any formal education (17%) are more likely to be the victims of cybercrime, while those with a college education and above are relatively less likely to be victims of cybercrime (13%).

Figure 4.3: Younger people are more vulnerable to cybercrimes



Note: The rest did not respond. All figures are in percentages. Data is from victims only.

Contrary to common assumptions, older people may not necessarily be more vulnerable to cyber-attacks. The data shows some variation across age groups, with the highest victimisation among younger age groups. Those less than 35 years of age are twice as likely to be victims of cybercrimes than those who are above 56 years of age (**Figure 4.3**). Over the past 2–3 years, 16 percent of respondents aged 18–35 years and 13 percent of those aged 36–55 years reported being victims of cybercrime, compared to just eight percent among respondents aged 56 years and above. This trend is more likely to be aligned with greater reliance on digital platforms like social media and UPI among younger age groups. At the same time, older individuals tend to use digital services less frequently (Please refer to **chapter 7**).

The data on cybercrime victimisation was also analysed across different economic classes and the gender of the victims, and no significant pattern was observed.

Across states, different patterns emerge. As shown in **Table 4.1,** survey data shows that Bihar (42%) has the highest reporting of digital crime amongst all states, followed by Rajasthan (29%), Telangana (22%), Delhi (20%) and Haryana (18%). Amongst the states with the lowest reporting are Uttar Pradesh (5%), Madhya Pradesh (4%), and Kerala, Karnataka and Assam (3%, each). Official figures reported in the table alongside show the rate of crime, which refers to the rate of incidents per one lakh of population. According to the National Crime Records Bureau (2024), Telangana (71.1) had the highest rate of crime, followed by Karnataka (32.2) and Kerala (8.2). The lowest rate of cybercrime was observed in Madhya Pradesh (1.2), Assam (1.1) and West Bengal (0.3).

Table 4.1: Cybercrime prevalence across different states

State	Victims (%)	Rate of crime* (Official NCRB report 2024)
Bihar	42	4.9
Rajasthan	29	1.9
Telangana	22	71.1
Delhi	20	1.8
Haryana	18	5.9
Odisha	17	5.4
Maharashtra	16	7.8
Gujarat	11	2.2
West Bengal	9	0.3
Tamil Nadu	7	7.5
Jharkhand	7	3.5
Uttar Pradesh	5	4.6
Madhya Pradesh	4	1.2
Kerala	3	8.2
Karnataka	3	32.2
Assam	3	1.1

**The rate of crime is the incidence of cybercrime per one lakh of population.*
Note: The figures here are from victims' responses.
Question asked: Have you been a victim of a cybercrime in the last 2-3 years?

4.2 Nature of Cybercrime

The expansion of digital platforms in recent times has created more areas for criminal activities. As spaces that were previously not digitised have moved online, opportunities for cybercriminals to exploit this growth have also increased. Cybercrime has evolved to tap into vulnerabilities from all dimensions. The methods through which a particular vulnerability is exploited are numerous: phishing, scam calls, exploiting verification processes, SIM swaps, malware and countless more. To contextualise the nature of cybercrimes, they can be broadly classified on the basis of occurrence and the nature of damage it has done.

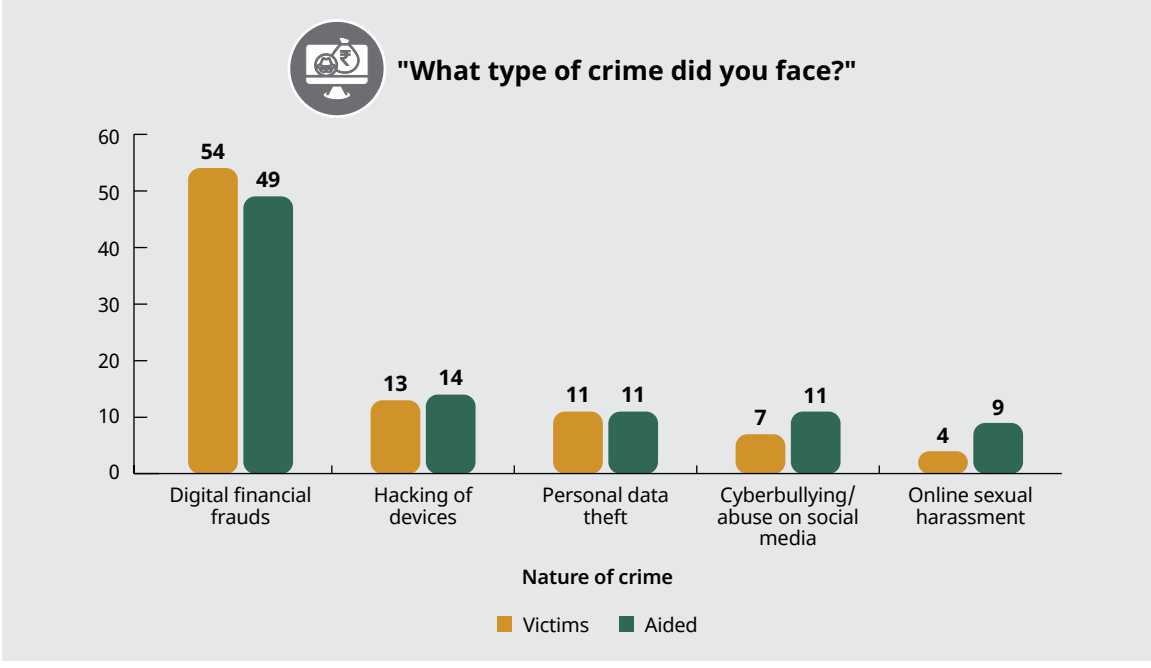
Digital financial fraud is the most prevalent type of cybercrime, as per the official statistics (CJP Team, 2025). Even in the current study, more than half of the victims (54%) experienced financial fraud. Among those who had closely aided a victim, 49 percent are affected by financial fraud. Hacking of devices and personal data theft are the second and third most frequent types of cybercrimes, with 13 percent and 11 percent of the victims being affected by either, respectively.

Cyberbullying, or harassment on social media, which includes threats, abuse, and general harassment, is prevalent across social media and makes up seven percent of cybercrimes. People who have aided victims report a slightly higher proportion (11%). Online sexual harassment is another type of crime that has major repercussions for the victim, but remains under-reported because of the social stigma attached to it. Four percent of the total victims reported being victims of this crime. A higher proportion (9%) reported having aided a victim of online sexual harassment (**Figure 4.4**).

Experts of cybercrimes pointed out that even though non-financial cybercrimes may be widespread, the reporting of such cases is significantly lower compared to financial cybercrimes, owing to, among other factors, the social stigma attached to them (see **Chapter 1** for more details).

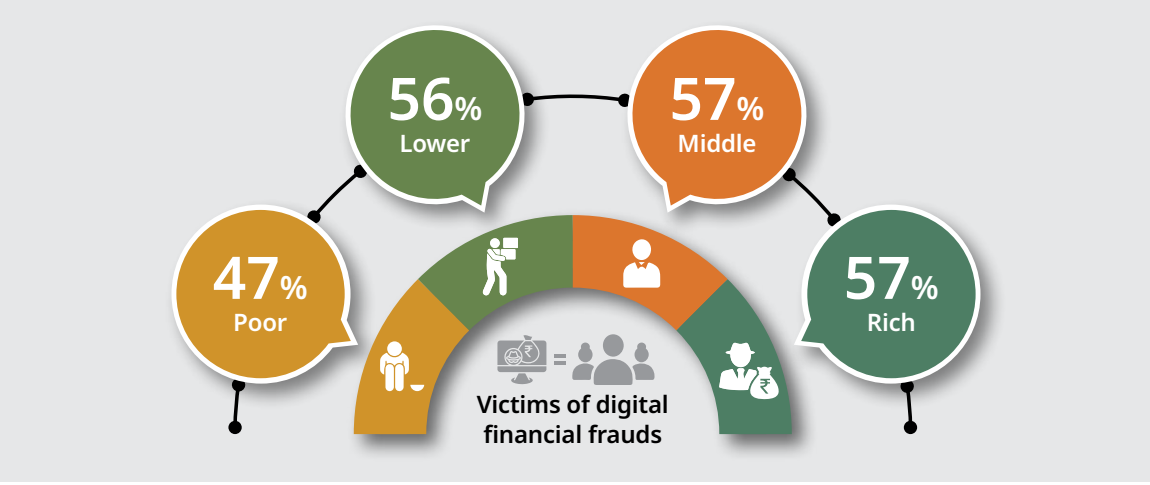
It is assumed that digital crimes might cross the boundaries of social and economic divisions and affect individuals equally. To verify this assumption, we checked the intersection between social groups and digital financial fraud.

Figure 4.4: More than half of all cybercrimes involve digital financial frauds



Note: The rest did not respond or reported facing other types of crime. All figures are in percentages.
Question asked: What type of crime did you face?

Figure 4.5: Rich respondents are more likely to be victims of digital financial frauds

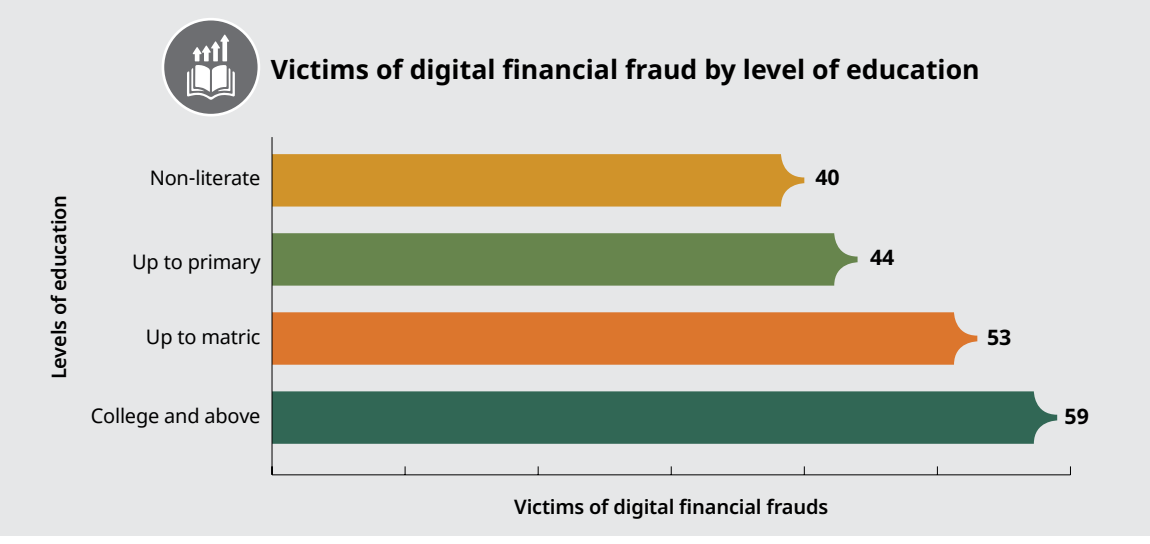


Note: The figures here only represent the analysis of digital financial fraud. All figures are in percentages. The figures here are from victims' responses only.

A closer look at the nature of crimes among different economic classes can help us understand these vulnerabilities better. Data suggest that rich people are more vulnerable to crimes like financial fraud. Fifty-seven percent of the rich respondents were victims of financial fraud compared to 47 percent of the economically disadvantaged respondents (**Figure 4.5**). Although the data suggests that there is less vulnerability among economically disadvantaged respondents, it is still important to note that nearly half of them (47%) are victims of digital financial fraud.

When analysed through different levels of education, the findings show an interesting pattern. As shown in **Figure 4.6,** there is a consistent increase in the proportion of digital fraud victims as the level of education increases. Two in five of the respondents (40%) without any formal education are victims of financial fraud, as compared to nearly three in five (59%) college graduates. This is in contrast to the findings on the overall cybercrime victimisation across educational levels. As seen in **Figure 4.2,** while non-literate respondents are slightly more likely

Figure 4.6: More educated respondents are more likely to be victims of digital financial frauds



Note: The figures here only represent the analysis of digital financial fraud. All figures are in percentages. The figures here are from victims' responses only.

to be victims of overall cybercrimes, when we look at the figures of only those who have been victims of digital financial frauds (**Figure 4.6**), the trend reverses, with non-literates being the least likely to be victims of digital financial fraud, indicating that the lesser educated responses may be more likely to be victims of non-financial cybercrimes.

Analysis across age groups showed no pattern of age-related vulnerability to digital financial fraud. Moreover, there is no significant difference in the number of men and women who reported being victims of online sexual harassment.

4.3 Economic Impact of Digital Financial Fraud

As seen before, over half of all cybercrimes are financial crimes. Given the magnitude and growing sophistication of digital financial frauds, it is important to assess their economic impact.

When asked if there was any financial loss, about nine percent of the digital financial fraud victims said they faced no financial loss. In comparison, over eight in ten victims of digital financial fraud reported some type of financial loss. The findings reveal that nearly a quarter of the victims (23%) have faced losses upwards of 20,000 rupees. While eight percent have lost up to Rs. 1,000, another 25 percent have lost between Rs. 1,001- 5,000. Cumulatively, about 29 percent have lost between Rs. 5,000 and Rs. 20,000 (**Table 4.2**).

Table 4.2: A fourth of digital financial fraud victims lost more than Rs. 20,000

Amount of financial loss suffered	Digital financial fraud victims (%)
No financial loss*	9
Up to Rs. 1,000	8
Rs. 1,001 to 5000	25
Rs. 5,001 to 10,000	16
Rs. 10,001 to 20,000	13
Above Rs 20,000	23

N – Digital financial fraud victims (583)
Note: The rest did not respond. All figures are in percentages.
**Since not all digital fraud resulted in loss of money, some people have reported no financial loss*
Question asked: If there was a financial loss, how much was it?

The respondents who suffered a financial loss were further asked about the type of banks from which the funds were misappropriated. The data reveals that there is, more or less, an equal amount of fraud that has taken

Figure 4.7: Nearly one-third of victims of digital financial frauds believe their personal financial data was leaked by a bank insider

Note: All figures are in percentages. The data corresponds to the digital financial fraud victims and those who assisted them. For more information on the index, please refer to index 16 in Appendix 3.
Question asked: Some victims of financial cybercrimes believe that their financial data was leaked by a bank insider, because of which they were targeted by criminals. In your case, do you think the crime occurred due to a breach of your personal data?

place in government banks (43%) and private banks (42%), indicating that holders of both government and private bank accounts are almost equally likely to be victims of digital financial fraud.

Some victims of cybercrime believe that their financial data was leaked by a bank insider, because of which they were targeted by criminals. In qualitative interviews with victims and cybercrime experts, this opinion has emerged repeatedly (please see **Chapter 2** for more details). The Government of India confirmed 248 data breaches across commercial banks over a period of four years in 2022 (Government of India, 2025).

In this context, digital financial fraud victims were asked about their opinion on whether, as victims of cybercrime, they feel that their data was leaked by a bank insider. About a third of the digital financial fraud victims (31%) believe that their data was leaked, leading them to be vulnerable to digital financial fraud (**Figure 4.7**). In contrast, 45 percent opined that their data was not leaked. A fourth of the victims (24%) were not sure which of these was the case.

The data was also analysed among different economic classes. The findings show a downward trend in the suspicions of data leaks as the economic class improves. Over half of the rich victims (59%) said their data was not leaked, compared to over two-fifths among the most economically disadvantaged sections (44%) (**Table 4.3**). Among the lower-income class, 45 percent said the same, and among middle-income groups, the proportion is 47 percent. However, a third of the economically disadvantaged (33%), lower (34%) and middle-income (33%) groups believed that their personal data was leaked by a bank insider.

4.4 Conclusion

The findings in this chapter reveal the scale and nature of cybercrime victimisation in India and help understand the profiles of the victims and their experiences. Official reports already point to a rapid growth in the prevalence and sophistication of cybercrime, and there is a growing concern around security and enforcement measures. While 13 percent of respondents reported being direct victims of cybercrimes, nearly a quarter of the total respondents surveyed have either directly experienced cybercrime or have been closely involved in assisting a victim in the past two to three years.

Various social dimensions affect the predisposition of a victim to cybercrime, and the findings support the broader theory that social marginalisation produces greater victimisation. Respondents who were less educated or non-literate were slightly more likely to be victims of cybercrimes, while those who are 56 years of age and above were slightly less likely to be victims of cybercrimes compared to their younger

Table 4.3: Rich respondents were less likely to believe that their personal data was leaked by a bank insider

Economic class	Personal data was leaked by the bank insider	Personal data was not leaked by the bank insider
Poor	33	44
Lower	34	45
Middle	33	47
Rich	29	59

Note: The rest did not respond. All figures are in percentages. The figures are from the victims only.
Question asked: Some victims of financial cybercrimes believe that their financial data was leaked by a bank insider, because of which they were targeted by criminals. In your case, do you think the crime occurred due to a breach of your personal data?

counterparts. However, the trend changes when one looks at only the trends within digital financial fraud (which made up more than half of the cybercrime cases reported). Rich and more educated respondents were more likely to be victims of digital financial fraud, while all age groups of respondents are almost equally likely to become victims of digital financial fraud. The likelihood of overall cybercrime victimisation is highest amongst the non-literate and less educated respondents.

However, when it comes to digital financial frauds, the highly-educated respondents are the most likely to report victimisation. Notably, there is no significant difference across genders—both on questions of whether they were victims of cybercrime as well as on the question about the nature of cybercrimes. Both men and women are nearly equally likely to be victims of cybercrimes such as digital financial frauds as well as online sexual harassment.

Concerning patterns of financial loss, the data of this study reveal that over eight in ten digital financial fraud victims faced some form of financial loss. Perhaps the most telling is the finding that nearly a third of victims believed they were targeted because their data was leaked by the bank or a bank insider. This view is more prominent among economically weaker groups and women. Overall, these conditions do call for greater transparency, accountability, and responsiveness from banks in how they handle both data and victims.

References

- CJP Team. (2025). Counting crimes, discounting justice: The NCRB's statistical blind spots. *Sabrang India*. https://cjp.org.in/counting-crimes-discounting-justice-the-ncrbs-statistical-blind-spots/
- Government of India. (2025, December 2). *Data breaches in commercial banks* (Lok Sabha Unstarred Question No. 452). Ministry of Home Affairs. https://www.mha.gov.in/MHA1/Par2017/pdfs/par2025-pdfs/LS02122025/452.pdf
- Manral, M. S. (2025, September 30). NCRB report for 2023: Cybercrimes rise by over 30%, maximum cases linked to fraud. *The Indian Express*. https://indianexpress.com/article/india/ncrb-report-for-2023-cybercrimes-rise-by-31-2-maximum-cases-linked-to-fraud-10279119
- Ministry of Home Affairs, Government of India. (2025, March 12). *Cyber fraud and awareness* (Rajya Sabha Unstarred Question No. 1517). Sansad. https://sansad.in/getFile/annex/267/AU1517_X6pokO.pdf?source=pqars
- Ministry of Home Affairs. (n.d.). *Learn about cybercrime*. National Cybercrime Reporting Portal, Government of India. https://cybercrime.gov.in/Webform/CrimeCatDes.aspx
- National Crime Records Bureau. (2024). *Cybercrimes (State/UT-wise) – 2022–2024* (Table 9A.1). Ministry of Home Affairs, Government of India. https://www.ncrb.gov.in/uploads/files/TABLE9A12.pdf
- Press Information Bureau, Government of India. (2025, October 8). *Curbing cyber frauds in Digital India* [Press release]. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2176146&reg=3&lang=2
- Singh, V. (2026, May 7). Rise in cybercrime but overall crime rate dropped in 2024, says latest NCRB report. *The Hindu*. https://www.thehindu.com/news/national/rise-in-cybercrime-but-overall-crime-rate-dropped-in-2024-says-latest-ncrb-report/article70948292.ece

CHAPTER

05

A mundane view outside the Jamtara railway station (Jamtara, Jharkhand- November 19 2022).

Photo by Cameranest/Shutterstock.

Perceptions of Cybercrime Redressal Mechanisms

Key Findings

- About half of the respondents (51%) complained to the police after the cybercrime, while another 11 percent went to the police initially but did not pursue the case.
- Amongst the victims to who complained to the police, nearly a quarter of the victims visited the police station five times or more. Victims from rural areas were more likely to visit five times or more, compared to those from urban areas.
- A little over two in five victims who complained to the police found the complaint registration process to be difficult, with 17 percent finding it 'very difficult' and 25 percent saying that it was 'somewhat difficult'.
- More than a quarter of the respondents (27%) who got their police complaint registered paid a bribe to the police. Poor victims are nearly four times most likely to pay bribe to the police, compared to the rich.
- Victims who paid a bribe to the police were three times more likely to recover the full amount lost, compared to those who did not pay a bribe.
- More than a third of the victims contacted their personal network so that the police would deal with the case properly. Victims who approached the police through a personal network were three times more likely to recover the full amount lost in cybercrime than those who did not contact anyone.

Perceptions of Cybercrime Redressal Mechanisms

Cybercrime has become a significant challenge for individuals, institutions and law enforcement alike. The concern is not just because of the variety of offences involved, but also about the nature and process of redressal. In India, the response system has expanded through the National Cybercrime Reporting Portal (NCRP), which allows citizens to report from a wide range of cyber offences (covering up to 24 different types of offences as of April 2026, Ministry of Home Affairs, Government of India, n.d.). It also allows citizens to track complaints through an online mechanism, along with the helpline '1930' for financial fraud cases. NCRP is part of the larger Indian Cyber Crime Coordination Centre (I4C) initiative by the Ministry of Home Affairs, which aims to deal with cybercrimes in the country in a coordinated and comprehensive manner. However, the existence of a reporting platform does not necessarily translate into justice, as victims have to navigate through many systems for registration and resolution of complaints, which is neither clearly structured nor well-coordinated (**see chapters 1 and 2**).

Existing global literature shows that cybercrime-related challenges are not unique to India, and they reflect larger systemic limitations. For instance, studies from England and Wales suggest that police agencies have been ill-equipped to address cyber threats (Lee et al., 2025) and that the majority of the police officers lack the necessary training or expertise to respond effectively to cybercrimes (Curtis & Oxburgh, 2022). In some contexts, police officers also report that the internet and the advent of cybercrime have made their jobs more difficult (Lee et al., 2019).

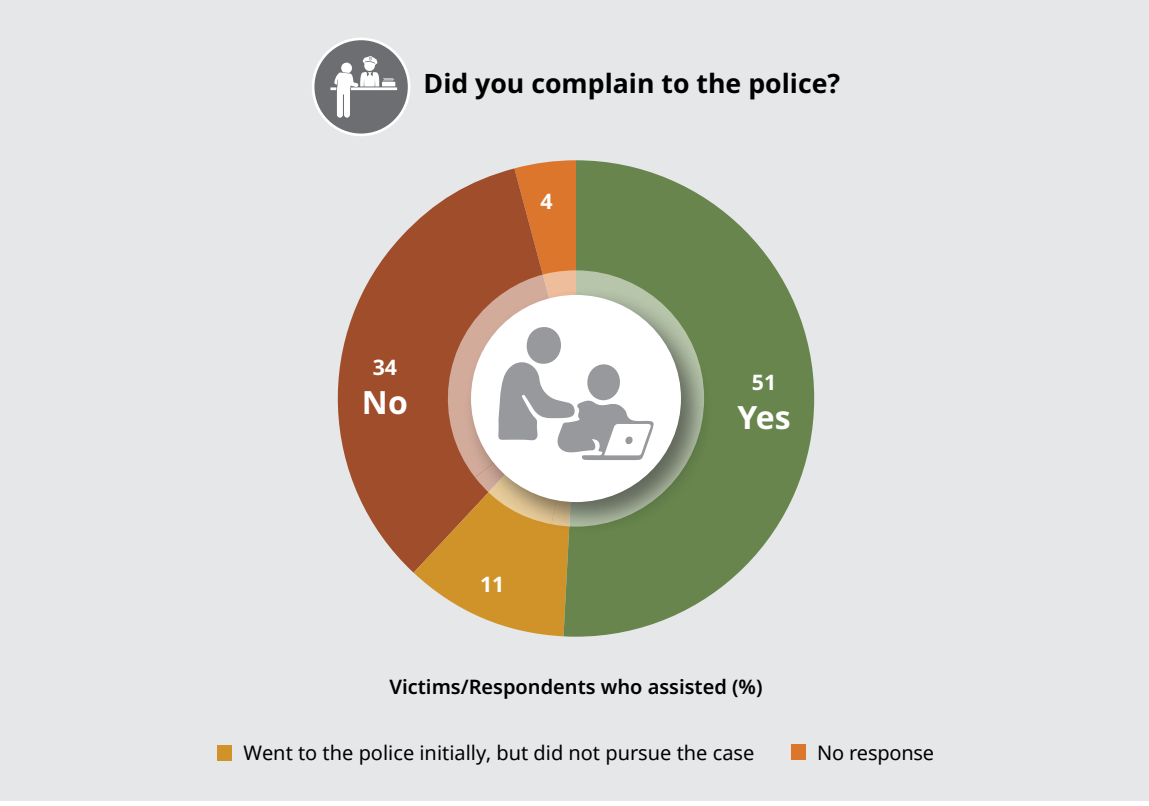
Similar patterns are evident in the Indian context, where Gupta and Singh (2025) identify a significant gap in technical expertise among the law enforcement personnel. The same study argues that due to the evolving nature of cybercrimes, there is a need for continuous education and training. A project report on capacity building at the police station level in cybercrime investigation by the National Police Commission from 2016 to 2017 also reports a shortage of trained cyber investigators, very few forensic facilities, and delays in receiving reports due to backlog (Bureau of Police Research and Development, n.d.).

While a growing body of literature focuses on institutional and capacity-related gaps, there remains a dearth of literature on how the victims actually perceive and navigate the process of seeking redressal from law enforcement authorities.

Against this background, the current chapter aims to understand how the victims of cybercrime, or those who assisted them through the complaint process, engage with redressal mechanisms and, in the process, interact with various official platforms such as the police, cyber cells and the courts. Further, it explores the entire cybercrime reporting process, from the initial decision of making a complaint to the police (or not), to registering an FIR, and thereafter various types of interaction with the police and, where applicable, the progression of cases within the courts. The chapter unfolds the hardships involved, including the intensity of time and efforts expended by victims, their perceived fears and instances of corruption, if any.

Beyond the procedure, the chapter also examines the quality of institutional response through measures of perceived satisfaction with the entire process, including police helpline numbers, online portals, the complaint registration system, and the court process.

Figure 5.1: About half of the respondents complained to the police after the cybercrime



Note: The figure includes responses from both the victims and those who assisted cybercrime victims.
Question asked: Did you complain to the police?

In doing so, the study recognises that satisfaction is as much shaped by timelines and transparency as by the treatment by authorities and the final legal outcome. Overall, the findings from cybercrime victims and governance-related perceptions aim to inform methods that may ultimately strengthen trust and encourage more effective reporting.

5.1 Initial Response to Cybercrime

Lodging a complaint with the police is a crucial step in seeking redressal. Filing a formal complaint involves visiting a police station or cyber cell, providing a detailed account of the incident, and submitting relevant evidence.

To understand this process, the victims and those who assisted cybercrime victims were asked whether they made a complaint to the police station. It is important to note that 13 percent of the respondents were victims, and among the non-victims, about 12 percent have helped someone deal with a cybercrime. It is these respondents who were queried about whether they made a complaint to the police station. Throughout the chapter, the responses of both the victims and those who assisted the victims have been merged, except where otherwise specified.

Over half of the victims of cybercrimes (51%) reported that they had complained to the police, while 11 percent went to the police initially but did not pursue the case (**Figure 5.1**). Over one-third (34%) did not complain to the police.

It was found that victims in rural areas (55%) were more likely to complain to the police than those living in urban areas (48%) (**Table 5.1**). Although the proportion of those who went to the police but did not pursue the case is more or less comparable between rural (11%) and urban (9%) areas, overall, about two in every three rural victims (66%) visited the police station to complain, compared to about six in ten (57%) among the urban victims.

Table 5.1: Victims in rural areas were more likely to report cybercrime to the police

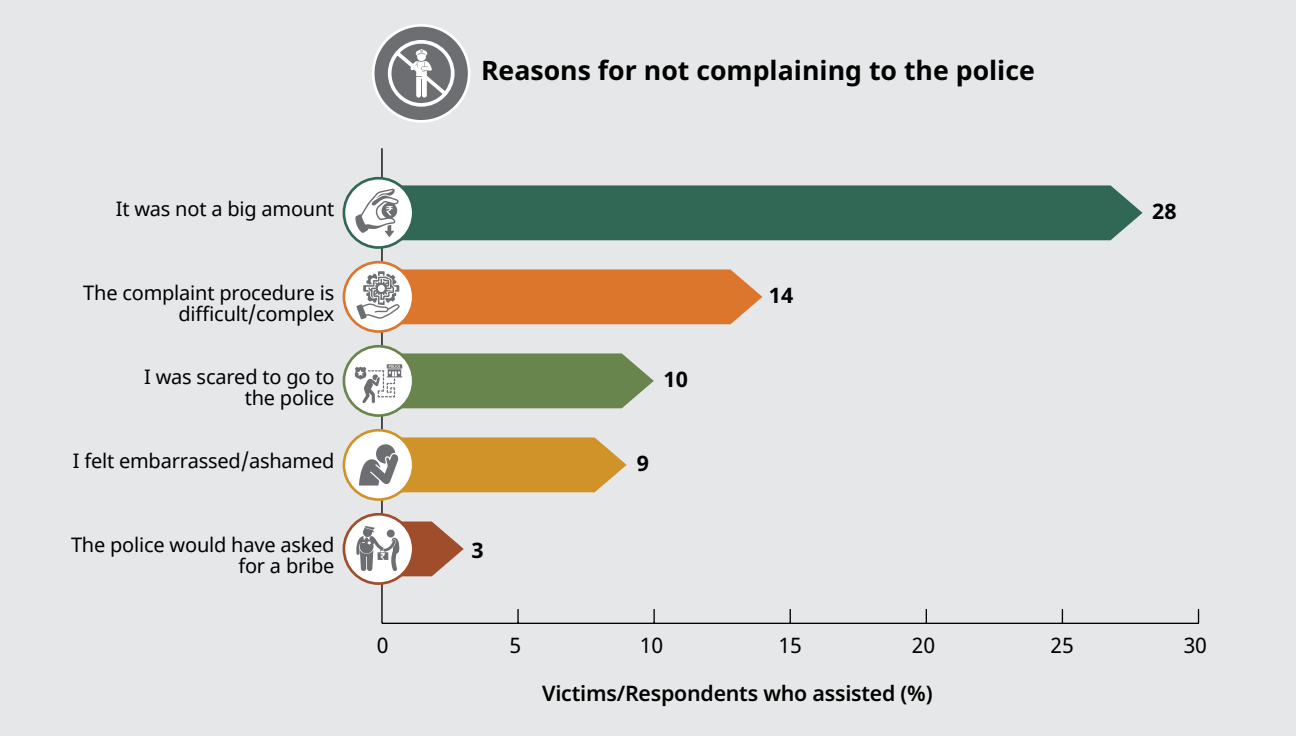
Locality	Overall proportion of victims	Complained to the police		
		Yes	Went to the police initially, but did not pursue the case	No
Rural	12	55	11	32
Urban	13	48	9	41

Note: The rest did not respond. The table includes responses from only the victims. All figures in percentages.
Question asked: Did you complain to the police?

Overall, a third of the respondents (34% of both the victims and those who assisted them) did not complain to the police (**Figure 5.1**). When asked why, more than a quarter (28%) said that it was because the amount was not big (**Figure 5.2**). About one in seven (14% of both the victims and those who helped/aided them) also reported that the complaint procedure is difficult or complex for them and that's why they didn't complain to the police. Ten percent of the victims/those who aided victims said that they were scared to visit the police station, and another nine percent said that they were embarrassed/ashamed. Three percent of the victims and those who aided victims said that they thought they would be asked for a bribe if they complained to the police, which is why they did not file a complaint with the police.

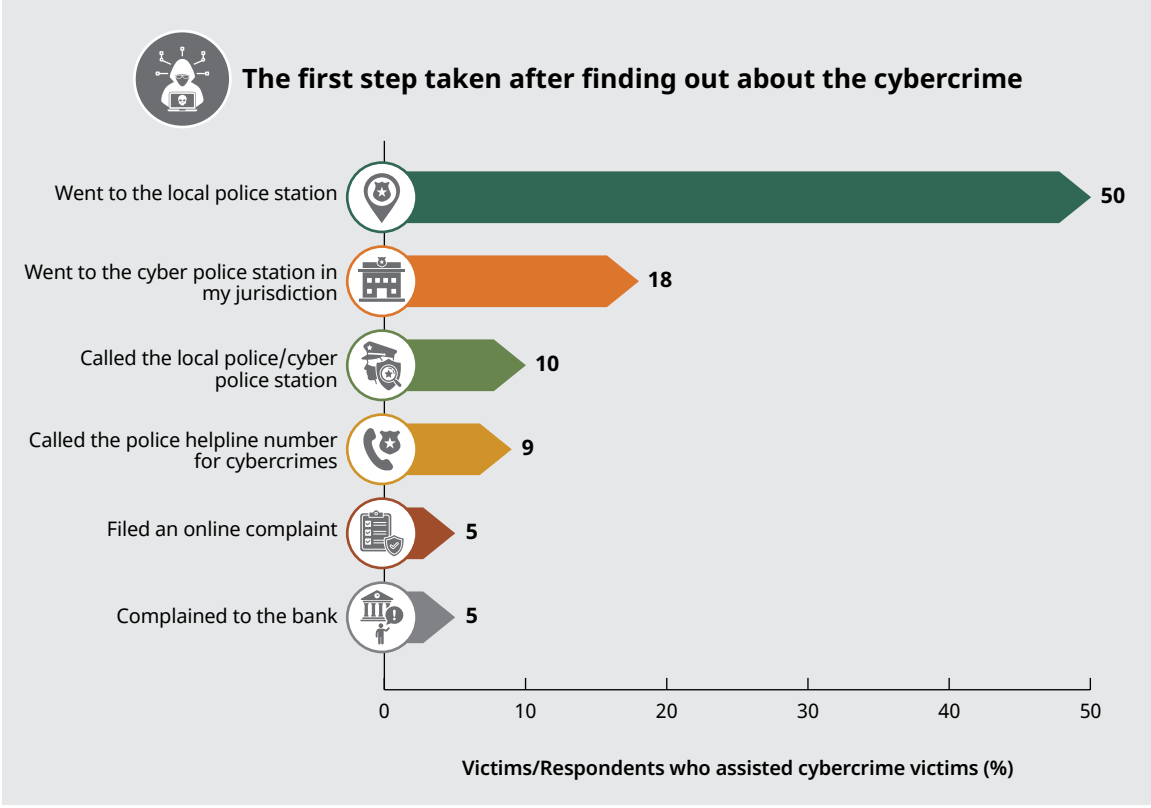
When people first realise they have been victims of a cybercrime, their first response is often shaped by a mix of urgency, confusion and fear.

Figure 5.2: More than a quarter of the victims did not report cybercrime because the amount lost was not substantial



Note: The rest either said other reasons or did not respond. The table includes responses from both the victims and those who assisted cybercrime victims.
Question asked: Why did you not complain to the police?

Figure 5.3: Half of the respondents went to the local police station after finding out about the cybercrime



Note: The rest either said other reasons or did not respond. The table includes responses from both the victims and those who assisted cybercrime victims. The responses here include only those who complained to the police or went to the police but did not pursue the case.
Question asked: What was the first step you took when you found out about the cybercrime?

In the case of financial fraud, while they may initially attempt to secure their accounts by changing passwords, blocking cards, contacting the bank or seeking informal advice (from family/friends), the recognition of personal or financial harm often compels them to engage with institutional mechanisms.

To better understand the initial mode of reporting, both the victims of cybercrimes and those who aided victims were queried. It is important to note that this question was asked of only those who filed a complaint with the police. Data shows that half of them (50%) went directly to the local police station as their first step, and about one in five (18%) went to the local cyber police station/unit within their jurisdiction (**Figure 5.3**). About one in ten (9%) called the police helpline number for cybercrimes, and a similar proportion (10%) called the local police station or cybercrime unit. The other five percent made an online complaint, and a similar proportion (5%) made a complaint to the bank.

5.2 Procedural Aspects of Accessing Police Services

Apart from the complaint process, interaction with the police shapes the victims' experiences of seeking redressal. However, this interaction is not always straightforward, as it may be influenced by a host of factors. These can include the time and effort required to engage with formal procedures, as well as situations that arise during the course of reporting and follow-up. To understand the victims' overall experience of the interaction with the police, it is important to understand how victims navigate through these processes.

Respondents were asked whether they had physically visited the police station. The data shows that half of them (50%) visited the local police station in person.

Table 5.2: Half of the respondents went to the local police station in person

Went to these places in person...	Victims/Respondent who assisted (%)
The local police station	50
The cyber police station/cell	26
Both the local police station and the cyber cell	10
Did not need to go	10

Note: The rest did not respond. The table includes responses from both the victims and those who assisted cybercrime victims.
Question asked: Did you need to go to the police station in person?

A little over a quarter (26%) visited the cyber police station/cell. One in ten (10%) visited both the local police station and the cyber cell, and a similar proportion (10%) said that they did not need to go (**Table 5.2**).

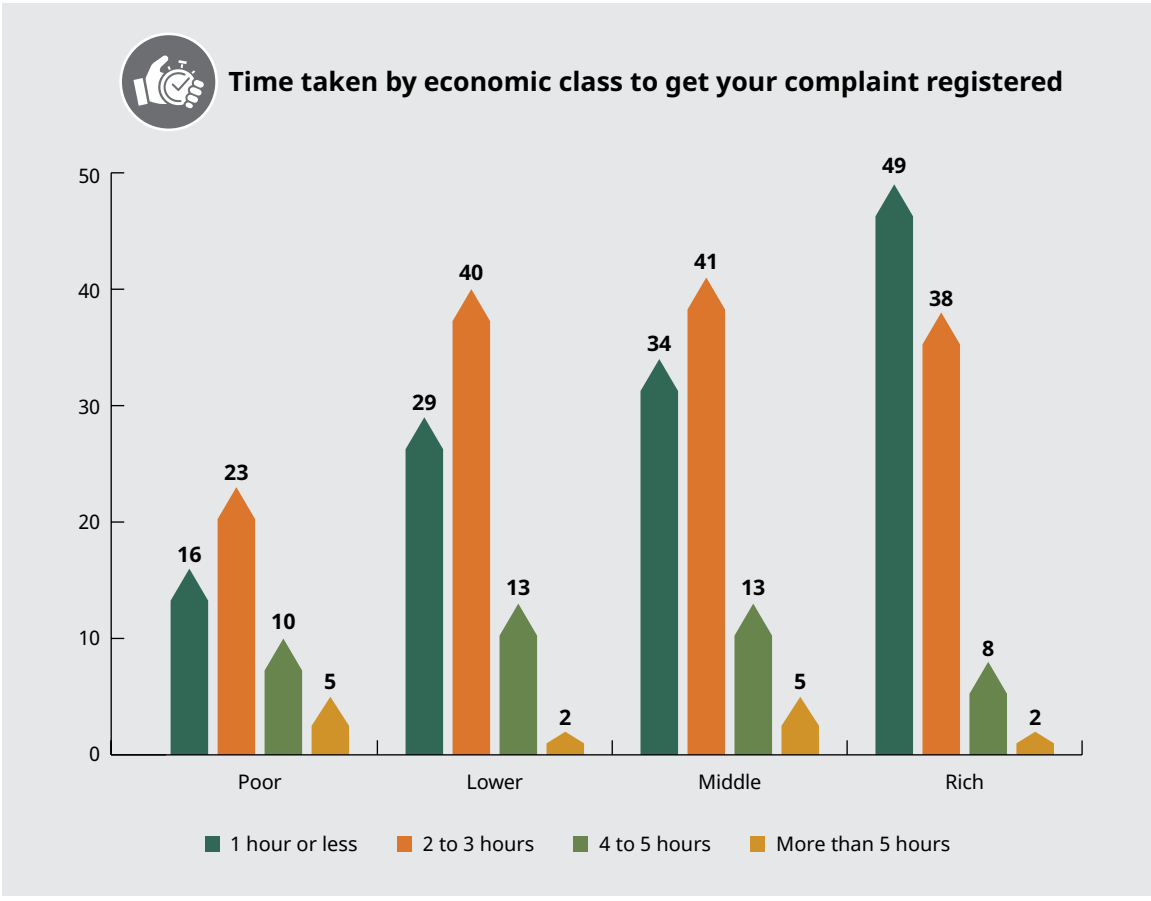
The victims as well as those assisting the cybercrime victims who visited the police station were further queried about how long they had to wait and the number of visits required to get their complaint registered. About one-third of the them (30%) said that they waited for up to an hour, and about half said that they waited for two to three hours (45%). One in ten (10%) waited for four to five hours and three percent had to wait for more than five hours (**Figure 5.4**).

The data, when analysed by economic class, shows an interesting pattern. Among the respondents from the rich economic group,

Figure 5.4: About a third of the victims waited for up to an hour to get their complaint registered

Note: The rest did not respond. The table includes responses from both the victims and those who assisted cybercrime victims.
Question asked: How long did you have to wait at the police station to get your complaint registered?

Figure 5.5: Rich victims reported shorter waiting times at police stations



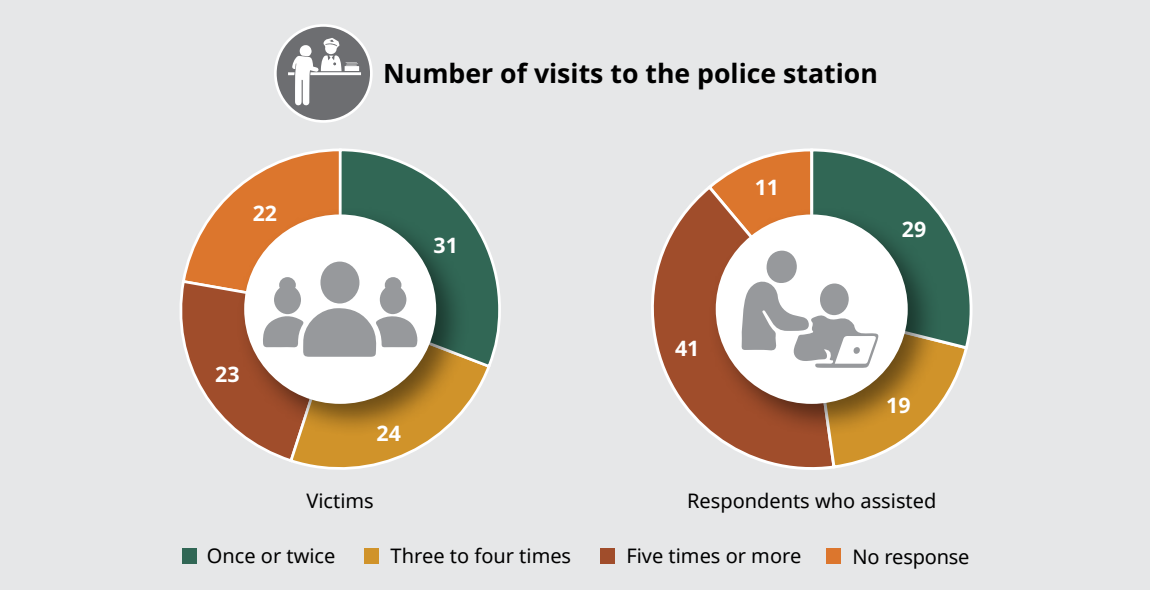
Note: The rest did not respond. The table includes responses only from the victims. All figures in percentages.
Question asked: How long did you have to wait at the police station to get your complaint registered?

about half of the respondents reported waiting for an hour or less (49%), while amongst the middle class, about one-third reported waiting for less than an hour (34%) and amongst the lower class, the figure was even lower, at 29 percent (**Figure 5.5**). The proportion is the lowest among the economically disadvantaged, wherein only 16 percent waited for up to an hour. On the other hand, the poor, lower and middle classes are slightly more likely to have a waiting time of 4-5 hours, compared to those from rich backgrounds. However, it must be noted that a little less than half of the respondents from poor economic backgrounds (46%) who visited the police station did not answer the question and the figures above only comprise 54 percent of those who reported their waiting times.

The respondents who went to the police station were also asked about how many times they had to visit the local cyber cell or the police station during the investigation process. About one in three (31%) of the victims and 29 percent of those who assisted the victims said they only had to visit once or twice (**Figure 5.6**). About a quarter of the victims (24%) and one-fifth (19%) of those who assisted the victims visited three or four times. About a quarter of the victims (23%) had to visit five times or more, and this proportion was relatively higher among those who assisted cybercrime victims (41%).

As emerging from the in-depth interviews with victims, visits to police station also has an added cost of losing income for many low-income victims and daily-wage workers (see **Chapter 1** for more details). Thus, this finding reveals the added procedural burden on the victim, which could be a major factor in the non-reporting of cybercrime cases, particularly of smaller amounts.

Figure 5.6: Nearly a quarter of the victims visited the police station five times or more



Note: All figures in percentages.
Question asked: How many times did you have to visit the police station (local/cyber) during the investigation process?

Table 5.3: Victims in rural areas were twice as likely to make five or more visits to the police station

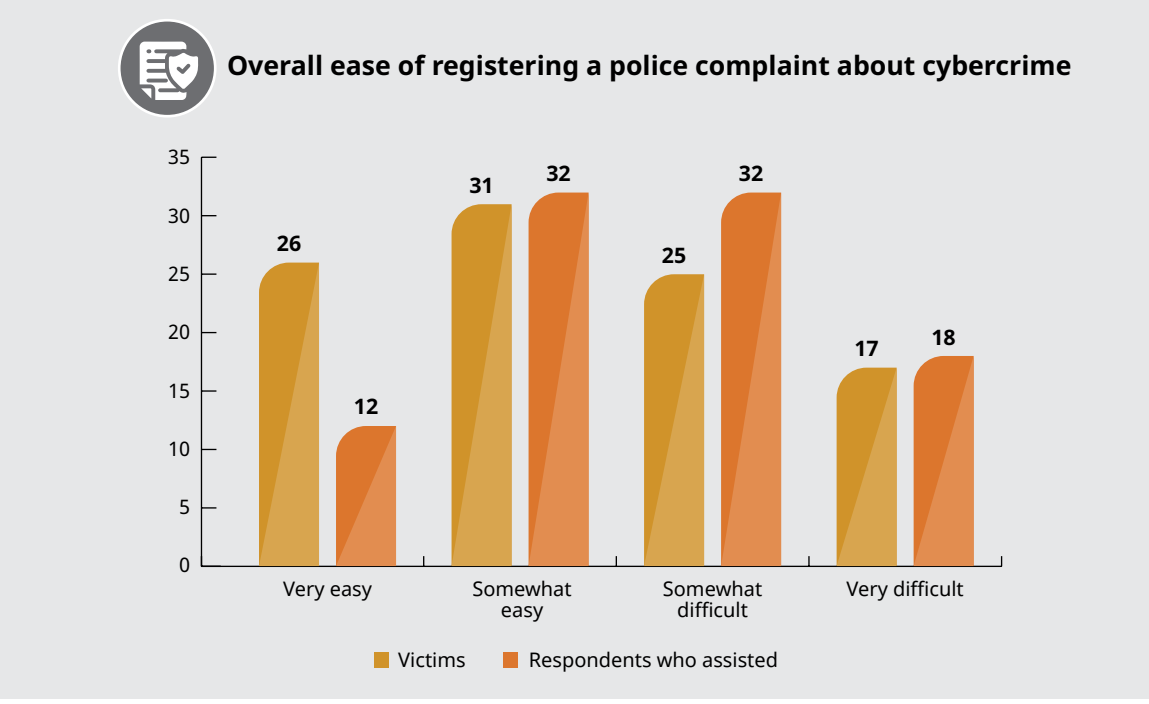
Locality	Number of visits to the police station		
	Once or twice	Three to four times	Five times or more
Rural	20	18	38
Urban	34	26	19

Note: The rest did not respond. The table includes responses only from the victims. All figures in percentages.
Question asked: How many times did you have to visit the police station (local/cyber) during the investigation process?

The data further shows that victims in rural areas reported a higher incidence of five or more visits to the police station (38%) compared to those residing in urban areas (19%) (**Table 5.3**). In contrast, over one-third (34%) of the victims in urban areas visited once or twice, as compared to about one-fifth (20%) of those in rural areas.

Apart from the number of visits and time consumed in the investigation process, the respondents were also asked to rate the overall ease of registering a complaint about cybercrime. Over half of the victims found the process easy, with a quarter saying it was "very easy" (26%), and 31 percent said it was "somewhat easy" (**Figure 5.7**). Among those who helped the cybercrime victims, more than two in five (44%) found the process of registering a complaint to be easy, with 12 percent saying the process was "very easy", and 32 percent saying the process was "somewhat easy". From the findings, it appears that victims were more likely to find the process to be easy than those who aided cybercrime victims. On the other hand, over two in five victims found the process to be difficult (42% combining "very difficult" – 17% and "somewhat difficult" – 25%), as compared to half among those who helped the cybercrime victims (50% combining "very difficult" – 18% and "somewhat difficult" – 32%).

Figure 5.7: Nearly one in five victims found registering a complaint very difficult



Note: The rest did not respond. All figures in percentages.
Question asked: Overall, how easy or difficult was it to register a police complaint about the cybercrime – very easy, somewhat easy, somewhat difficult, or very difficult?

The data was analysed across different social demographics. The categories of 'very easy' and "somewhat easy" were merged to form "easy", and "very difficult" and "somewhat difficult" were merged to form "difficult." The data shows that victims in urban areas were relatively more likely to report the process as difficult, compared to those in rural areas (42% versus 39%, respectively), whereas three in five victims in rural areas (60%) said the process was easy (**Table 5.4**). This could be a contributing factor in the relatively higher reporting of cybercrime cases in rural areas, compared to urban areas, as seen in **Table 5.1** above.

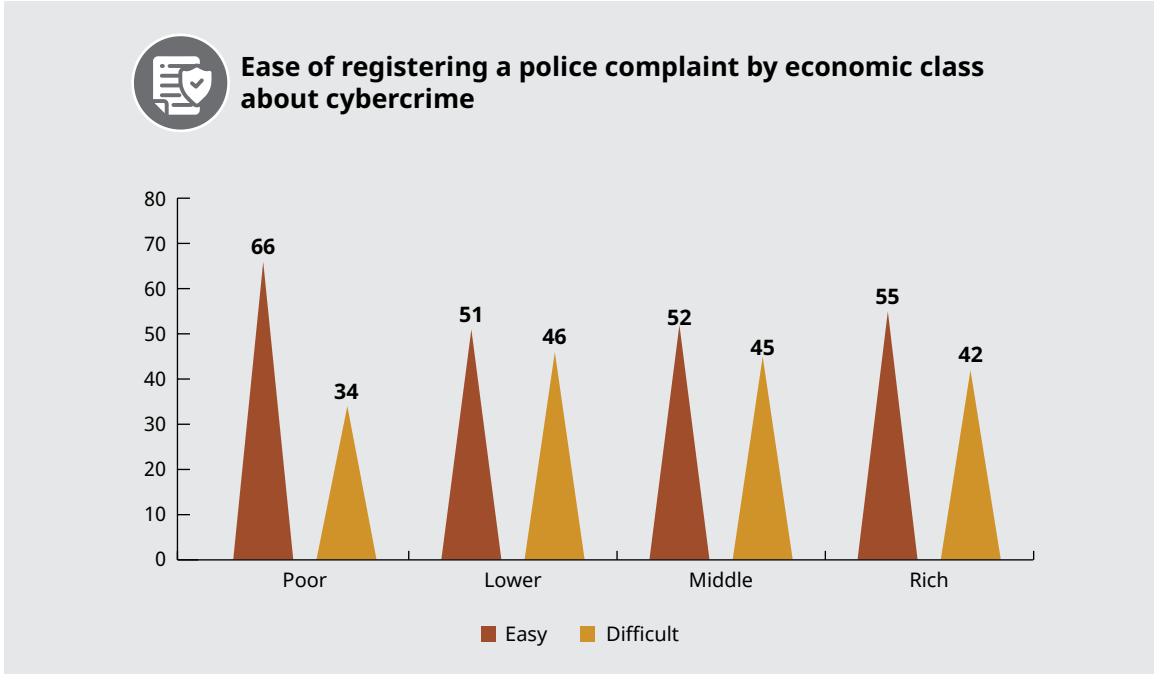
In terms of economic class, two in three of the economically disadvantaged respondents (66%) said the process was easy, the highest among all income groups, while those in the lower income category (46%), middle income category (45%) and the affluent group (42%) were relatively more likely to report difficulty (**Figure 5.8**). Across genders, women respondents were more likely to rate the process easier than men (61% and 54%, respectively) (**Figure 5.9**).

Table 5.4: Victims in rural areas report more ease in registering a police complaint

Locality		Ease of registering a police complaint about cybercrime	
		Easy	Difficult
	Rural	60	39
	Urban	55	42

Note: The rest did not respond. The table includes responses only from the victims. All figures in percentages. The categories 'very easy' and 'somewhat easy' were merged to form 'easy', and 'difficult' and 'very difficult' were merged to form 'difficult'.
Question asked: Overall, how easy or difficult was it to register a police complaint about the cybercrime – very easy, somewhat easy, somewhat difficult, or very difficult?

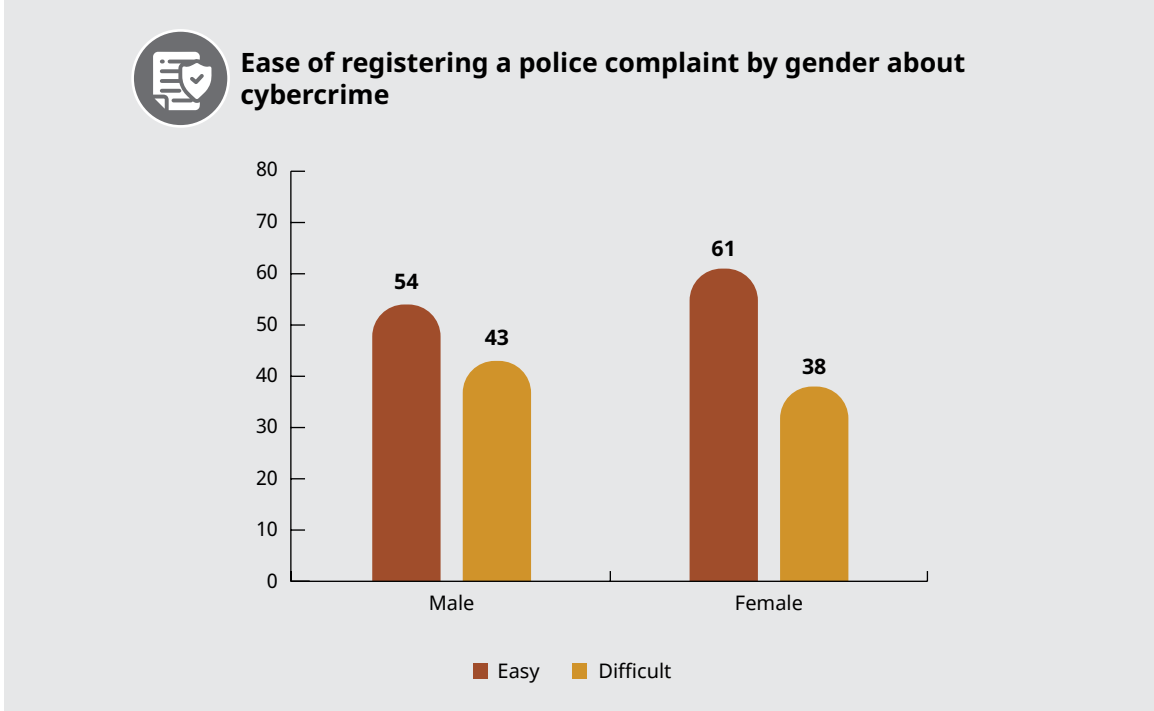
Figure 5.8: Economically disadvantaged victims are most likely to say that registering a complaint is easy



Note: The rest did not respond. The table includes responses only from the victims. All figures in percentages. The categories 'very easy' and 'somewhat easy' were merged to form 'easy', and 'difficult' and 'very difficult' were merged to form 'difficult'.

Question asked: Overall, how easy or difficult was it to register a police complaint about the cybercrime – very easy, somewhat easy, somewhat difficult, or very difficult?

Figure 5.9: Female victims are more likely to report that registering a complaint is easy



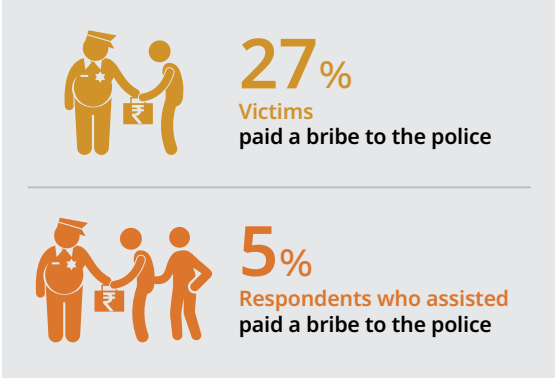
Note: The rest did not respond. The table includes responses only from the victims. All figures in percentages. The categories 'very easy' and 'somewhat easy' were merged to form 'easy', and 'difficult' and 'very difficult' were merged to form 'difficult'.

Question asked: Overall, how easy or difficult was it to register a police complaint about the cybercrime – very easy, somewhat easy, somewhat difficult, or very difficult?

5.3 Nature of Interaction with Police Personnel

While procedural delays, including the time taken and number of visits required, shape an important part of the victim's experience, they capture only the visible or logistical aspect of the process. The other, less tangible aspect involves the nature of interactions with the police personnel themselves. This may include situations where victims feel the need to offer bribes to get their work done, or where, in the absence of any concrete action, they rely on personal networks or intermediaries to exert pressure on the police. As seen in **Chapter 1,** using personal networks and connections to exert pressure on the police and other authorities are important determining factors in the recovery of money. Thus, analysing this dynamic using survey data will give a more nuanced understanding of how victims experience the process of seeking redressal.

Figure 5.10: More than a quarter of the respondents who complained to the police paid a bribe to the police



Note: The rest either said they did not pay a bribe to the police or did not respond. The sample of those who aided is very small (N – 26 for those who aided the victims and N – 170 for victims).

The responses are among those who complained to the police or went to the police but did not pursue the case.

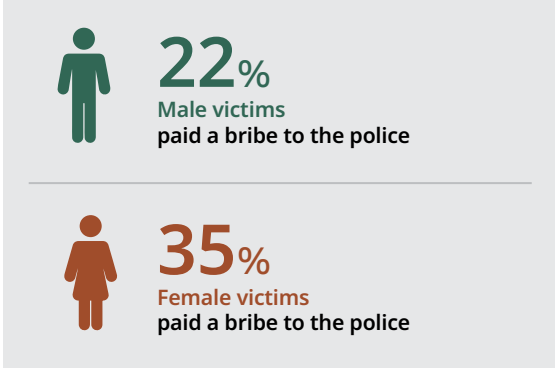
Question asked: Did you have to make any payment to the police at any point?

To understand whether any bribe was given at any point in time during the investigation, the respondents were asked about their experiences. The questions were asked only of the respondents who approached the police. More than a quarter of the victims reported that they had paid a bribe (27%), compared to only five percent among those who had helped the cybercrime victims (**Figure 5.10**).

The data was further analysed across socio-demographic variables to identify patterns. The data reveals that the poorest victims, women and victims from rural areas are significantly more likely to pay a bribe to the police in a cybercrime case, compared to their respective counterparts.

In terms of gender, over one-third of the women victims (35%) paid a bribe to the police, as compared to nearly a quarter of the male victims (22%) (**Figure 5.11**). Across economic classes, there was a noticeable disparity. Over half of the victims from poor economic backgrounds (51%) paid a bribe, as compared to only 12 percent of the rich respondents (**Figure 5.12**). Across rural and urban areas, over a third (36%) of the rural residents paid a bribe as compared to a quarter (24%) of victims in urban areas (**Figure 5.13**).

Figure 5.11: Over one-third of women victims paid a bribe to the police



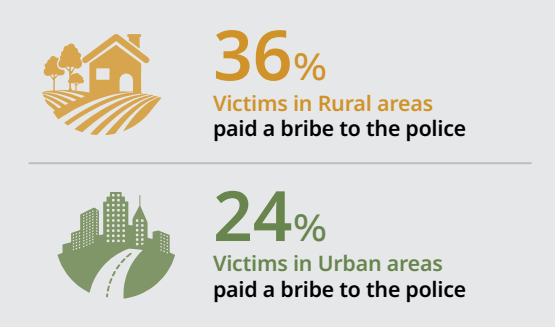
Note: The responses include only the victims who made a payment to the police.

Question asked: Did you have to make any payment to the police at any point?

Figure 5.12: Poor victims are nearly four times more likely to pay a bribe to the police, compared to the rich

Note: The responses include only the victims who made a payment to the police.
Question asked: Did you have to make any payment to the police at any point?

Figure 5.13: Over a third of victims in rural areas paid a bribe



Note: The responses include only the victims who made a payment to the police.
Question asked: Did you have to make any payment to the police at any point?

Those who reported paying a bribe were also asked how much money they had to pay to the police. It is important to note that a majority of cybercrime victims and a significant proportion of those who assisted victims chose not to answer this question (65% and 31%, respectively). Among the victims, nearly 16 percent paid up to one thousand rupees, nine percent paid between Rs. 1,001 and Rs. 2,000, and 11 percent paid more than Rs. 2,001. Among those who helped cybercrime victims, about a third paid up to a thousand rupees (31%), and another one-third paid Rs. 2,001 and above (31%) (**Table 5.5**).

Table 5.5: The amount of bribe paid to the police

	Bribe amount paid to the police (%)			
	Up to Rs. 1,000	Rs. 1,001 to Rs. 2,000	Rs. 2,001 and above	Did not respond
Victims	16	9	11	65
Respondents who assisted	31	8	31	31

N – 170 (victims) and 26 (respondents who assisted). The responses in the table are from those who said they had to make a payment to the police.
Note: The figures here only include those who paid a bribe. The sum might be more than 100 since the numbers are rounded off.
Question asked: Did you have to make any payment to the police at any point?

Moreover, the data was also analysed among the victims and those assisting the victims who paid a bribe to the police, and the amount of money recovered, to understand if there is a correlation between the two. The findings show that victims (and those assisting the victims) who reported paying a bribe were substantially more likely to report recovering the money they had lost. Among those who paid a bribe, a substantial proportion, 38 percent, recovered the full amount, and 16 percent recovered a partial amount (**Table 5.6**). Conversely, among those who did not pay a bribe, only 12 percent were able to recover the full amount, and only one in ten recovered a partial amount (10%). Among those who did not pay a bribe, as many as three in four (75%) said that they did not recover any of their money, as compared to nearly half of this figure among those who paid a bribe to the police (38%).

Respondents who made a complaint to the police were also asked whether they contacted someone in their personal network to put pressure on the police. About two in five of the victims (37%) and 13 percent of those who aided victims said that they had contacted someone they knew to exert some pressure on the police in handling their cybercrime complaint (**Table 5.7**).

The data was also analysed across the socio-demographics of the victims. When analysed by gender, women victims (41%) are relatively more likely to contact someone in their personal network to put pressure on the police as compared to men (35%) (**Figure 5.14**). In terms of economic class, over half of the victims from economically disadvantaged sections (55%) contacted their personal network as compared to about three in ten among other economic groups (lower – 28%, middle – 31% and rich – 30%) (**Figure 5.15**). In rural areas, the victims were more likely to rely on their personal network to put pressure on the police as compared to those residing in urban areas (44% and 35%, respectively) (**Figure 5.16**).

Table 5.6: Victims and those assisting victims who paid a bribe to the police were three times more likely to recover the full amount lost, compared to those who did not pay a bribe

Victims		"Were you able to recover your lost money?"		
		Yes, full amount	Yes, partial amount	No amount recovered
	Paid a bribe to the police	38	16	38
	Did not pay a bribe	12	10	75

Note: Rest did not respond to either of the questions. All the figures are in percentages. The table includes responses from both the victims and those who assisted cybercrime victims.

Question asked: Were you able to recover your lost money – yes, full amount; yes, partial amount; no?

Question asked: Did you have to make any payment to the police at any point?

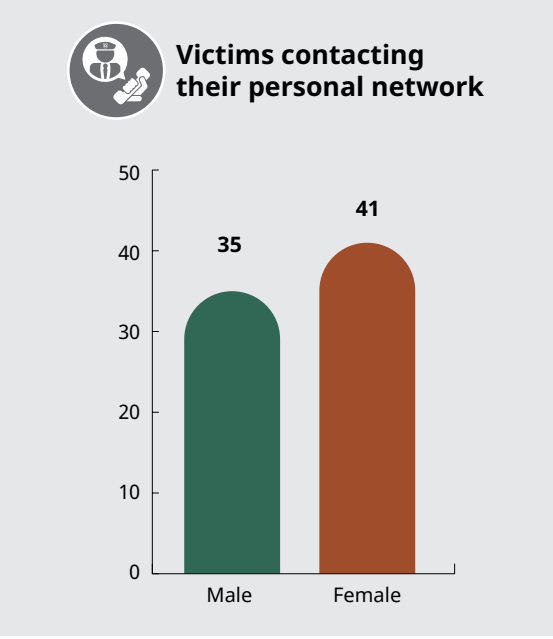
Table 5.7: More than a third of the victims contacted their personal network so that the police would deal with the case properly

Contacted personal network to put pressure on the police	Victim (%)	Respondents who assisted (%)
Yes	37	13

Note: The rest either said they did not contact anyone or did not respond. The sample in the aided segment is very small (N – 69 for those who aided; N – 235 for victims).

Question asked: Did you have to contact someone in your personal network to put pressure on the police to deal with your case properly?

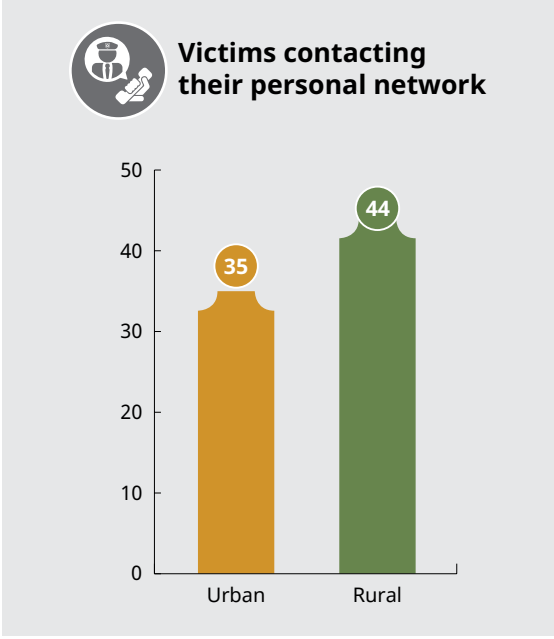
Figure 5.14: Women more likely to contact their personal network so that the police would deal with the case properly



Note: The responses include only the victims who contacted someone in their personal network.

Question asked: Did you have to contact someone in your personal network to put pressure on the police to deal with your case properly?

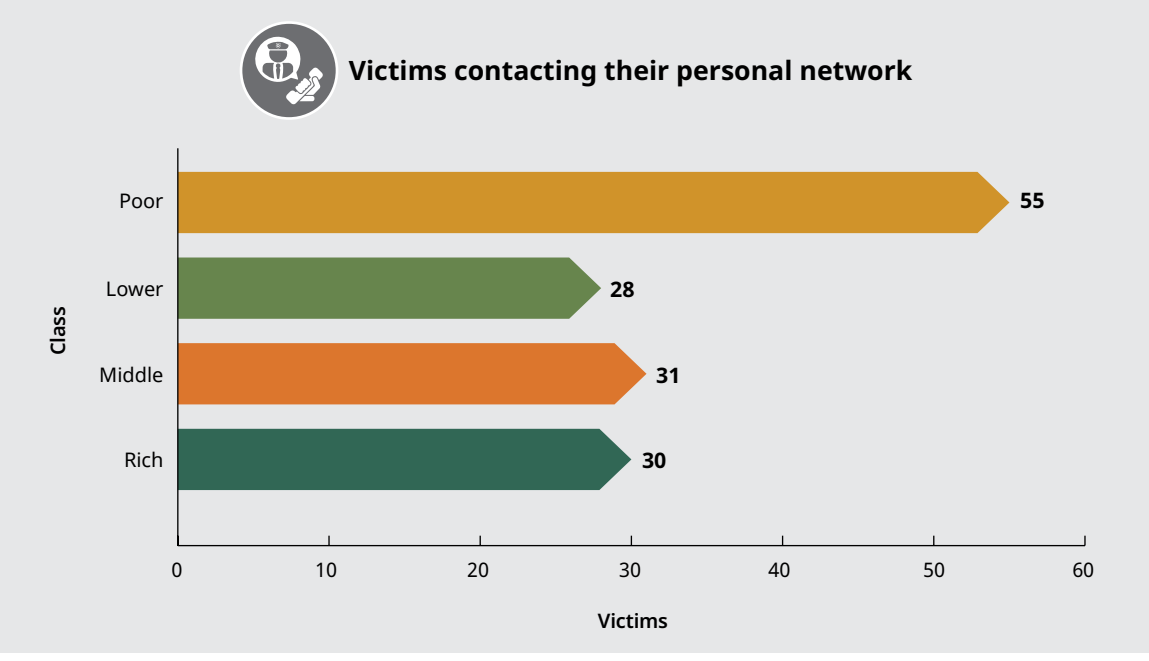
Figure 5.16: Victims from rural areas more likely to contact their personal network to put pressure on the police, compared to those from urban areas



Note: The responses include only the victims who contacted someone in their personal network.

Question asked: Did you have to contact someone in your personal network to put pressure on the police to deal with your case properly?

Figure 5.15: Over half of the victims from poor economic background contacted someone from their personal network so the police would deal with their case properly



Note: The responses include only the victims who contacted someone in their personal network.

Question asked: Did you have to contact someone in your personal network to put pressure on the police to deal with your case properly?

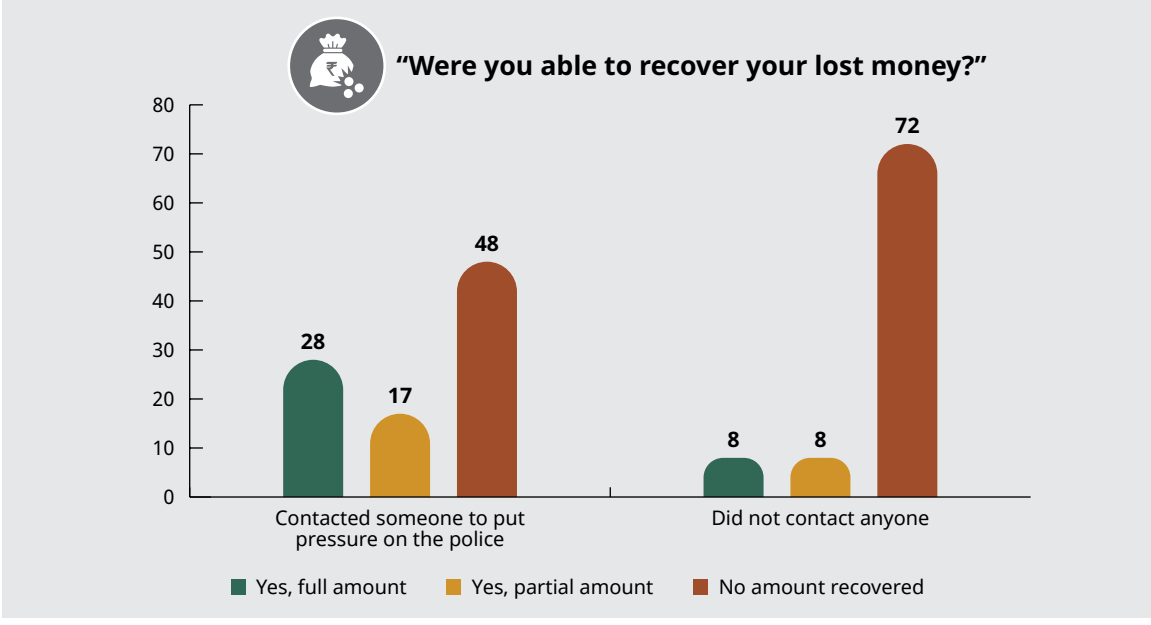
Table 5.8: Nearly half of the respondents who approached someone in their network to put pressure on the police contacted senior police officials

The person contacted to put pressure on the police	Victims/Respondents who assisted (%)
Senior police officers	47
Senior government officials	16
Local politician	13
Local person of influence	12
Media	5

Note: The rest were either naming other people/organisations or did not respond.
The responses of the victims and respondents who assisted were merged in this table.
Question asked: Who did you contact?

The respondents who had to contact someone in their personal network were also asked whom they contacted to put pressure on the police. Among the cybercrime victims and those who helped the victims, nearly half contacted senior police officials (47%), about one in six contacted senior government officials (16%), 13 percent contacted a local politician, and 12 percent contacted a local person of influence. Five percent of the victims said they contacted the media (**Table 5.8**).

Figure 5.17: Victims and those assisting victims who approached the police through a personal network were three times more likely to recover the full amount lost in cybercrime than those who did not contact anyone



Note: Rest did not respond to either of the questions. All figures are in percentages. The table includes responses from both the victims and those who assisted cybercrime victims.
Question asked: Were you able to recover your lost money – yes, full amount; yes, partial amount; no?
Question asked: Did you have to contact someone in your personal network to put pressure on the police to deal with your case properly?

The findings further show that those who contacted an influential person were more likely to report recovering their money lost in the cybercrime. Among those who approached the police through their personal network, more than a quarter were able to recover their money fully (28%), while less than one in five were able to obtain a partial recovery (17%). Among those who did not contact anyone, about one in ten were able to recover their money either fully (8%) or partially (8%), with a significant 72 percent saying they did not recover any of the money they lost due to the cybercrime (**Figure 5.17**).

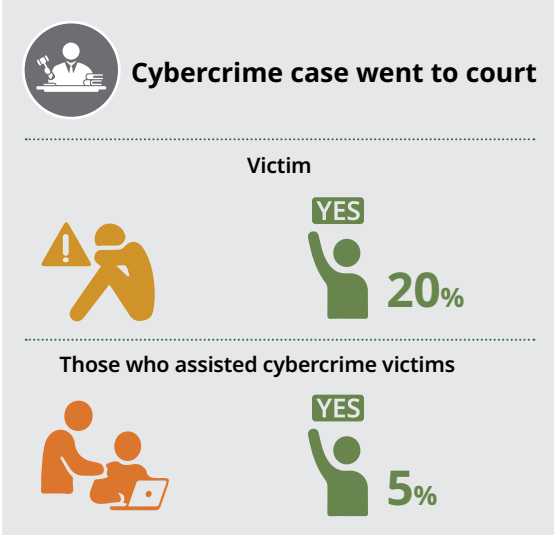
Both **Table 5.6** and **Figure 5.17** suggest that bribing the police as well as approaching a person of influence are important factors determining whether a victim of cybercrime will recover the money they lost due to the fraud or not. This also verifies the finding from the in-depth interviews with victims (see **Chapter 1**), which suggests that personal connections with police and other authorities play a significant role in the recovery of money in cybercrime cases. Even though it is an open secret that people often rely on bribes or influence to get work done by the police in India, there is little empirical data to support this. This finding, therefore, verifies such an association, particularly in the context of cybercrimes.

5.4 Progress of Cybercrime Cases in the Judicial System

Following the reporting and investigation stages, a subset of cybercrime cases also proceeds to the court. However, not all cases progress to the court. Examining this stage can offer insights into the extent to which victims have access to formal legal remedies through the judicial system.

To understand this, the respondents who were the victims of cybercrimes were asked whether their case went to the court or not. One in five of the cybercrime victims (20%) reported that their case went to the courts, and five percent of those who helped the other cybercrime victims said the case they assisted with went to the court (**Figure 5.18**).

Figure 5.18: One-fifth of the victims said their cybercrime case went to court

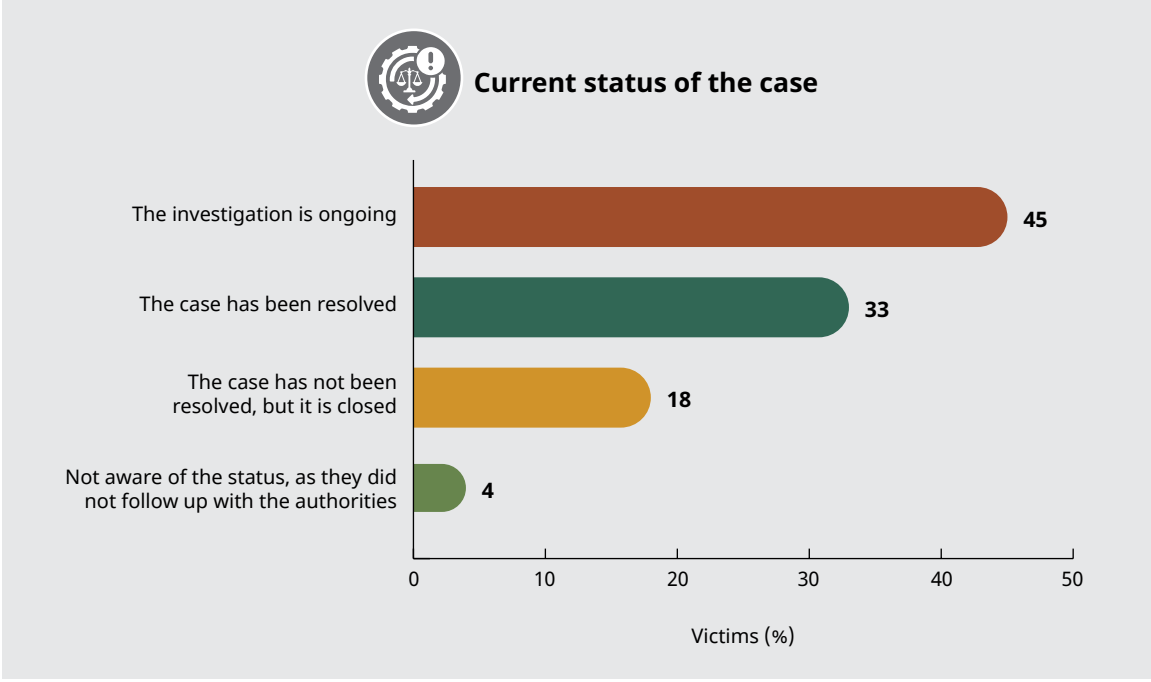


Note: The rest either said their case did not go to the court or did not respond.
Question asked: Did your case go to court?

Among those whose cases went to the court, nearly half of the victims (45%) said that the investigation was ongoing and one-third (33%) said that their case had been resolved. About one-fifth (18%) said that their case has not been resolved, but was closed. Four percent of the victims said that they are not aware of their case status, as they did not follow up with the authorities (**Figure 5.19**). The proportion of those who aided the cybercrime victims was very small and was not analysed.

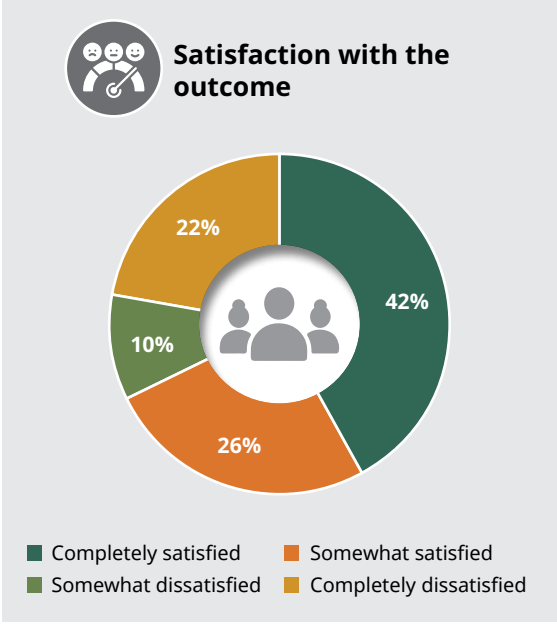
Those victims whose case has either been resolved or closed were further asked about their overall satisfaction levels with the outcome. Over two in every three (68%) said that they are satisfied with the outcome, with more than two-fifth of the victims (42%) being 'completely satisfied' and over a quarter (26%) being 'somewhat satisfied'. On the other hand, nearly one-third of the victims (32%) were dissatisfied with the outcome of their case (10% were 'somewhat dissatisfied' and 22% were 'completely dissatisfied') (**Figure 5.20**). It is important to note that those whose cases have either been resolved or closed form a very small part of the sample.

Figure 5.19: Nearly half of the victims whose cases went to court said their investigation is ongoing



Note: The rest did not respond. The table includes responses only from the victims. N – 215 (victims).
Question asked: What is the current status of your case?

Figure 5.20: Nearly one-third of victims were dissatisfied with the outcome of their case in court



Note: The rest did not respond. The table includes responses from only those victims who reported that their case has either been resolved or closed (N – 109).
Question asked: How satisfied were you with the outcome – completely satisfied, somewhat satisfied, somewhat dissatisfied, or completely dissatisfied?

5.5 Satisfaction with Police and Courts

Having examined the timelines, procedural pathways, interaction with the police and progression of cases through the courts, it becomes important to examine how victims evaluate these processes. One of the parameters could be the satisfaction of the victims, in terms of interaction with police and courts, or related services across different stages. Some of the parameters across which satisfaction of the victims has been ranked include the police helpline for cyber complaints, the usability of online reporting portals, and the complaint registration process at cyber police stations. Further, victim satisfaction with the conduct and effectiveness of police investigations, as well as the manner in which cases are handled within the courts have also been assessed. Bringing these elements together can help in giving a more nuanced understanding of cybercrime victims' perceptions about the redressal mechanism.

Respondents were asked to rate their satisfaction with various police or related services. The findings show that half of the victims (50% combining 'very satisfied' and 'somewhat satisfied') said that they are satisfied with the police helpline number for cyber complaints. Out of this proportion, about one-fifth (18%) were 'very satisfied' (**Table 5.9**). A little over a quarter (27%) expressed dissatisfaction (14% were 'very dissatisfied' and 13% were 'somewhat dissatisfied'), and another one-fifth (20%) said that they have never used the helpline number. Similarly, nearly half of the victims (47%) were satisfied with the online police portal for cybercrimes (16% were 'very satisfied' and 31% were 'somewhat satisfied'), and a quarter (25%) were dissatisfied (combining 12% 'very dissatisfied' and 13 percent 'somewhat dissatisfied'), and another quarter of the respondents (24%) said that they had not used the online police portal.

About half of the victims (46%) were also satisfied with the complaint registration process at the cyber police station, with about one in six (16%) being 'completely satisfied'. A little over a quarter expressed dissatisfaction (26%), with 12 percent being 'very dissatisfied'. About a quarter of victims (23%) reported that they had not been a part of the complaint registration process at the cyber police station (**Table 5.9**).

Over two in five victims (43%) are satisfied with the investigation of cybercrimes by the police (combining 17% 'very satisfied' and 26% 'somewhat satisfied'), and a greater proportion of dissatisfaction was observed when compared to other satisfaction levels, with three in ten of the victims being dissatisfied with the investigation of cybercrime by the police (30% combining 17% 'very dissatisfied' and 13% 'somewhat dissatisfied') (**Table 5.9**). A little over one in five (22%) said that their case did not reach the investigation stage. Furthermore, about one-third of the victims said that they were satisfied with the court dealing with their case (34% combining 13% 'very satisfied' and 21% 'somewhat satisfied'), with about a quarter expressing dissatisfaction (11% 'very dissatisfied' and 14% 'somewhat dissatisfied'). More than one-third of the victims (35%) also said their case never made it to the court.

Table 5.9: Satisfaction of the victims of cybercrimes with various police and court services

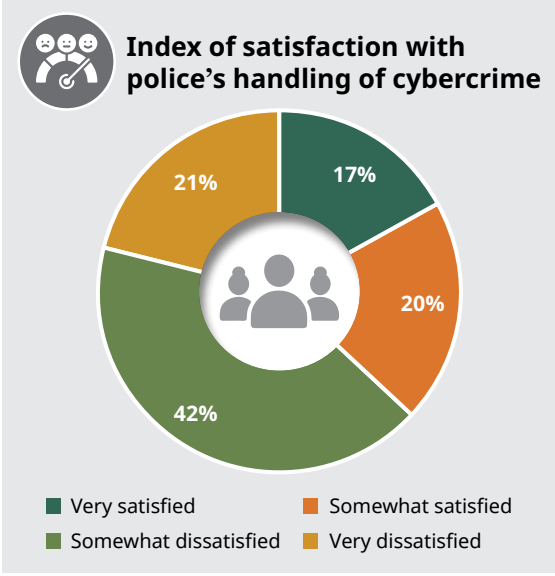
	Degree of satisfaction (Victims)				
	Very satisfied	Somewhat satisfied	Somewhat dissatisfied	Very dissatisfied	Never used these services*
Police helpline number for cyber complaints	18	32	13	14	20
Online police portal for cyber crimes	16	31	13	12	24
Complaint registration process at the cyber police station	16	30	14	12	23
Investigation of cybercrimes by the police	17	26	13	17	22
Court dealing with your case of cybercrime	13	21	14	11	35

**This was a silent option and was only coded if the respondent explicitly said that.*

Note: All figures are in percentages. The rest did not respond. The table includes responses only from the victims.

Question asked: How satisfied were you with the following – very satisfied, somewhat satisfied, somewhat dissatisfied, or very dissatisfied?

Figure 5.21: About two in every three victims are dissatisfied with the police handling of cybercrime



Note: The index was created from these questions posed to victims: police helpline number for cyber complaints, online police portal for cybercrime, complaint registration process at cyber police station and investigation of cybercrimes by the police. Please refer to Appendix 3 to see how the index was created.

The data was further analysed by constructing a satisfaction index using questions posed to the victims on topics such as the police helpline number for cyber complaints, the online police portal for cybercrime, the complaint registration process at the cyber police station and investigation of cybercrimes by the police. The data shows that nearly four in ten victims (37%) are satisfied with how police handle cybercrimes (17% 'very satisfied' and 20% 'somewhat satisfied'), while about two-thirds are dissatisfied (63% combining 42% 'somewhat dissatisfied' and 21% 'very dissatisfied') (**Figure 5.21**).

Thus, the victims are largely dissatisfied with the police's handling of cybercrimes. This finding resonates with the perceptions emerging from in-depth interviews with victims of cybercrimes, with the overall satisfaction with the police being relatively low, with an average rating of 2.4 out of 5 (see **Chapter 2** for more details).

Table 5.10: Women are more dissatisfied with the police handling of cybercrimes than men

Gender	Index of satisfaction with police handling cybercrime			
	Very satisfied	Somewhat satisfied	Somewhat dissatisfied	Very dissatisfied
Male	19	21	42	18
Female	15	17	42	26

Note: All figures are in percentages.
The index was created from these questions posed to victims: police helpline number for cyber complaints, online police portal for cybercrime, complaint registration process at cyber police station and investigation of cybercrimes by the police.
Please refer to Appendix 3 to see how the index was created.

Table 5.11: About a third of victims from rural areas are very dissatisfied with the police's handling of cybercrimes

Locality	Index of satisfaction with police handling cybercrime			
	Very satisfied	Somewhat satisfied	Somewhat dissatisfied	Very dissatisfied
Rural	22	14	32	32
Urban	16	21	45	18

Note: The index was created from these questions posed to victims: police helpline number for cyber complaints, online police portal for cybercrime, complaint registration process at cyber police station and investigation of cybercrimes by the police. All figures are in percentages.
Please refer to Appendix 3 to see how the index was created.

Table 5.12: Nearly a third of the economically disadvantaged section is very dissatisfied with police's handling of cybercrime

Economic class	Index of satisfaction with police handling cybercrime			
	Very satisfied	Somewhat satisfied	Somewhat dissatisfied	Very dissatisfied
Poor	18	17	36	29
Lower	22	18	46	14
Middle	16	20	45	19
Rich	11	25	42	22

Note: The index was created from these questions posed to victims: police helpline number for cyber complaints, online police portal for cybercrime, complaint registration process at cyber police station and investigation of cybercrimes by the police. All figures are in percentages. Please refer to Appendix 3 to see how the index was created.

The data was further analysed across social demographics with the satisfaction index of the police handling of cybercrime. Overall, women, the poorest and victims from rural areas are likely to be the most dissatisfied with the police's handling of cybercrimes. Female victims are more likely to be 'very dissatisfied' with how police handle cybercrime as compared to male victims (26% and 18%, respectively), thereby male victims show a greater satisfaction than women (21% versus 17% as 'somewhat satisfied' and 19% versus 15% as 'very satisfied') (**Table 5.10**). Across rural and urban areas, rural victims were far more likely to be 'very dissatisfied' than urban victims (32% versus 18%) (**Table 5.11**). Across economic classes, nearly a third of the economically disadvantaged cybercrime victims (29%) were 'very dissatisfied', the highest among all economic groups (**Table 5.12**).

5.6 Conclusion

The findings of this chapter suggest that while India's cybercrime redressal framework appears to have expanded significantly, the experiences of victims are varied. For a majority of respondents, the engagement with formal institutions, particularly local police stations, appears to be clearly their first step, and a substantial proportion are able to make a formal complaint and even FIRs, although the proportions differ to some extent. Rural victims were relatively more likely to approach the police than their urban counterparts, while younger victims were the least likely to do so across all age groups. However, this engagement appears to be not as seamless.

At the entry stage, barriers such as perceived complexity, fear, embarrassment and the belief that the loss is too small appear to discourage a share of victims from reporting the cybercrime. Even among those who do approach the police, the process involves considerable time with multiple visits—a burden that falls more heavily on rural victims, who were twice as likely to make multiple visits as urban victims, and on the economically disadvantaged, who were least likely to have their complaint registered within an hour. Women and the economically disadvantaged, however, were more likely to rate the process as easy, pointing to possible differences in baseline expectations across groups.

Beyond formal procedures, the findings show the continued relevance of informal mechanisms within the system. A sizeable proportion of victims had to pay bribes to the police, disproportionately so among the poor and rural victims, and in some cases, rely on personal networks to put pressure on the police to ensure responsiveness, a pattern especially pronounced among the economically disadvantaged and women. The payment of bribes and approaching a person of influence through personal networks are factors that have a significant bearing on the outcome of the

case. The findings reveal that those who paid a bribe to the police or those who approached the police through a personal network were significantly more likely to recover the money that they lost due to the cybercrime.

Only a limited fraction of the cases ended up reaching the courts, and even fewer were resolved, and the satisfaction among those whose cases were resolved appears to be on the higher end. Overall, the level of satisfaction with the police handling of cybercrimes is low, with nearly two out of three victims being dissatisfied with the police handling of cybercrimes in varying degrees.

Moreover, the findings also reveal that the women, rural victims and the poorest victims were more likely to face barriers with the police, such as long waiting times, multiple visits to the police station/unit, having to pay bribes and contacting persons of influence to get the work done, and were also more likely to show greater dissatisfaction with the police's handling of cybercrimes.

Taken together, the findings do show a system that functions but appears not to have consistently met the expectation when it comes to efficiency and fairness, and one where the burden of navigating it is unequally distributed. The fact that more marginalised groups, such as the poor, rural residents and women, are simultaneously more likely to encounter corruption, rely on informal networks, and report greater dissatisfaction with the police's handling of their cases shows how disadvantage compounds within the system, instead of being offset by it. The challenge is therefore not just of access, but also of experience and equity. A strong focus on simplifying procedures, improving responsiveness and reducing dependence on informal channels may contribute towards enhancing the trust in institutions.

References

- Bureau of Police Research and Development. (n.d.). *Capacity building at the PS level in cybercrime investigation*. Ministry of Home Affairs, Government of India. https://bprd.nic.in/uploads/pdf/Capacity%20Building%20at%20PS%20Level%20in%20Cyber%20Crime%20Investigation.pdf
- Curtis, J., & Oxburgh, G. (2022). Understanding cybercrime in 'real world' policing and law enforcement. *The Police Journal, 96*(4), 573-592.
- Gupta, M., & Singh, R. K. (2025). Cybercrime and investigation in India: Role of law enforcement and challenges faced. *Indian Journal of Legal Review (IJLR), 5*(5), 17–28.
- Lee, J. R., Holt, T. J., Burruss, G. W., & Bossler, A. M. (2019). Examining English and Welsh detectives' views of online crime. *International Criminal Justice Review, 31*(1), 20–39. https://doi.org/10.1177/1057567719846224
- Lee, J. R., Nam, Y., Lee, W.-G., Holt, T. J., & Bossler, A. M. (2025). Police capacity for cybercrime response: Assessing the impact of officers' perceptions and agency-level factors on England and Wales constables' capability responding to computer hacking offenses. *Journal of Criminal Justice, 101,* Article 102541. https://doi.org/10.1016/j.jcrimjus.2025.102541
- Ministry of Home Affairs, Government of India. (n.d.). *Categories of cyber crime*. Cyber Crime Portal. https://cybercrime.gov.in/Webform/CrimeCatDes.aspx

CHAPTER

06

An advertisement by Saharanpur Police on an underconstructed Flyover (Saharanpur, Uttar Pradesh- September 13, 2026).

Photo by Mohd Aasif/Common Cause.

Role of Banks and Inter-Institutional Coordination

Key Findings

- One in two victims of digital financial fraud (52%) complained separately to the bank. Nearly two-thirds of financial fraud victims (63%) reported the fraud within 24 hours to the bank.
- About three out of four victims (72%) could not recover any of their lost money.
- Nearly a quarter of the victims of cyber fraud (22%) are 'very dissatisfied' with the bank's role in recovery of money.
- One in five victims of digital financial frauds (20%) are 'very dissatisfied' with the bank-police coordination in their case.
- Amongst those victims who fully recovered their money, almost all (49% 'fully satisfied' and 43% 'somewhat satisfied' reported being satisfied with the coordination between police and banks.
- Two-fifths of the victims who complained separately to the bank (40%) feel that cybercrime occurred due to a breach of personal data by the bank.

Role of Banks and Inter-Institutional Coordination

Cybercrimes, from cyber threats and financial fraud to other malicious activities, are increasing globally at an alarming rate. Being at the centre of the growing scale of digital financial frauds, banks play an important role in their prevention and redressal. To do so, banks are required to coordinate with the police and various other institutions, including the Reserve Bank of India (RBI), Indian Cyber Crime Coordination Centre (I4C), Indian Computer Emergency Response Team (CERT-In) and others. They are also required to comply with a set of institutional guidelines to handle and mitigate cybercrimes across India. These guidelines require banks to strengthen their cybersecurity defences through proactive risk management and continuous real-time monitoring via established Security Operations Centres (SOCs). Together, these measures emphasise banks' responsibility to address evolving cyber threats through strategic planning and continuous preparedness.

The scale of this responsibility becomes clearer when one looks at the data. Concerns around digitisation are primarily related to accessibility or security of one's data and information. The Crime in India 2024 report showed an upward trajectory in rising cybercrimes, with 101,928 cases recorded in 2024, a 17 percent increase over the previous year. Fraud emerged as the predominant issue, accounting for 72.6 percent of all cybercrime incidents (73,987 cases), thereby reinforcing the pattern observed in prior years, that financial channels such as UPI, card transactions, phishing, and unauthorised transfers serve as the primary vectors of digital crime (National Crime Records Bureau, 2026). The fraud-related offences have now crossed the one-lakh-case threshold for the first time, highlighting the growing need for banks and financial intermediaries to strengthen real-time detection, customer authentication, and inter-institutional coordination with law enforcement.

Against this backdrop, the current chapter focuses on various aspects of interaction between cybercrime victims and financial systems. It first explores issues concerning the complaint process and response of the bank, recovery of funds, measures taken by banks to mitigate digital fraud, and the time taken by banks to recover the money of the victims. It then explores victims' perceptions of satisfaction with regulatory bodies like the Reserve Bank of India (RBI) and the bank's role in recovering their money. Lastly, it examines perceptions about the coordination between banks and police, as well as victim's perceptions of whether their banking data may have been compromised, thereby making them targets of cybercrime.

6.1 Complaints to the Bank

The rapid escalation of cybercrime in India has underscored the need for a systematic response mechanism, including prompt reporting of cyber fraud to banks by victims. In this context, the data in **Figure 6.1** helps in understanding the response of digital financial fraud victims who lodged complaints directly with the bank and those who were assisting cybercrime victims. Over half of the victims of digital financial fraud (52%) reported lodging complaints independently with the bank. In contrast, four in ten of those who aided or helped a victim of cybercrime (41%) reported that a complaint was filed separately with the bank. At the same time, over two-fifths of the victims (44%) and close to half (47%) of those who assisted the cybercrime victims did not file a separate complaint with the bank (**Figure 6.1**).

Figure 6.1: One in two victims complained separately to the bank

Note: The rest did not respond. The question was asked to digital financial fraud victims and those who assisted cybercrime victims of this kind.

Question asked: Did you/they complain separately to the bank?

To understand reporting behaviour across socio-economic groups, the responses were analysed by the economic class of the victims. The data reveals a clear class-based pattern in complaint behaviour. Respondents from rich economic backgrounds show the highest likelihood of filing complaints with banks (63%), compared to other income groups. In contrast, the most economically disadvantaged (43%) and those from lower income brackets (50%) were less likely to complain to the bank separately (**Table 6.1**).

Furthermore, the data shows that there is a slight difference in complaint behaviour based on locality, as victims in rural areas (55%) are slightly more likely to report complaints to the bank than those in urban areas (51%). Similarly, women victims (49%) were slightly less likely to lodge a complaint with the bank than men (53%). These patterns are consistent with the trends in reporting to the police, wherein victims from rural areas are more likely to complain to the police (See **Table 5.1, Chapter 5** for more details). No significant patterns were observed across age and educational status of the victims.

Timely reporting is one of the most important aspects in cases of cybercrime, as it increases the chances of the defrauded money being recovered. **Figure 6.2** indicates that about more than two in three digital financial fraud victims (including those who assisted victims) (63%) reported the fraud within 24 hours of its occurrence to the bank. This shows that a majority of respondents acted immediately once the incident was detected. Furthermore, one-fifth reported the fraud within 48 hours, and 11 percent reported 48 hours after the occurrence of the cybercrime (**Figure 6.2**).

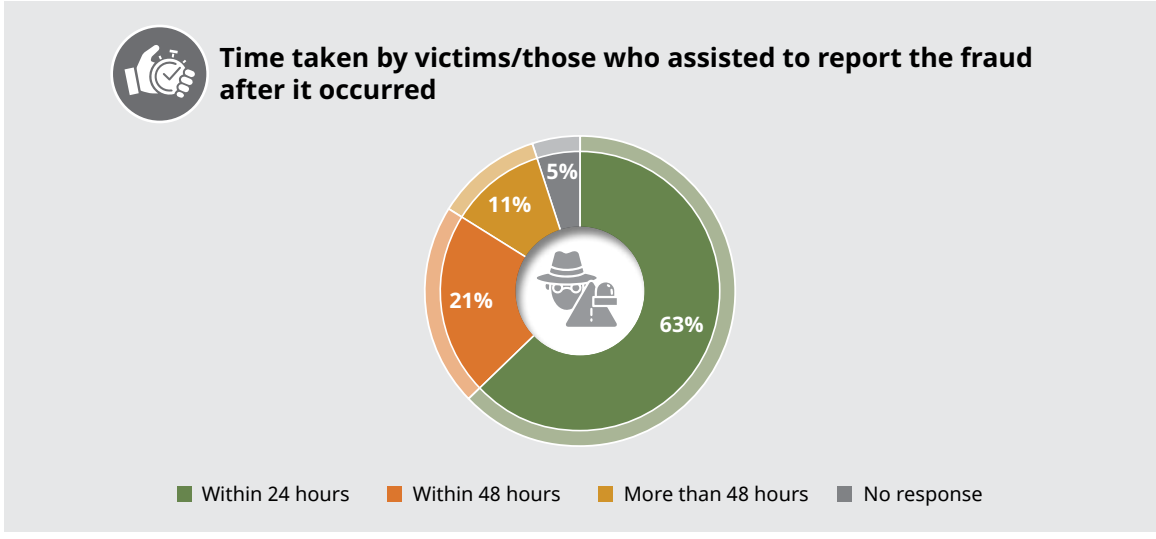
Table 6.1: Digital financial fraud victims from rich backgrounds are the most likely to lodge a separate complaint with the bank

Class	Complained to the bank	
	Yes	No
Poor	43	52
Lower Class	50	47
Middle	56	38
Rich	63	36

Note: All figures are in percentages. The rest did not respond. The responses are among digital financial fraud victims only.

Question asked: Did you/they complain separately to the bank?

Figure 6.2: Nearly two-thirds of financial fraud victims and those who closely aided the victims reported the fraud within 24 hours to the bank

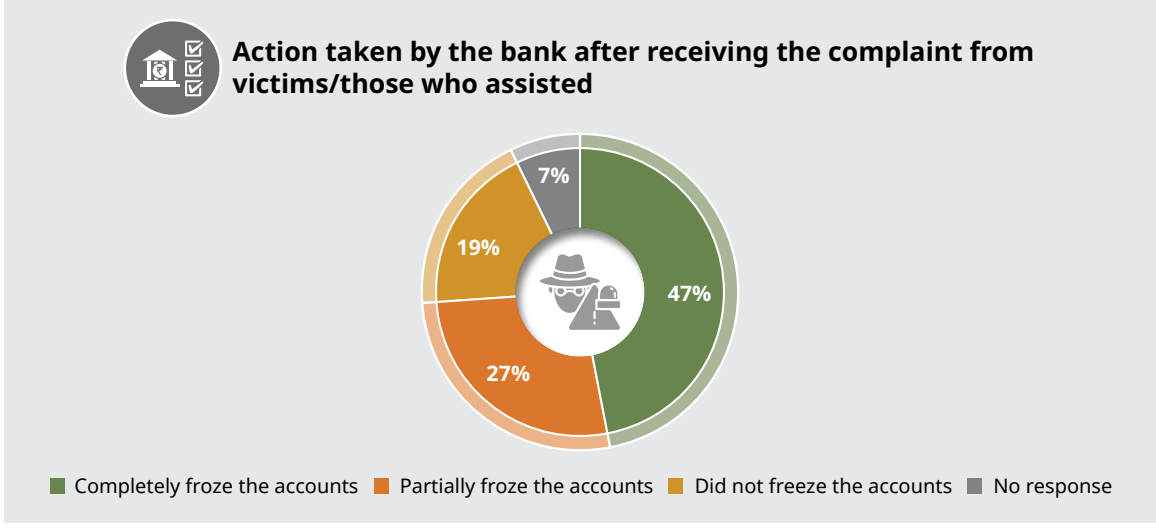


Note: For more information on the index, refer to Appendix 3. The table includes responses from both the victims and those who assisted victims of digital financial fraud.
Question asked: How soon after the fraud did you/they report it?

While a significant proportion of victims report cyber fraud promptly, the effectiveness of such reporting also depends on the responsiveness of banks after receiving the complaint. With the increasing use of digital financial transactions, the reliance on banking facilities has expanded considerably. In order to understand the bank's promptness in addressing the fraud, the financial fraud victims were asked whether the bank took any action after receiving the complaint.

The data shows that among those who complained to the bank separately, a little under half (47%) of the victims and those who assisted cybercrime victims reported that the bank completely froze all accounts after receiving the complaint (**Figure 6.3**). Over one in four (27%) said the accounts were partially frozen, while nearly one-fifth (19%) said the accounts were not frozen at all.

Figure 6.3: Nearly half of victims and those who assisted them indicated that the bank completely froze their accounts upon receiving the complaint



Note: For more information on the index, refer to Appendix 3. The table includes responses from both the victims and those who assisted cybercrime victims of digital financial fraud.
Question asked: Did the bank take any action, such as freezing all your accounts, etc., after receiving the complaint?

6.2 Recovery of Money

An important measure of the effectiveness of cybercrime response systems is the extent to which people are able to recover their financial losses caused by digital fraud. To understand this, victims and those who assisted cybercrime victims were queried whether they were able to recover their lost money. Data shows that, collectively, about three in four victims and those who assisted cybercrime victims (72%) reported that no amount of their lost money was recovered (**Figure 6.4**). Only one in ten said that the whole amount was recovered, and seven percent said that a partial amount was recovered. Taken together, only 17 percent of the victims of digital financial fraud were able to recover their money fully or partially. Overall, these figures indicate that the vast majority of individuals affected by financial loss experienced very limited or no restitution, thus failing to achieve meaningful recovery.

Figure 6.4: About three out of four victims and those who assisted them could not recover any of their lost money

Note: The rest did not respond. For more information on the index, refer to Appendix 3. The table includes responses from both the victims and those who assisted cybercrime victims of digital financial fraud.

Question asked: Were you able to recover your lost money?

Victims' experiences with cyber fraud resolution are not only shaped by whether their lost money is recovered but also by how quickly the recovery takes place. The time taken to restore funds can significantly influence victims' perceptions of the effectiveness of institutional response mechanisms. The victims whose money was recovered were asked how long it took to recover their lost money following the cyber-fraud incident.

The data indicates that financial recovery, when it occurs, tends to happen relatively early for a significant proportion of victims. Nearly a third of the victims and those who assisted cybercrime victims (32%) reported recovering their money within 15 days of the incident, while 17 percent were able to recover the amount within 16 to 30 days (**Figure 6.5**). About a quarter (24%) reported that they were able to recover their money between one to two months, and one in ten said that it took more than two months to recover their money.

Figure 6.5: One-third of victims and those who assisted them were able to recover their money within 15 days

Note: The rest did not respond. For more information on the index, refer to Appendix 3. The table includes responses from both the victims and those who assisted cybercrime victims of digital financial fraud who were able to recover either the whole or partial amounts.

Question asked: How long after the cyber fraud did you recover the money?

6.3 Institutional Response and Effectiveness

Victims of cybercrime encounter multiple institutions while seeking resolution, including banks and regulatory bodies such as the RBI and the Banking Ombudsman. Their experiences with, and assessments of, these institutions may vary considerably depending on the nature of engagement and the effectiveness of institutional responses.

While banks are one of the first points of contacts for the victims, data shows that their performance receives mixed evaluations. In terms of the bank's role in recovering money, 32 percent of digital financial fraud victims and those who assisted victims reported satisfaction (11% were 'very satisfied' and 21% were 'somewhat satisfied'), while 38 percent expressed dissatisfaction (16% - 'somewhat dissatisfied' and 22% - 'very dissatisfied') (**Table 6.2**). Notably, one in four victims and those who assisted (24%) said that they never used this service.

With respect to the RBI Banking Lokpal mechanism, a little more than a quarter (27%) expressed satisfaction (9% 'very satisfied' and 18% 'somewhat satisfied'), whereas one in five reported dissatisfaction (20% combining "somewhat dissatisfied" and "very dissatisfied"), but a striking 46 percent reported never having used the Lokpal services (**Table 6.2**). One possible reason for this could be limited awareness about the availability of the RBI Banking Lokpal mechanism among victims.

Raj (2024) identifies low consumer awareness and operational limitations as key shortcomings of the Banking Ombudsman Scheme, as they capture only those respondents who were aware of and able to access the formal grievance redressal mechanism. This may help explain both the limited Lokpal engagement and the moderate satisfaction levels observed across both respondent groups.

Satisfaction with the bank's role is influenced by the bank's ability to recover the victim's money. A partial or full recovery of money versus no recovery can differently impact a victim's perception and their levels of satisfaction. **Table 6.3** shows how these two factors are associated with each other. Data shows that nine out of ten (90%) victims who fully recovered their financial losses report being satisfied (58% are 'very satisfied' and 32% are 'somewhat satisfied') with the bank's efforts in facilitating recovery. Among those who were able to recover a partial amount, about two-thirds (65%) are satisfied (13% are 'very satisfied' and 52% are 'somewhat satisfied'). In contrast, a substantial proportion of those who did not recover any money, three in ten (30%), reported being 'very dissatisfied' with the bank's role in the recovery

Table 6.2: Nearly a quarter of the victims of cyber fraud are very dissatisfied with the bank's role in recovery of money

"How satisfied were you with..."		Degree of satisfaction				
		Very satisfied	Somewhat satisfied	Somewhat dissatisfied	Very dissatisfied	Never used this service*
	The bank's role in recovering the money	11	21	16	22	24
	RBI Banking Lokpal	9	18	11	9	46

**This was a silent option and was only coded if the respondent explicitly said that.*

Note: The rest did not respond. All figures are in percentages. The table includes responses from both the victims and those who assisted cybercrime victims of digital financial fraud. For more information on the indices, refer to Appendix 3.

Question asked: How satisfied were you with the following – very satisfied, somewhat satisfied, somewhat dissatisfied, or very dissatisfied?

Table 6.3: Victims whose money was recovered are more likely to be satisfied with the bank's role in recovering it

"Was the lost money recovered?"	Level of satisfaction with the bank's role in recovering the money			
	Very satisfied	Somewhat satisfied	Somewhat dissatisfied	Very dissatisfied
Yes, the whole amount	58	32	4	4
Yes, a partial amount	13	52	15	7
No	4	13	18	30

Note: The rest either did not respond or have never used this service. All figures are in percentages. The responses are from the victims only.

Question asked: How satisfied were you with the bank's role in recovering your money – very satisfied, somewhat satisfied, somewhat dissatisfied, or very dissatisfied?

process. These findings indicate that positive perceptions of the bank's role are strongly linked to successful restitution, whereas dissatisfaction overwhelmingly corresponds with complete or near-complete financial loss (**Table 6.3**).

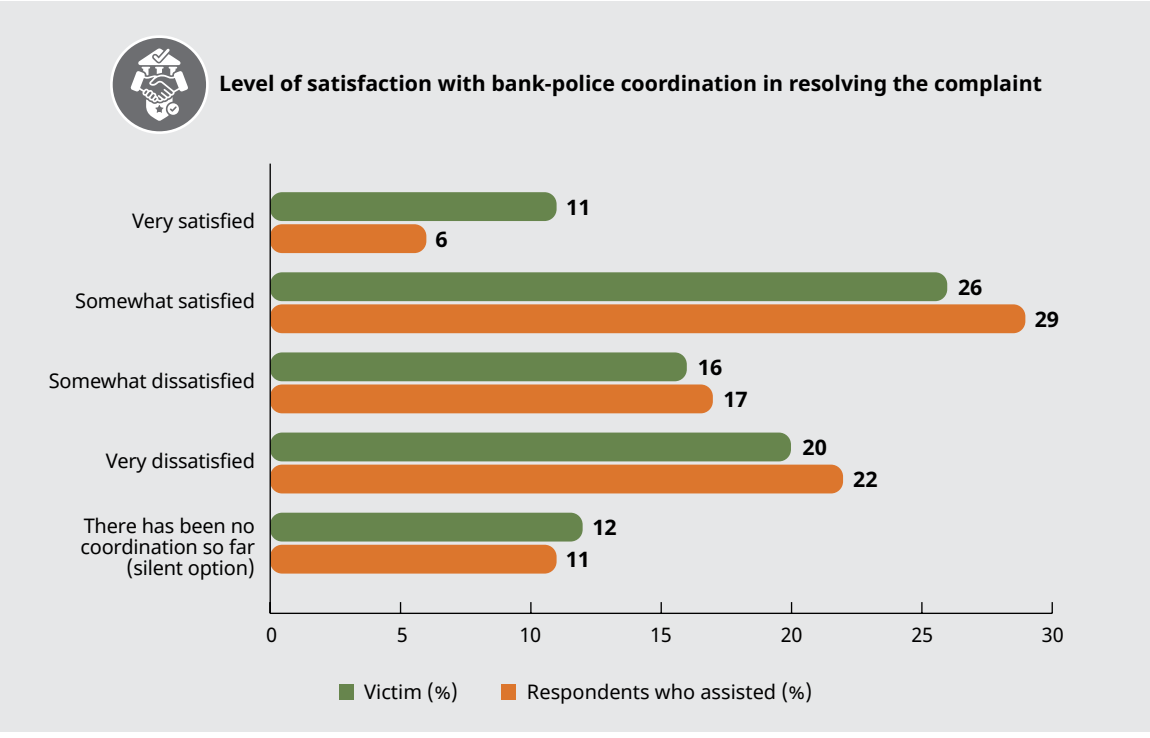
6.4 Institutional Coordination and Service Satisfaction

A crucial aspect of complaint redressal in cases of financial cybercrimes is the coordination between different institutions, particularly between the bank and the police. While this coordination is facilitated by systems such as the Indian Cyber Crime Coordination Centre (I4C) and is supposed to work seamlessly, in reality, there are major gaps in this coordination, which make the complaint redressal process significantly more difficult for victims of cybercrimes. This is also reflected in the survey data, with a notable proportion of the victims and those who assisted victims reporting low satisfaction with coordination between the bank and the police.

When respondents were asked about their level of satisfaction with bank–police coordination in complaint resolution, the data in **Figure 6.6** reflects mixed levels of satisfaction among both victims and those who assisted the victims. While 11 percent of the financial fraud victims said that they were 'very satisfied' with the coordination between the bank and the police, the corresponding percentage among those who assisted the victims fell by nearly half, to six percent. However, the overall levels of satisfaction remained similar between the two groups (37% among victims and 35% among those who assisted digital fraud victims). Notably, as many as 20 percent of victims and 22 percent of those who assisted victims reported being 'very dissatisfied' with this coordination, while another 16 percent of the victims and 17 percent of those who assisted the victims said that they were 'somewhat dissatisfied'. At the same time, over one in ten respondents in both groups reported that there has been no coordination so far between the bank and the police (**Figure 6.6**).

The perceived effectiveness of coordination between banks and the police is also influenced by whether victims are able to recover the money lost in fraudulent transactions. **Table 6.4** highlights the relationship between these two factors. Among those who recovered the full amount, about half of the victims (49%) reported being 'very satisfied' and more than two in five victims (43%) were 'somewhat satisfied' with bank-police coordination. Moreover, none of the respondents who recovered the whole amount reported being 'very dissatisfied'. In contrast, respondents who experienced only partial recovery reported more mixed experiences; just under one in five (17%) were 'very satisfied',

Figure 6.6: One in five victims of digital financial frauds are very dissatisfied with the bank-police coordination in their case



Note: The rest either did not respond or did complain to the bank/police.

**This was a silent option and was only coded if the respondent explicitly said that.*

Question asked: How satisfied are you/they with the coordination between the bank and the police in resolving your cybercrime complaint – very satisfied, somewhat satisfied, somewhat dissatisfied, or very dissatisfied?

while more than half (54%) reported being 'somewhat satisfied', with a small share expressing dissatisfaction (20% combining 7% 'very dissatisfied' and 13% 'somewhat dissatisfied'). The dissatisfaction is highest among those who were not able to recover their money, with over a quarter (27%) being 'very dissatisfied', and 19 percent saying they were 'somewhat dissatisfied' (**Table 6.4**). This goes on to show how the recovery of money strongly influences perceptions of effective coordination between two important stakeholders.

Table 6.4: Almost all victims whose money was fully recovered report being satisfied with the coordination between police and banks

"Was the lost money recovered?"	Level of satisfaction with bank-police coordination in resolving the complaint			
	Very satisfied	Somewhat satisfied	Somewhat dissatisfied	Very dissatisfied
Yes, the whole amount	49	43	4	<1
Yes, a partial amount	17	54	13	7
No	4	19	19	27

Note: The rest either did not respond or have never used this service. All figures are in percentages. The responses are from the victims only.

Question asked: How satisfied were you with the bank's role in recovering your money – very satisfied, somewhat satisfied, somewhat dissatisfied, or very dissatisfied?

Victims' responses to cybercrimes are also shaped by their interpretation of where the responsibility for the breach lies. The data in **Figure 6.7** highlights a relationship between making a complaint directly to the bank and identifying data security as the root cause of the incident. Among those who made a complaint separately to the bank, four in ten believed it was a cause of personal data being leaked, and a slightly higher proportion (44%), reported that it was not the case. Among victims who did not interact with the banks, over half (54%) believed it was not caused by the breach of personal data.

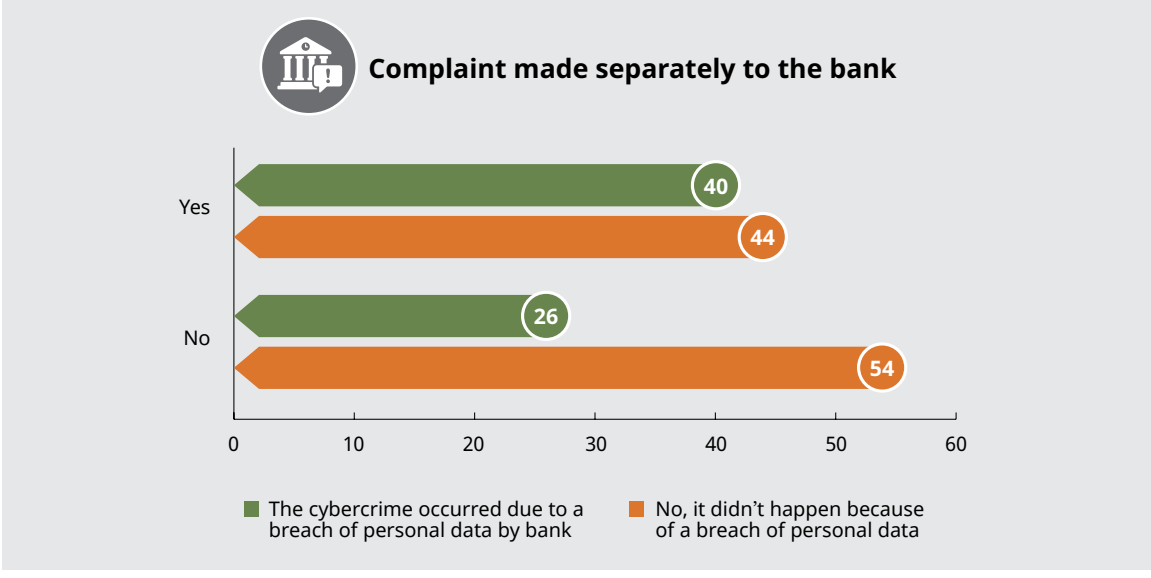
6.5 Conclusion

In summary, this chapter examines how banks and regulatory institutions respond to cybercrime victims and how satisfied the latter are with that response. The findings reveal that the banking system is partially functional, accessible to some, and, importantly, uneven in its effectiveness.

Data shows that although a significant proportion of victims have engaged with their banks after experiencing cybercrime and made complaints separately, the act of complaining did not translate into meaningful recovery. Nearly two-thirds reported the fraud within 24 hours, and nearly half had their bank accounts frozen after complaining to the bank. However, a vast majority of victims were not able to recover anything, and even among those who did, the process is slow (except for a third of the victims who recovered it within 15 days). Rich and rural victims were more likely to lodge complaints with banks.

Satisfaction with both the bank's role in recovering money and the RBI Banking Lokpal is tepid, with around three in ten reporting being satisfied, and a similar proportion reporting being dissatisfied. However, a significant share of victims never sought the bank's help in recovering money (24%), and even a larger share never even accessed the RBI Lokpal mechanism (46%). Moreover, financial

Figure 6.7: Two-fifths of the victims who complained separately to the bank feel that cybercrime occurred due to a breach of personal data



Note: The rest did not respond. All figures are in percentages. The responses are among the victims only.

Question asked: Some victims of financial cybercrimes believe that their financial data was leaked by a bank insider because of which they were targeted by criminals. In your case, do you think the crime occurred due to a breach of your personal data by the bank or its personnel?

Statement 1: Yes, it occurred due to a breach of personal data; Statement 2: No, it didn't happen because of that.

fraud victims whose money was fully recovered were more likely to be satisfied with the bank's role in recovering money.

An important part of effective cybercrime resolution is a seamless coordination between the banks and the police. While a third of both victims and those who assisted cybercrime victims are satisfied with bank and police coordination, a slightly higher proportion of victims are also dissatisfied with the same.

References

- National Crime Records Bureau. (2026). *Crime in India 2024*. Ministry of Home Affairs, Government of India. https://ncrb.gov.in
- Raj, S. (2024). Evaluating the Banking Ombudsman Scheme as an effective customer grievance redressal mechanism for the customers of banks operated in India. SSRN. https://ssrn.com/abstract=5019857

CHAPTER

07

Indian Cyber Crime Coordination Centre and Kolkata Police dismantle a nationwide cyber fraud racket (Kolkata, India – April 20, 2026).

Photo by Kolkata Police Facebook Page.

Digital Financial Behaviour and Cyber Safety Perceptions

Key Findings

- One out of two respondents (49%) use UPI apps daily.
- Men, urban and upper-class respondents are more likely to use online payment modes than their counterparts.
- UPI is considered extremely safe for online banking by over a third of the respondents (34%). Over three in five respondents perceive online banking methods to be safe (23% said “very safe” and 40% said “somewhat safe”).
- Those respondents who are most vulnerable to unsafe online practices are also the most likely to consider online banking very safe.
- About three in four respondents (72%) use social media apps/websites daily. Younger, richer and urban respondents are more likely to use social media frequently compared to their counterparts.
- Those who use UPI regularly are slightly more prone to cybercrime than those who are not regular users.
- Close to three in five people feel either fully or partially safe in sharing their personal data on social media platforms. However, those who feel very safe in sharing personal data on social media platforms are slightly more likely to have been a victim of cybercrime than those who felt very unsafe.

Digital Financial Behaviour and Cyber Safety Perceptions

India is among the largest and fastest emerging digital economies in the world. According to the Internet in India Report (2025), the country now has 958 million active internet users, marking a year-on-year increase of eight percent in 2025. Of these, 57 percent – i.e. about 548 million users – are based in rural regions (*The Hindu,* 2026). This points to a significant structural shift in the scale of digital adoption across the country. Data from the 79th round of the National Sample Survey Office (NSSO) conducted in 2022-23 corroborates this trend: over 85 percent of individuals aged 15 years and above are able to operate a smartphone, while nearly 60 percent can access the internet (NSSO, 2024). In fact, more than 30 percent of the rural and over 50 percent of the urban population are capable of conducting online banking transactions (Marathe, 2025). As per Ministry of Finance statistics, India's digital payments ecosystem expanded substantially in FY 2023–24, driven largely by UPI, which contributed around 80 percent of all retail transactions nationwide. Total transaction volume crossed 131 billion, while the cumulative value exceeded Rs. 200 lakh crore (Ministry of Finance, 2025).

However, the rapid expansion of the digital payments ecosystem has also produced a parallel expansion in digital financial risks and insecurities. As financial transactions, banking services, and payment infrastructures increasingly migrate online, concerns surrounding the security of personal and financial data have become vital. Cyber fraud today extends beyond isolated technical breaches and includes phishing, identity theft, fraudulent payment links, fake loan and investment applications, SIM-swap fraud, and unauthorised access to banking credentials. The growing dependence on online financial platforms has simultaneously widened the scope for financially motivated cybercrime. According to the India Cyber Threat Report 2023 by the Data Security Council of India and SEQRITE (2023), the country records an average of 761 cyber threat detections every minute. Official statistics further indicate that reported cybersecurity incidents increased from 10.29 lakh in 2022 to 22.68 lakh in 2024, reflecting both the expanding reach of digital financial infrastructure and the increasing sophistication of cyber threats (Press Information Bureau, 2025). In this evolving environment, digital financial security is no longer merely a technical concern for institutions or regulators; rather, it has become a crucial aspect of everyday financial behaviour, shaping how individuals engage with trust, and navigate digital financial systems.

It is in this context that the question of trust becomes central to understanding digital financial behaviour. Research consistently shows that users' willingness to adopt and sustain engagement with digital payment platforms is deeply tied to how safe they perceive those platforms to be. Aljaradat and Shukla (2025), in a study of digital payment adoption in India, found that trust and perceived cybersecurity form the foundation of digital payment usage. Users are unlikely to adopt or consistently use digital platforms if they doubt the safety of their financial data or transactions. Understanding where Indians stand on this question – how deeply they are embedded in the digital financial ecosystem, how they use it, and how safe they feel within it – has direct implications for understanding the scale and depth of their usage patterns. Such understanding can help in policymaking or course correction.

Against this backdrop, this chapter examines the online financial behaviour of Indians – mapping how deeply they are integrated into the digital ecosystem. It further discusses the extent of exposure to social media, digital banking, online investment and loan services among Indians. Additionally, the chapter analyses the usage of various digital payment modes such as UPI, NEFT/RTGS, cards, and wallets, and the purposes for which they are used. It also explores how safe Indians perceive different online banking channels, telecom services, and social media platforms to be. The chapter concludes by listing significant findings and suggestions for policy relevance.

7.1 How India Pays: Modes and Purposes of Online Transactions

When asked about their frequency of UPI usage, half of the respondents (49%) reported daily use of UPI, while a quarter (24%) used UPI only once or twice a week (**Table 7.1**). Close to one-fifth (17%) also said that they had never used UPI. Upon inquiring about the use of mobile banking apps and/or net-banking websites, those who used them daily dropped to 22 percent, indicating limited popularity of these modes of banking. In fact, over a third of the respondents (34%) reported that they had never used either mobile banking apps or net-banking websites.

When asked about their engagement with online investment and financial services such as fixed deposits, mutual funds, and stock trading, it was found that the majority of respondents are unlikely to be frequent users of such services. Well over half of the respondents (55%) reported having "never" used these services, while only about one-tenth (9%) said that they used them daily (**Table 7.1**). The usage of digital loan apps is even lower, with two in three respondents (66%) saying that they had "never" used them, in contrast to only five percent who reported using them daily. These figures suggest that while UPI has achieved widespread penetration, more specialised financial services have not yet become a popular use case for most Indians.

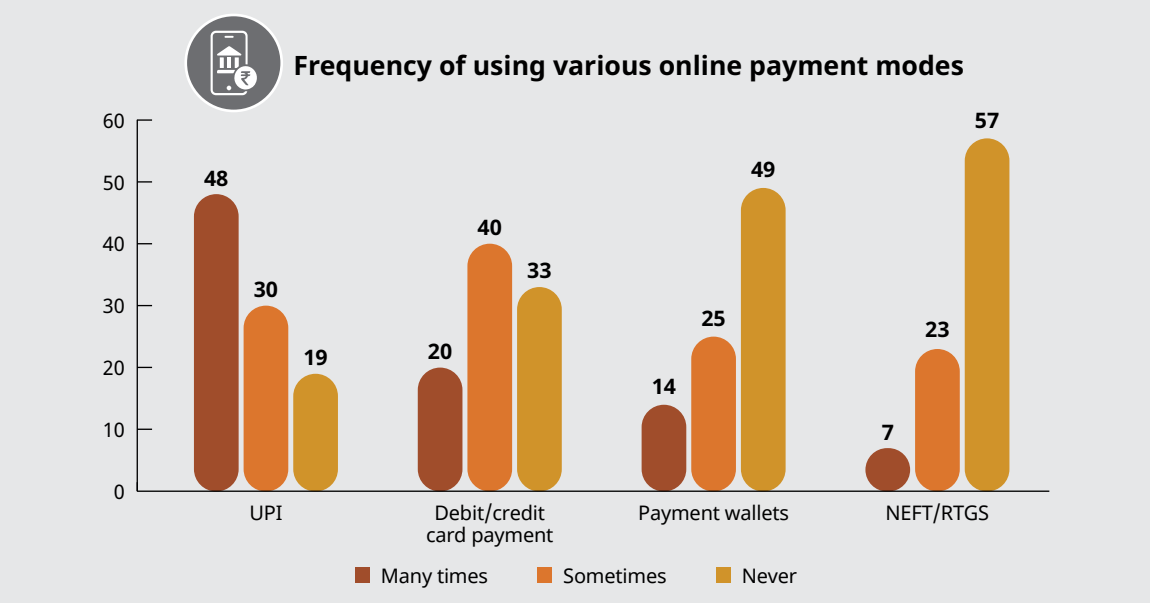
When asked about various modes used for making online payments, UPI emerges as the most popular option. Close to half of all respondents (48%) said that they used UPI "many times" for online payments, while about three in ten (30%) said that they used it "sometimes" and a fifth (19%) have "never" used UPI (**Figure 7.1**). Debit and credit card payments stood in distant second place, with one in five respondents (20%) reporting very frequent use, two in five (40%) using them "sometimes", and a third (33%) having "never" used them. Payment wallets were used "many times" by only about one in seven respondents (14%), a quarter use them "sometimes" (25%), and nearly half (49%) have "never" used them.

Table 7.1: One out of two respondents use UPI apps daily

Usage of...	Frequency of use			
	Daily	Once or twice a week	Once or twice a month	Never
UPI	49	24	8	17
Mobile banking apps/net-banking websites	22	25	15	34
Online investment or other financial services (FDs, mutual funds, stock trading, etc.)	9	18	13	55
Digital loan apps (LazyPay, MoneyTap, etc.)	5	11	12	66

Note: All figures are in percentages. The rest did not respond.
Question asked: How often do you use the following – daily, once or twice a week, once or twice a month, or never?

Figure 7.1: Almost half of the respondents use UPI frequently to make online payments

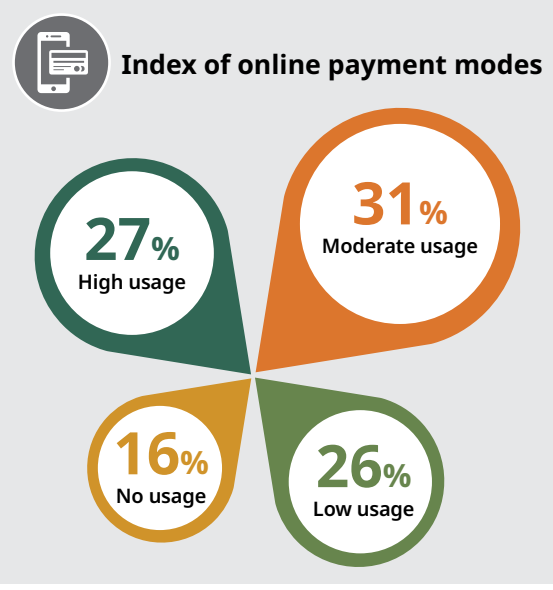


Note: All figures are in percentages. The rest did not respond. The categories 'never' and 'I don't make online payments' are merged to form the 'never' category.

Question asked: When making payments online, how frequently do you use the following: a) UPI b) NEFT/RTGS c) Debit/credit card payment d) Payment wallets – many times, sometimes, or never?

NEFT/RTGS was the least used mode while making payments online – only seven percent of respondents used it "many times", and nearly a quarter (23%) used it "sometimes", whereas well over half (57%) had "never" used it at all. These figures collectively point to UPI's dominant position in India's online payments landscape, with more traditional and institutional modes of transfer such as NEFT/RTGS remaining largely outside the everyday use of most users.

Figure 7.2: Over a quarter have high usage of online payment



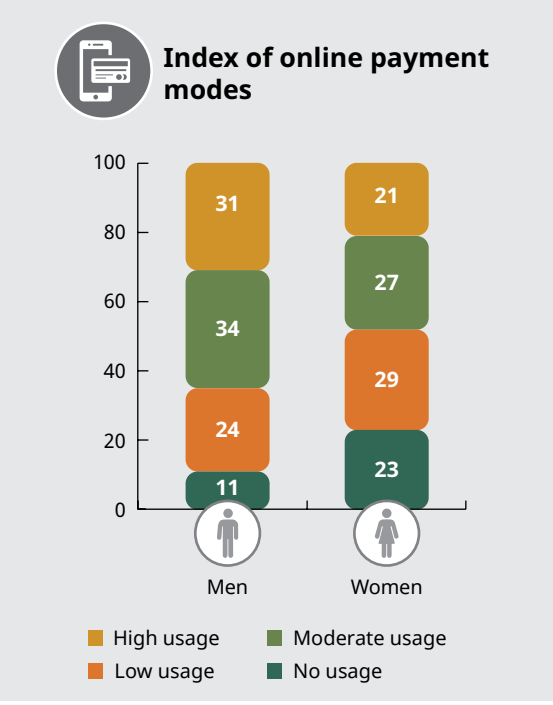
Note: All figures are in percentages. Please refer to Appendix 3 to see how the index was created.

Question asked: When making payments online, how frequently do you use the following: a) UPI b) NEFT/RTGS c) Debit/credit card payment d) Payment wallets – many times, sometimes, or never?

An index of online payment modes was created to better understand the usage of online payments via the usage of UPI, debit/credit card, payment wallets and NEFT/RTGS. The data shows that 16 percent of the respondents have not used any online payment modes, 26 percent have low usage, 31 percent have moderate usage, and 27 percent have high usage (**Figure 7.2**).

When examined by gender, men are noticeably more likely to use online payments than women. About one in three men (31%) reported high usage of online payment options, compared to one in five women (21%) (**Figure 7.3**). On the other hand, about one in four women (23%) reported no usage of online payment modes while the corresponding figure for men was nearly half of that of women, at 11 percent. This gender gap in the use of online payment options reflects continued disparities in women's participation in India's digital financial ecosystem.

Figure 7.3: Men are more likely to use online payment modes than women



Note: All figures are in percentages. Please refer to Appendix 3 to see how the index was created.

Question asked: When making payments online, how frequently do you use the following: a) UPI b) NEFT/RTGS c) Debit/credit card payment d) Payment wallets – many times, sometimes, or never?

The class-based divide in the use of online payment modes is even more pronounced. Among those from poor economic backgrounds, only 16 percent reported high usage of online payment options (**Table 7.2**). However, as the economic status improves, the proportion of frequent users rises steadily – about one in four among the lower-class respondents (23%), about one in three among the middle-class respondents (33%), and over two-fifths among the rich respondents (42%). Conversely, nearly three in ten respondents (27%) from poor economic households reported no use of online payment modes, and this figure dropped to eight percent amongst the rich.

The urban-rural divide in the use of online payment modes, while present, is somewhat less pronounced than the class-based gap. About three in ten urban respondents (29%) reported high usage of online payment options, compared with 18 percent of rural respondents – a difference of 11 percentage points (**Figure 7.4**). While the gap between rural and urban residents is meaningful, it is still smaller than one might expect, suggesting that online payment modes, particularly UPI, have achieved reasonably broad reach even in rural areas.

When examined by age, the data predictably points to higher usage among younger cohorts – about three in ten of those between 18 and 25 years of age (29%) frequently used various online payment options. Similar trends were observed among those between 26 and 35 years of age (33%) as well as those between 36 and 45 years of age (30%) (**Figure 7.5**).

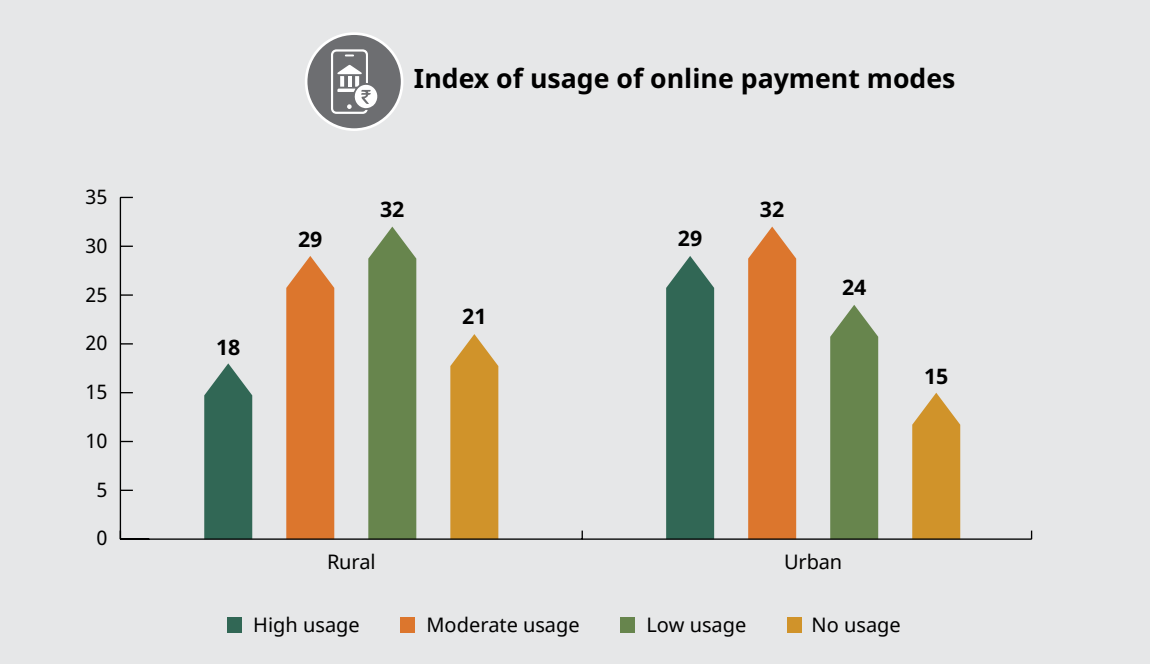
Table 7.2: Higher-income respondents are substantially more likely to report high use of online payment modes

Class	Index of usage of online payment modes			
	High usage	Moderate usage	Low usage	No usage
Poor	16	26	31	27
Lower	23	33	29	15
Middle	33	31	25	11
Rich	42	35	14	8

Note: All figures are in percentages. Please refer to Appendix 3 to see how the index was created.

Question asked: When making payments online, how frequently do you use the following: a) UPI b) NEFT/RTGS c) Debit/credit card payment d) Payment wallets – many times, sometimes, or never?

Figure 7.4: Urban residents are more likely to use online payment methods than rural residents

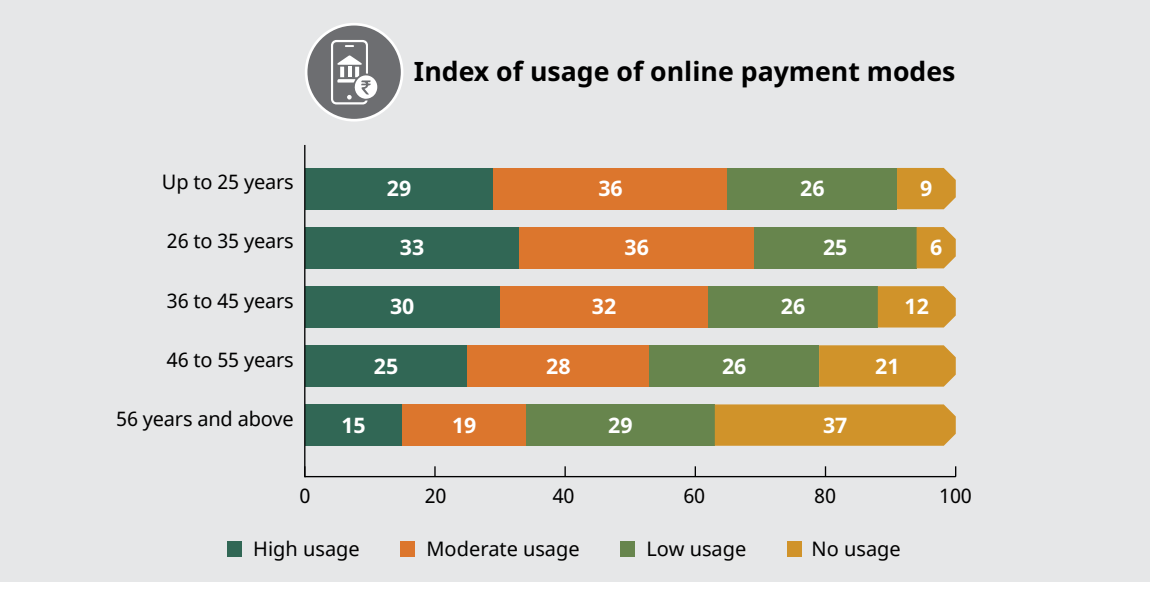


Note: All figures are in percentages. Please refer to Appendix 3 to see how the index was created.
Question asked: When making payments online, how frequently do you use the following: a) UPI b) NEFT/RTGS c) Debit/credit card payment d) Payment wallets – many times, sometimes, or never?

With older age groups, the proportion of frequent users of online payment methods declines consistently – from one in four among those between 46 and 55 years (25%) to 15 percent among those aged 56 years and above.

The data on the purposes for which online payments are made reveals that routine utility-centric transactions dominate the digital payments landscape in India. Bill payments for electricity, water, mobile recharges, etc.

Figure 7.5: High usage of online payment methods peaks among those aged 26 to 35 years



Note: All figures are in percentages. Please refer to Appendix 3 to see how the index was created.
Question asked: When making payments online, how frequently do you use the following: a) UPI b) NEFT/RTGS c) Debit/credit card payment d) Payment wallets – many times, sometimes, or never?

Table 7.3: Over one-third people regularly make online payments to pay bills as well as sending to or receiving money from family

Using online payments for...	Frequency of use of online payment modes		
	Regularly	Sometimes	Never
Bill payments (electricity, water, mobile recharge, etc.)	36	36	26
Sending/receiving money to/from family	34	37	25
Online shopping for groceries and other items (Flipkart, Amazon, etc.)	30	37	29
Rent, fees, or EMIs	25	32	38
Booking a ticket or travel	19	29	45
International transactions	6	10	69

Note: All figures are in percentages. The rest did not respond. The categories 'never' and 'I don't use online payments' are merged to form the 'never' category.

Question asked: How frequently do you make online payments for the following purposes – regularly, sometimes, or never?

(36%) and family remittances (34%) are the most common and regular use cases for making online payments (**Table 7.3**). Online shopping for groceries and other items was also widely reported, with three in ten respondents (30%) doing so "regularly". The use of online payments for paying rent, fees, and/or EMIs was somewhat lower – about a quarter (25%) used online payments "regularly", while nearly two-fifths (38%) "never" used them at all for paying rent, fees, EMIs, etc. Regular use is even lower for booking a ticket or travel (19%), whereas international transactions remain the least common use of online payments, with only six percent of respondents using them regularly.

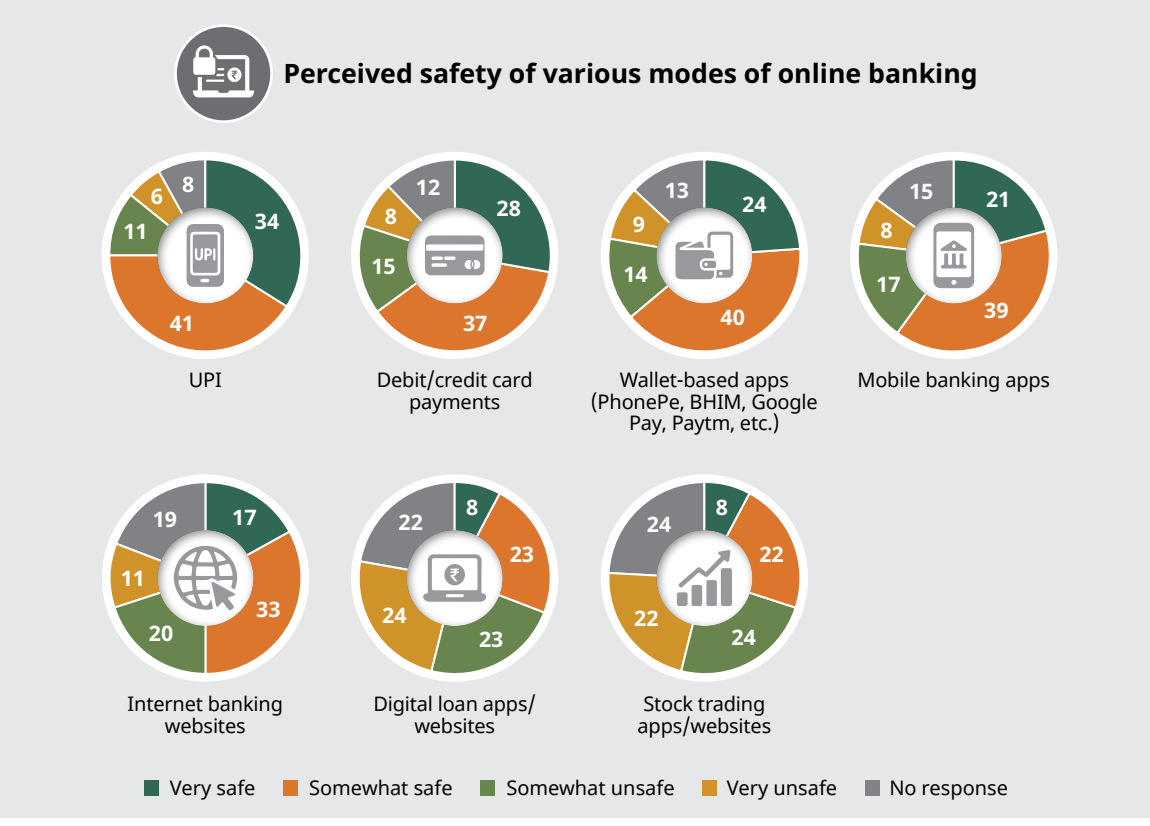
7.2 Perceptions of Safety in Online Payment Modes

When asked about the perceived safety of various modes of online banking, UPI received the highest safety ratings among all the platforms examined. Over a third of the respondents (34%) found it to be "very safe", and another two in five (41%) reported it to be "somewhat safe", bringing the combined positive perception to about three-fourths of the respondents – 75 percent (**Figure 7.6**). The perceived safety of UPI was followed by debit and credit card payments, with two-thirds of the respondents (65%) considering them to be safe (combining "very safe" - 28% and "somewhat safe" - 37%). Wallet-based apps followed a similar pattern, with nearly two in every three respondents (64%) believing them to be safe (combining "very safe" - 24% and "somewhat safe" - 40%).

Perceptions of safety dropped further for mobile banking apps and internet banking websites, where the combined proportion perceiving these modes as safe decreased to 60 percent and 50 percent, respectively (**Figure 7.6**). The greatest safety concern was directed at digital loan apps and stock trading apps/websites, where only eight percent in each case rated the modes as "very safe", while the combined proportion of perceived risk was reported to be 47 percent and 46 percent respectively ("very unsafe" and "somewhat unsafe" combined). While UPI and card payments occupy a position of relative trust, more specialised platforms continue to attract substantial scepticism as well as limited use.

To better understand the perceptions about the safety of various modes of online banking, an

Figure 7.6: UPI is considered extremely safe for online banking by over a third of the respondents



Note: All figures are in percentages.

Question asked: In your opinion, how safe are these modes of online banking – very safe, somewhat safe, somewhat unsafe, or very unsafe?

index was created by adding up the responses on the perceived safety of UPI, mobile banking apps, internet banking websites, debit/credit card payments and wallet-based apps (PhonePe, BHIM, Google Pay, Paytm, etc.). The data shows that 37 percent perceive these modes of online banking to be unsafe (combining 12% "very unsafe" and 25% "somewhat unsafe"), whereas a majority – 63 percent (combining 23% "very safe" and 40% "somewhat safe") – consider it to be safe (**Figure 7.7**).

As seen in **Chapter 8**, ten percent of the respondents have a high likelihood of responding to unsolicited calls or messages (**Figure 8.3**). Here, respondents' perception of safety while using online banking apps has been analysed against their vulnerability vis-à-vis unsolicited calls or messages. The data suggests that those respondents who are more vulnerable to potential frauds also tend to report higher perceived safety of various modes of online banking.

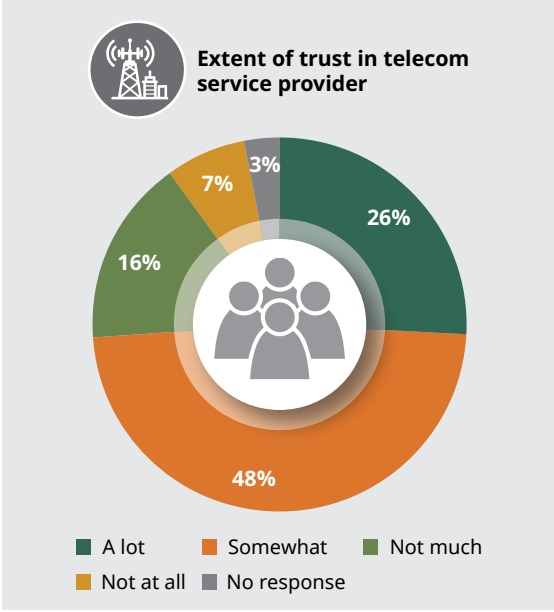
Figure 7.7: Over three in five respondents perceive online banking methods to be safe

Note: Please refer to Appendix 3 to see how the index was created.

Question asked: In your opinion, how safe are these modes of online banking: UPI, mobile banking apps, internet banking websites, debit/credit card payments and wallet-based apps (PhonePe, BHIM, Google Pay, Paytm, etc.) – very safe, somewhat safe, somewhat unsafe, or very unsafe?

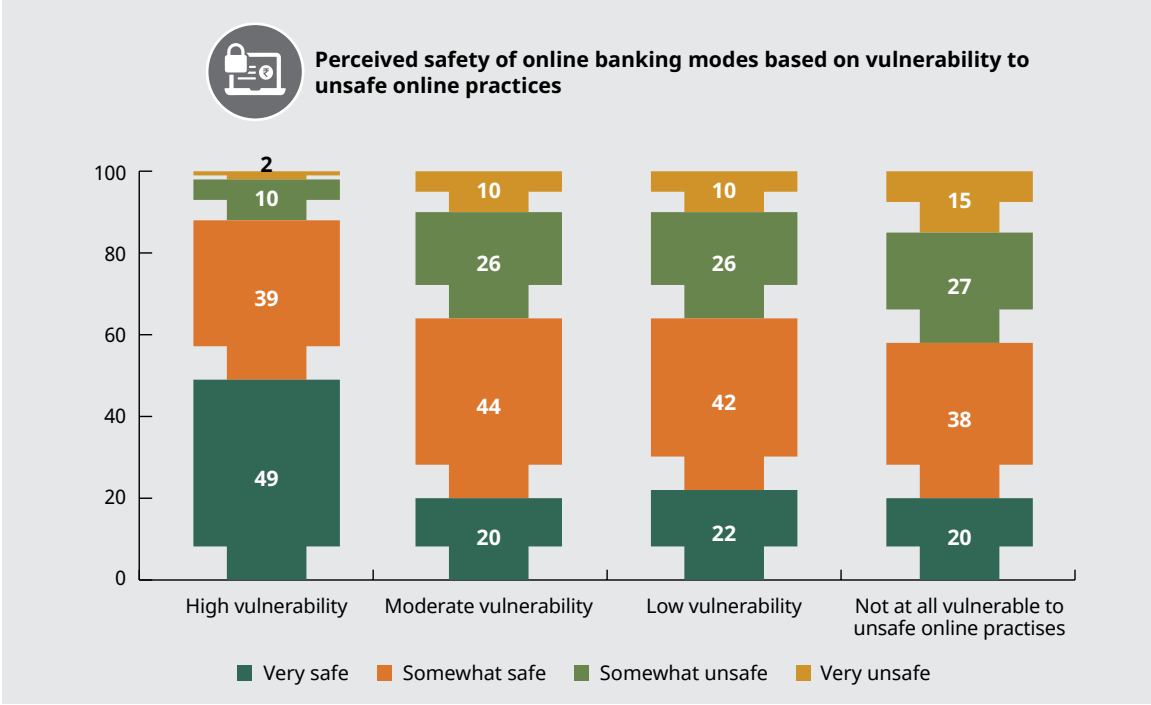
This means that those who have a high likelihood of clicking on unknown links, opening unknown files, or sharing OTPs on unknown calls, etc., are also more likely to perceive various modes of online banking as safe. Amongst the respondents with high vulnerability to unsolicited calls/texts, about half (49%) rated modes of online banking to be "very safe" and another four in ten (39%) rated them to be "somewhat safe" (**Figure 7.8**). In contrast, among those who were the least likely to act on unsolicited attempts at contact, only about one in five respondents (20%) considered online banking to be "very safe". This points to a noteworthy trend – those who are most vulnerable to cyber fraud are simultaneously the most confident in the safety of online banking platforms. This confluence of low digital vigilance and high confidence in the safety of online payment modes creates a fertile ground for cybercrime. This further underscores the importance of designing awareness campaigns that foster a realistic and calibrated sense of risk.

Figure 7.9: Just a little over one-fourth of people fully trust their telecom service provider to keep their personal information safe



Question asked: How much do you trust your telecom service provider to keep your number and related personal information safe – a lot, somewhat, not much, or not at all?

Figure 7.8: Those most vulnerable to unsafe online practices are also the most likely to consider online banking very safe



Note: All figures are in percentages. Please refer to Appendix 3 to see how the index was created.

Question asked: If you receive any of the following from an unknown person or number, will you do the following: a) Click on a link that you received c) Open a photo, video or other type of file d) Press a button or number if an unknown caller asks you to do that e) Share an OTP with the caller – yes, mostly; yes, sometimes; or never?

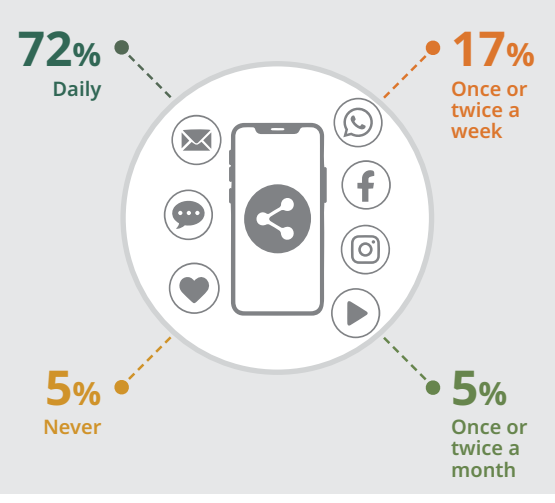
Question asked: In your opinion, how safe are these modes of online banking: a) UPI b) Mobile banking apps c) Internet banking websites d) Debit/credit card payments g) Wallet-based apps – very safe, somewhat safe, somewhat unsafe, or very unsafe?

When asked about the extent to which they trusted their telecom service provider to keep their numbers and personal information safe, only a little more than a quarter of the respondents (26%) said that they trusted their telecom provider "a lot", while close to half of the respondents (48%) reported moderate trust (**Figure 7.9**). However, about one in six respondents (16%) also said that they did not trust their telecom service providers much, and another seven percent reported not trusting them at all. Given the widespread prevalence of telecom-related frauds and the pivotal role played by the telecom providers in securing communication infrastructure and helping prevent frauds, the finding that close to three quarters of respondents (74% combining "a lot" and "somewhat" trust) expressed a high or moderate level trust in their telecom providers is a noteworthy indicator of public confidence in telecom providers' ability to safeguard personal information.

7.3 Use of Social Media and Perceptions of Safety

Social media platforms, financial digital apps and services often become the site of financial cyber fraud and other types of cybercrime. Thus, this survey included questions on people's exposure to various digital platforms and services. The results indicate high levels of daily engagement with social media platforms, with about three-fourths of the respondents (72%) reporting daily use of apps like WhatsApp, Instagram, Facebook, etc. (**Figure 7.10**).

Figure 7.10: About three in four respondents use social media apps/ websites daily

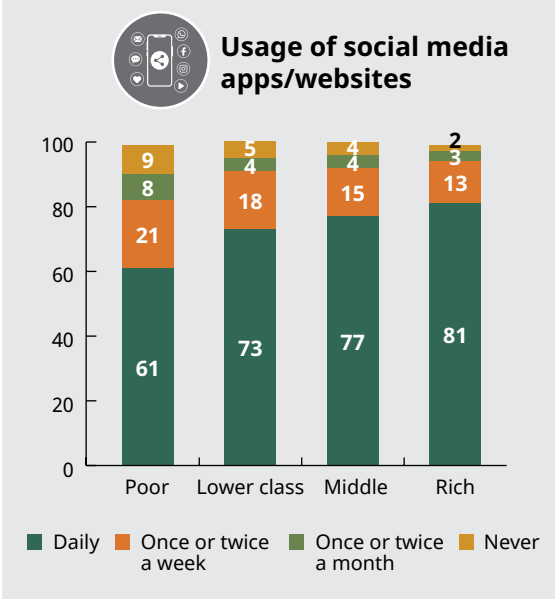


Note: The rest did not respond.

Question asked: How often do you use social media apps/ websites (WhatsApp, Instagram, Facebook, etc.) – daily, once or twice a week, once or twice a month, or never?

Upon analysing these responses across the economic classes, it is observed that those belonging to economically affluent backgrounds are more exposed to the everyday use of social media. While three in five respondents (61%) from poor economic backgrounds reported daily use of social media apps and websites, the figure increased by 20 percentage points to about four in five (81%) among those who were rich (**Figure 7.11**). Conversely, the limited usage of social media apps and websites also decreased with economic affluence, indicating that the social media is consumed more by those from economically well-off backgrounds.

Figure 7.11: Richer respondents are more likely to use social media apps daily

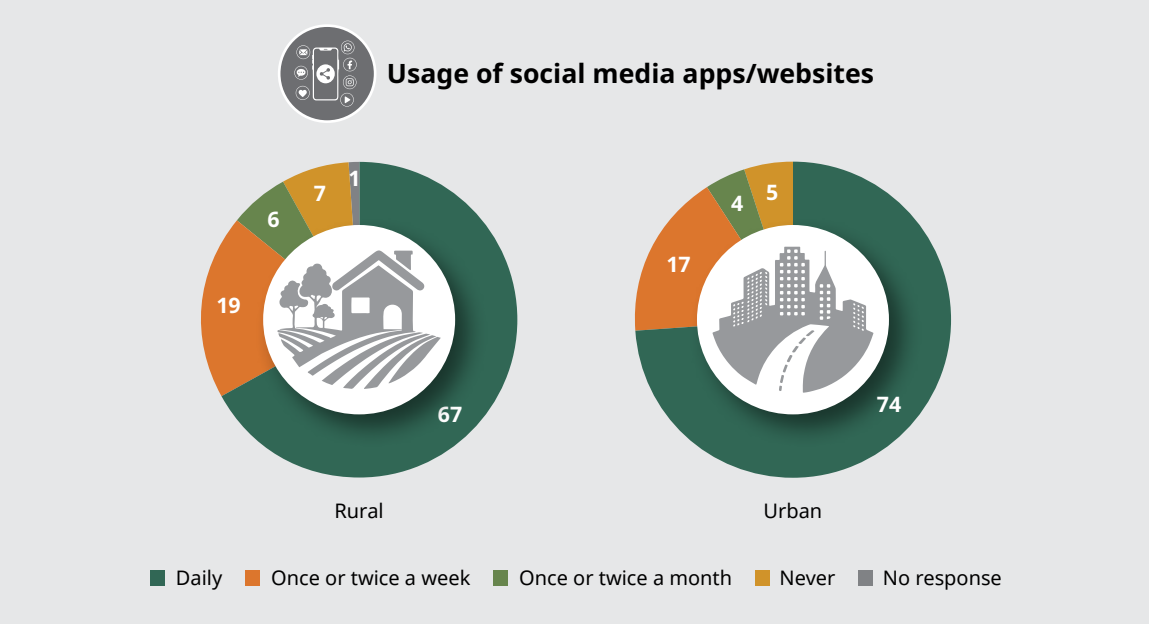


Note: All figures are in percentages. The rest did not respond.

Question asked: How often do you use social media apps/websites – daily, once or twice a week, once or twice a month, or never?

When these responses are examined across locality, it emerges that urban residents are slightly more exposed to the use of social media than their rural counterparts. While three-fourths of the urban respondents (74%) reported using social media apps and websites

Figure 7.12: Urban residents are more likely to use social media platforms daily compared to rural residents



Note: All figures are in percentages.
Question asked: How often do you use social media apps/websites – daily, once or twice a week, once or twice a month, or never?

daily, the figure dropped by seven percentage points to about two in three (67%) among rural respondents (**Figure 7.12**).

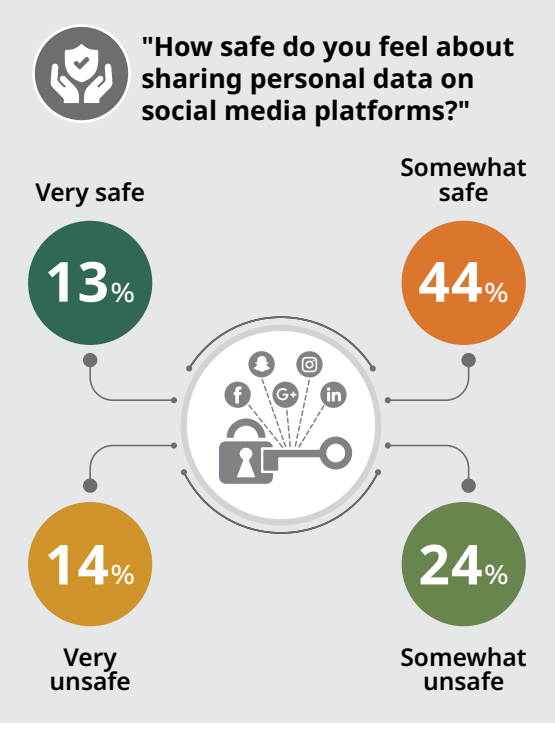
When social media usage is examined by age, a consistent and steep decline is visible as respondents grow older. Nearly nine in ten respondents between 18 and 25 years of age (88%) reported using social media daily, followed closely by those among the 26 to 35 years age group (83%) (**Table 7.4**). However, the proportion of those who frequently use social media begins to fall notably in the 36 to 45 years age group (75%), as well as 46 to 55 years age group (62%). Among those aged 56 years and above, fewer than half (45%) reported using social media daily, and in fact, about one in six (16%) said they never used social media at all. This consistent age-based decline points to lower digital engagement among older Indians, but it also indicates a more fundamental gap in familiarity with digital platforms.

Table 7.4: Daily use of social media apps/websites declines sharply among older age groups

Age	Usage of social media apps/websites			
	Daily	Once or twice a week	Once or twice a month	Never
Up to 25 years	88	10	1	1
26 to 35 years	83	12	3	2
36 to 45 years	75	19	3	3
46 to 55 years	62	23	6	8
56 years and above	45	27	11	16

Note: All figures are in percentages. The rest did not respond.
Question asked: How often do you use social media apps/websites – daily, once or twice a week, once or twice a month, or never?

Figure 7.13: Close to three in five people feel either fully or partially safe in sharing their personal data on social media platforms



Note: The rest did not respond.

Question asked: How safe do you feel about sharing or posting personal data on social media platforms – very safe, somewhat safe, somewhat unsafe, or very unsafe?

When respondents were asked about how safe they felt about sharing or posting their personal data on social media platforms, a majority of them expressed at least some sense of safety. About one in eight (13%) said that they felt "very safe" and another 44 percent said that they felt "somewhat safe" (**Figure 7.13**). However, about a quarter of the respondents (24%) also felt "somewhat unsafe", and 14 percent felt "very unsafe". There is very little variation across gender and age groups in the perception of safety regarding sharing personal data on social media platforms.

7.4 Patterns of Use of Digital Services and Cybercrime Victimisation

When the frequency of UPI usage is examined alongside cybercrime victimisation, it emerges that among those who used UPI frequently, 16 percent had reportedly been a victim of cybercrime in the last two to three years, compared to seven percent of those who never used UPI (**Table 7.5**). This points to a consistent trend where frequent UPI users are somewhat more likely to report having experienced cybercrime, possibly reflecting their greater exposure to digital payment transactions and related risks.

However, this trend is not so sharp when we look at the overall usage of online payment modes amongst victims and non-victims. While there is a slight variation with victims of cybercrimes being slightly more likely to use various kinds of online payment modes, the difference is not significant. In other words, apart from UPI, usage of other online payment modes has little impact on the likelihood of the users being victims of cybercrimes.

Table 7.5: Those who use UPI regularly are more prone to becoming victims of cybercrimes than those who do not use it

Usage of UPI	"Have you been a victim of a cybercrime in the last 2-3 years?"	
	Yes	No
Many times	16	81
Sometimes	12	85
Never	7	89

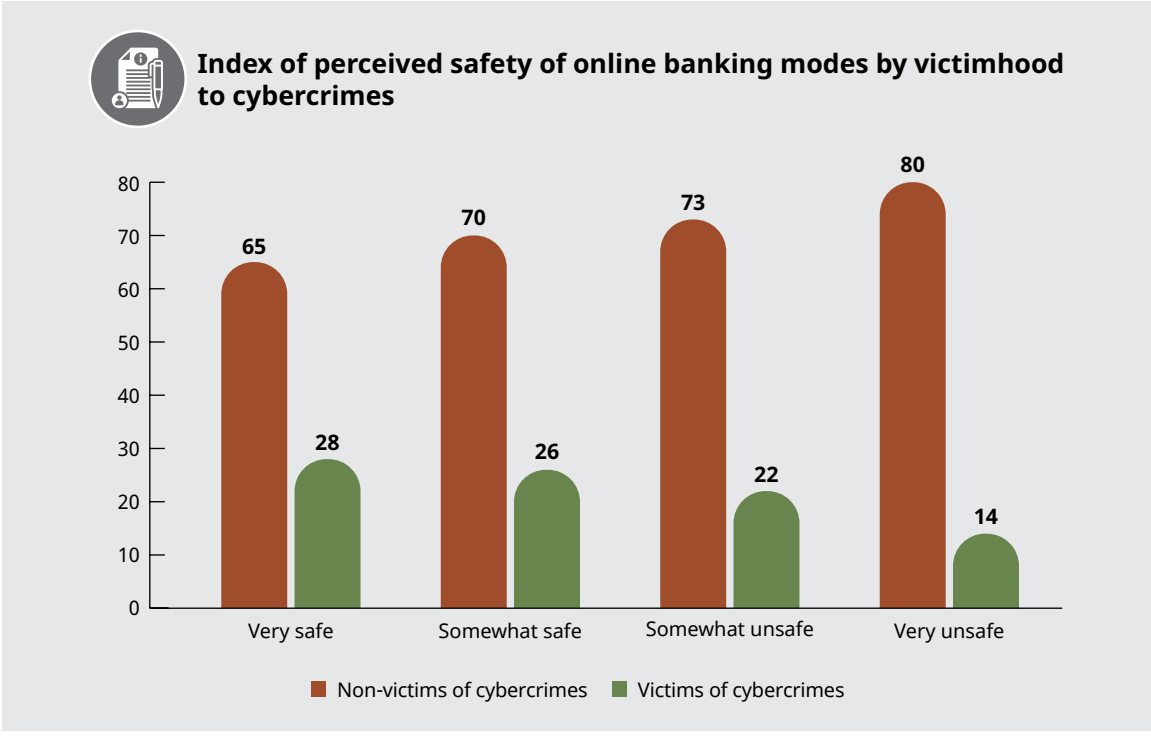
Note: All figures are in percentages. The rest did not respond. The categories 'never' and 'I don't make online payments' are merged to form the 'never' category.

Question asked: Have you been a victim of a cybercrime in the last 2-3 years?

Question asked: When making payments online, how frequently do you use UPI – many times, sometimes, or never?

When the index of perceived safety of various online banking modes is examined alongside cybercrime experience, it shows that those who rate various online banking platforms positively are more likely to either have been the victims or have closely helped the victims of cybercrime in the last 2-3 years. Among those who believed online banking modes to be "very safe", over one in every four respondents (28%) had either been a cybercrime victim or a close aide of the victim (**Figure 7.14**).

Figure 7.14: Those who consider online banking to be safe are more likely to be victims of cybercrimes



Note: All figures are in percentages. The rest did not respond. Please refer to Appendix 3 to see how the index was created.

Question asked: Have you been a victim of a cybercrime in the last 2-3 years; or did you help the victim closely in registering the cyber complaint or in handling the overall issue?

Question asked: In your opinion, how safe are these modes of online banking: a) UPI b) Mobile banking apps c) Internet banking websites d) Debit/credit card payments g) Wallet-based apps – very safe, somewhat safe, somewhat unsafe, or very unsafe?

On the other hand, among those who considered online banking modes to be "very unsafe", the proportion of victims or the close aides of victims dropped by half (14%). Furthermore, amongst those who considered online banking to be "very safe", 65 percent of respondents had not been victims of cybercrimes, while the corresponding figure amongst those who felt it was "very unsafe" was higher, at 80 percent. In other words, those who positively perceive the safety of various online banking modes are more likely to fall prey to cybercrime victimisation.

When looking at the relationship between perceived safety in sharing personal data on social media platforms and victimisation to cybercrime, the data reveals a marginal difference. Those who feel very safe in sharing personal data on social media are slightly more likely to have been victims of cybercrimes in the recent past. Among those who reported feeling "very safe" in sharing their personal information on social media, about one in five of them (19%) had been a victim of a cybercrime in the last 2-3 years, while amongst those who felt "very unsafe", the corresponding figure was at 13 percent (**Table 7.6**). Conversely, the proportion of non-victims was also slightly higher among those who felt "very unsafe" (85%) than those who felt "very safe" (79%). This suggests a modest difference in the likelihood of being a victim of cybercrimes based on perceived sense of safety while sharing personal data online.

7.5 Conclusion

The findings of this chapter map the contours of how Indians engage with the digital financial ecosystem. Social media has achieved widespread penetration, with close to three-fourths of respondents using it daily, and UPI has firmly established itself as the dominant mode of online payment. However, engagement with more specialised platforms - mobile

Table 7.6: Those who feel very safe in sharing personal data on social media platforms are slightly more likely to have been a victim of cybercrime than those who felt very unsafe

Feel safe in sharing personal data on social media platforms?	"Have you been a victim of a cybercrime in the last 2-3 years?"	
	Yes	No
Very safe	19	79
Somewhat safe	12	84
Somewhat unsafe	14	84
Very unsafe	13	85

Note: All figures are in percentages. The rest did not respond.

Question asked: How safe do you feel about sharing or posting personal data on social media platforms – very safe, somewhat safe, somewhat unsafe, or very unsafe?

Question asked: Have you been a victim of a cybercrime in the last 2-3 years?

banking apps/internet banking websites, online investment services, and digital loan apps - remains considerably more limited, with a majority having never used the latter two at all. Cutting across all these dimensions is a persistent pattern of structural inequality: men, rich respondents, urban residents, and younger age groups consistently show deeper and more varied digital financial engagement. These divides are not merely descriptive; they define who is most integrated into - and therefore most exposed to - India's rapidly expanding digital financial world.

On the question of perceived safety, the chapter reveals a landscape that is reassuring on the surface but more complex beneath it. UPI, card payments and wallet-based apps inspire relatively broad confidence, yet this confidence is sharply stratified by class and age. More specialised platforms like digital loan apps and stock trading websites are both significantly less in use as well as attract widespread unease, suggesting that public trust in the digital financial ecosystem is far from uniform. Most strikingly, the data points to the high confidence in the safety of online payment modes amongst those who are more vulnerable to cyber risks, i.e., those who are more likely to open unknown links, share OTPs, etc.

The findings also suggest higher vulnerability to cybercrime victimisation amongst those who are UPI users. Those who perceive online banking methods as "very safe" are also twice as likely to have been victims of cybercrimes, compared to those who consider these platforms as "very unsafe". Similarly, those who feel safe in sharing personal data online are also slightly more likely to have been victims of cybercrimes in the recent past, compared to those who feel unsafe in sharing personal data. This suggests the crying need for building cyber resilience and preparedness amongst those who are the most at risk against cybercrimes, particularly in their use of the digital financial services.

These findings carry several implications. Initiatives aimed at expanding digital financial inclusion must be paired with targeted digital literacy programmes for women, older users, and lower income groups - those less integrated into digital finance but not necessarily less exposed to its risks. Cybersecurity awareness campaigns must move beyond informing users that threats exist, and focus on developing practical skills, risk awareness, and safer digital behaviours.

References

- Aljaradat, A., & Shukla, S. K. (2025). Trust and cybersecurity in digital payment adoption: Socioeconomic insights from India. *Journal of Business and Socio-economic Development, 5*(4), 382–386. https://doi.org/10.1108/JBSED-04-2025-0119

- Data Security Council of India & SEQRITE. (2023). *India cyber threat report 2023*. https://www.dsci.in/resource/content/india-cyber-threat-report-2023
- Marathe, V. (2025). Is India ready for the next wave of digital threats? *SPRF*. https://sprf.in/is-india-ready-for-the-next-wave-of-digital-threats/
- Ministry of Finance, Government of India. (2025, January). *Unified Payments Interface (UPI) provides an opportunity to other countries to learn from the Indian experience* [Press release]. Press Information Bureau. https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=2106794
- National Sample Survey Office. (2024, October). *Comprehensive annual modular survey, 2022–23*. Ministry of Statistics and Programme Implementation, Government of India. https://www.mospi.gov.in/sites/default/files/publication_reports/CAMS%20Report_October_N.pdf
- Press Information Bureau, Government of India. (2025, October 8). *Curbing cyber frauds in Digital India* [Press release]. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2176146
- The Hindu. (2026, January 29). India now has 958 million active internet users, 57% of these are from rural areas. https://www.thehindu.com/sci-tech/technology/india-now-has-958-million-active-internet-users-57-of-these-are-from-rural-areas/article70566646.ece

CHAPTER

08

QR code display at a local shop (Noida, Uttar Pradesh- November 26, 2021).
Photo By Pradeep Gaur/Shutterstock.

Cyber Hygiene in the Digital Age: Awareness and Adoption

Key Findings

- One out of five people (20%) reported not using 2-step verification while making transactions on UPI apps. Younger, more educated, urban and rich respondents are more likely to use 2-step verification on UPI apps compared to their counterparts.
- More than two in three respondents (68%) said that they never share an OTP or click a button when asked by an unknown person.
- One in ten people are highly vulnerable to responding to unsolicited calls or texts by an unknown person.
- One-fifth of the respondents (21%) reported always following secure cyber practises like avoiding public Wifi, checking app permissions, verifying website or app authenticity, etc. Another 21 percent said they "never" follow these practises. Younger, more educated and urban respondents are more likely to follow these practises compared to their counterparts.

Cyber Hygiene in the Digital Age: Awareness and Adoption

India ranks tenth in the world cybercrime index, developed by the University of Oxford and the University of New South Wales, UNSW (Bruce et al., 2024). From 2020 to 2026, India lost a staggering ₹52,976 crore due to cyber frauds (*Livemint,* 2026) and experienced a 217 percent increase in cybercrimes over five years, from 2018 to 2023 (Safer Internet India, 2025). In 2025 alone, the Indian Computer Emergency Response Team (CERT-In) handled over 29.44 lakh cyber incidents (Press Information Bureau, 2026). At the outset, these numbers show the pervasiveness of cybercrimes in India.

Everyday activities such as banking, shopping, accessing government services, and paying utility bills have increasingly become digital. In the last decade, India has witnessed an unprecedented transformation in the way individuals interact, transact, and communicate. Digital payments dominated India's financial ecosystem, accounting for nearly 99 percent of the entire transaction volume in the first half of 2025, and UPI accounted for 85 percent of transactions in terms of volume in the same period (*The Economic Times,* 2025).

With the simultaneous rise in cybercrime and the rapid expansion of digital financial systems, there emerges an urgent need to examine the precautions and security measures adopted by the users of these digital services. Against this background, the present chapter examines the use of security measures like 2-step verification for UPI or internet banking apps and the extent of cybersecurity awareness when it comes to attending unsolicited calls or texts. It further examines government outreach mechanisms for cybersecurity awareness and measures its impact, and lastly aims to understand the extent of adoption of digital hygiene measures.

8.1 The Security Apparatus for Everyday Financial Apps

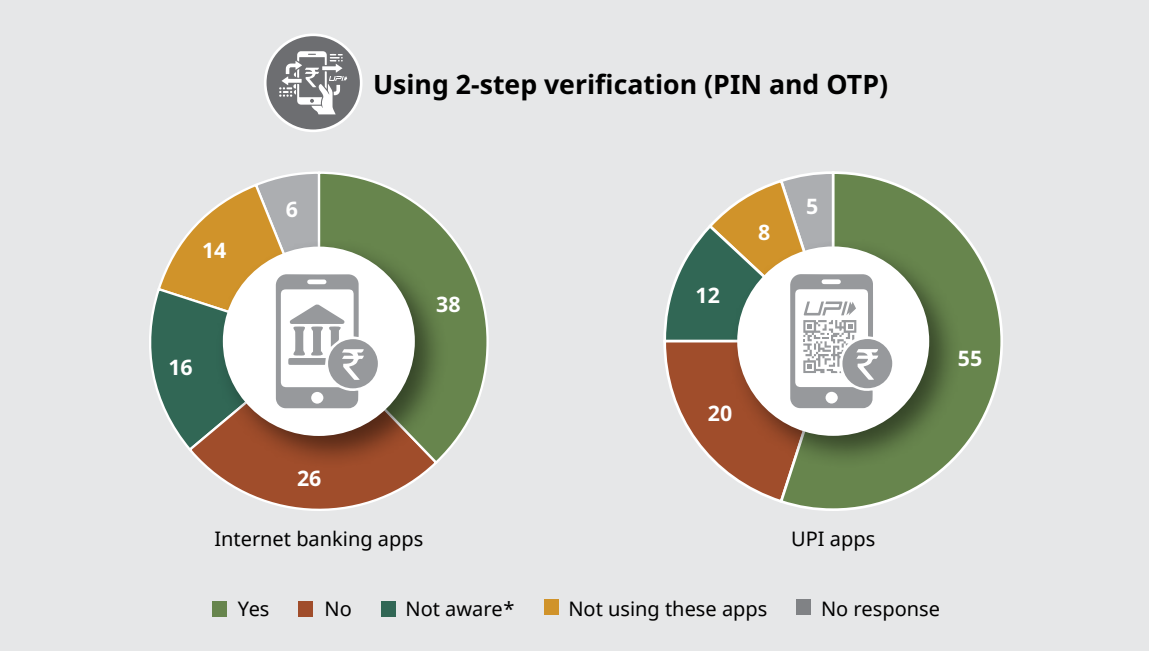
While a large majority appear to be using digital methods for online transactions, information on the type of security used for transactions is rather limited. To understand whether the respondents were aware of and used such protective measures, a question was posed asking them whether they used a 2-step verification system, such as PIN and OTP, on internet banking and UPI apps.

The findings reveal that 55 percent of the respondents used a two-step verification system in UPI apps, whereas 38 percent of the respondents enabled it for internet banking (**Figure 8.1**). On the other hand, a little over a quarter (26%) said they do not use it for internet banking, and one-fifth (20%) have not used it for UPI apps.

Importantly, 16 percent were not aware of two-step verification for internet banking and 12 percent were not aware in the case of UPI apps (**Figure 8.1**). Fourteen percent of the respondents have never used internet banking apps and eight percent have not used UPI apps. In sum, it can be said that UPI users are relatively more likely to employ protective measures as compared to users of internet banking apps.

The use of 2-step verification for digital payments was further examined across different age groups. The findings show that only three in ten (31%) of those aged 56 years and above used 2-step verification on UPI apps, as opposed to nearly seven out of ten respondents (68%) below 25 years of age (**Table 8.1**). This pattern is partly explained by lower overall usage of UPI apps among older respondents, where about a fifth of the oldest age group (20%) reported not using UPI apps at all, compared to only four percent among the youngest.

Figure 8.1: One out of five people reported not using 2-step verification while making transactions on UPI apps



*Note: All figures are in percentages. *The option "I don't know about this" was a silent option.*
Question asked: Do you have a 2-step verification system, like using PIN and OTP, on the Internet banking apps/UPI apps?"

There is a similar pattern observed in the use of 2-step verification for internet banking. The youngest age group, those between 18 and 25 years of age, are twice as likely to use 2-step verification for internet banking (45%) as those who are 56 years and above (21%) (**Table 8.1**). Here too, lower adoption of internet banking apps among older respondents is a contributing factor. Over a quarter (26%) of the oldest age group did not use internet banking, compared to only one in ten (11%) among the youngest.

Table 8.1: Younger respondents are more likely to use 2-step verification for banking and digital payments

Age groups	Internet banking apps		UPI	
	Use two-step verification	Don't use the app	Use two-step verification	Don't use the app
Up to 25 years	45	11	68	4
26 to 35 years	47	9	66	3
36 to 45 years	40	12	58	6
46 to 55 years	29	16	45	11
56 years and above	21	26	31	20

Note: All figures are in percentages. The figures reflect only the respondents who said "yes" to using the mentioned two-step verification process and those who said they "do not use these apps".

Table 8.2: College educated respondents are most likely to use two-step verification for internet banking and UPI apps

Education level	Internet banking apps		UPI	
	Use two-step verification	Don't use the app	Use two-step verification	Don't use the app
Non-literate	13	32	26	28
Up to primary	16	26	25	20
Up to matric	30	16	49	9
College and above	52	9	71	3

Note: All figures are in percentages. The figures reflect only the respondents who said "yes" to using the mentioned two-step verification process and those who said they "do not use these apps".

In addition to age, the education level also plays a role in determining whether a person is likely to use a 2-step verification system or not. The data shows that only a quarter (26%) of those without any formal education use a 2-step verification on UPI apps, and thirteen percent do so in internet banking. These proportions increase significantly as the educational levels increase, and the usage of two-step verification is most prominent among those with college degrees (71% for UPI apps and 52% for internet banking) **(Table 8.2**). Conversely, non-use is significantly higher among those without formal education: about a third did not use internet banking (32%) and 28 percent did not use UPI apps, compared to only nine percent of graduates who did not use internet banking and three percent who did not use UPI apps. Thus, the data suggests that more educated users are more likely to adopt the safer practice of 2-step verification while making digital transactions.

The data was also analysed across rural and urban locations, and a pattern emerged. Urban respondents are more likely to use two-step verification for internet banking and UPI apps than their rural counterparts. Four in ten (40%) urban respondents use two-step verification on their internet banking apps, in comparison to three in ten (29%) rural residents (**Table 8.3**). Similarly, 57 percent of the urban respondents use two-step verification for UPI compared to 48 percent in the rural areas. In terms of access, both of these apps are less likely to be used in rural areas than in urban areas. A fifth of the respondents in rural areas (20%) don't use internet banking apps, as opposed to 13 percent in urban areas, and 12 percent of the rural residents don't use UPI apps as compared to only seven percent in urban areas.

Data, when analysed across economic classes, showed an interesting pattern that as a person's financial capacity increased, so did their proclivity to use two-step verification for internet banking and UPI apps. Those at the bottom of the economic ladder were comparatively less likely to use these digital payment protections. In terms of internet banking apps, well over half (56%) of the rich respondents use two-step verification process, and within UPI, it is more than two in every three respondents from rich economic backgrounds (68%) (**Table 8.4**). In contrast, only a quarter of the economically disadvantaged use two-step verification for internet banking apps (24%), and more than two-fifths (43%) of the same use it for UPI apps. A fifth of the economically disadvantaged

Table 8.3: Urban respondents are more likely to use two-step verification for internet banking and UPI apps

Locality	Internet banking apps		UPI apps	
	Use two-step verification	Don't use the app	Use two-step verification	Don't use the app
Rural	29	20	48	12
Urban	40	13	57	7

Note: All figures are in percentages. The figures reflect only the respondents who said "yes" to using the mentioned two-step verification process and those who said they "do not use these apps".

don't use internet banking apps (20%), and 13 percent don't use UPI apps. In comparison, only nine percent of those from affluent backgrounds don't use internet banking apps, and five percent don't use UPI apps.

8.2 Understanding Unsolicited Calls/Text

According to a Truecaller Report 2025, Indians received more than four thousand crore spam calls in the year 2025, with India being the fifth most spam-hit country worldwide (*The Economic Times,* 2026b). As per the McAfee State of the Scamiverse report 2026, Indians receive an average of 13 scam messages per day (McAfee, 2026). With the proliferation of spam calls and messages, many of which may be potential cybercrime threats, it becomes important to understand people's vulnerability in the digital space.

One way to estimate this vulnerability is by assessing individuals' adherence to safe practices while using their devices, such as not sharing OTPs with unknown callers, not downloading images or videos received from unknown numbers, not clicking on unverified links, and avoiding merging calls or taking calls from unknown numbers.

Table 8.4: Rich respondents are more likely to use two-step verification for internet banking and UPI apps

Economic class	Internet banking apps		UPI apps	
	Use two-step verification	Don't use the app	Use two-step verification	Don't use the app
Poor	24	20	43	13
Lower	37	15	56	8
Middle	43	11	59	5
Rich	56	9	68	5

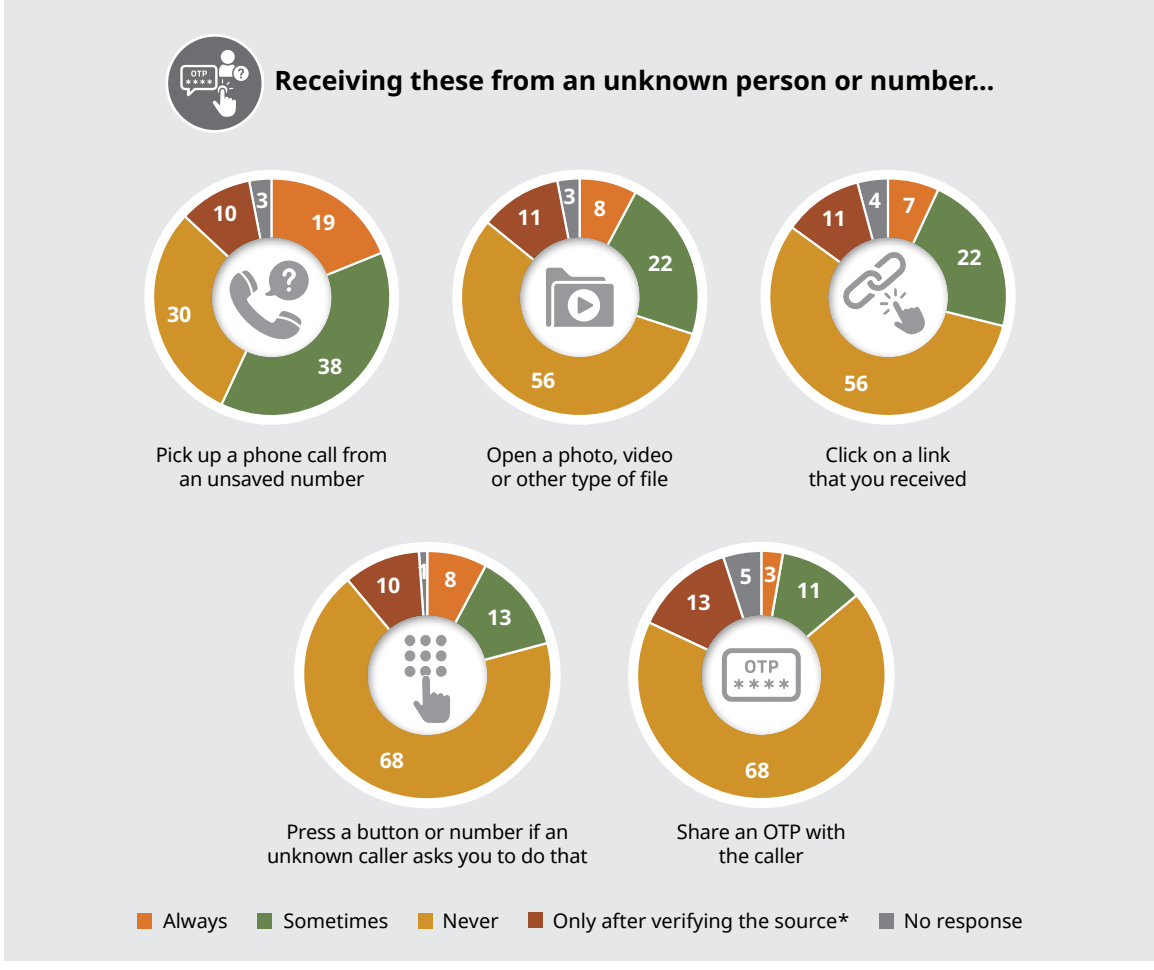
Note: All figures are in percentages. The figures reflect only the respondents who said "yes" to using the mentioned two-step verification process and those who said they "do not use these apps".

To understand the extent to which such practices are being adopted, the respondents were queried on the same. While a notable 30 percent of the respondents said that they 'never' answer calls from an unknown number, one-fifth (19%) said that they 'always' answer such calls (**Figure 8.2**). Ten percent said that they do so only after verifying the number. It should be noted that the option of "verifying the source" was not read out to the respondents and was provided as a silent option.

Respondents seem to be cautious when asked by a caller to click a button or share an OTP, with over two in three (68%) saying that they 'never' share an OTP or click a button, and one in ten do so only after 'verifying the source'. However, one-fifth (8% "always" and 13% "sometimes") reported clicking a button when asked by an unknown caller to do so, and 14 percent (3% "always" and 11% "sometimes") said they share OTPs with a caller (**Figure 8.2**).

When queried on whether they have clicked on a link received from an unknown number or opened a photo or video received from an unknown person, seven and eight percent of respondents, respectively, said that they

Figure 8.2: More than two in three respondents said that they will not share an OTP or click a button when asked by an unknown person



*Note: All figures are in percentages. *The option "I will do it only after verifying the source" was a silent option.*

Question asked: If you receive any of the following from an unknown person or number, will you do the following: Click on a link that you received from an unknown person or number/ Pick up a phone call from an unsaved number/ Open a photo, video or other type of file received from an unknown person or number/ Press a button or number if an unknown caller asks you do that/ Share an OTP with the unknown caller or number – yes, mostly; yes, sometimes; or never?

"always" do so, whereas 22 percent said that they click on such links or open such files "sometimes". The majority, 56 percent, said they "never" click on such links or open such files, while a little over one in ten (11%) reported that they only do these actions after verifying the source (**Figure 8.2**).

The data was used to create an index based on the following risk behaviours: opening a photo, video, or other unsolicited file; clicking on a link received from an unknown number; pressing a button when an unknown caller asks; and sharing an OTP with an unknown caller. The data suggests that one in ten of the respondents (10%) were highly vulnerable, while close to a quarter (23%) were moderately vulnerable (**Figure 8.3**). However, a majority of the respondents, more than two-fifths (44%), were not vulnerable at all.

The index was analysed by different demographics such as age, gender, and levels of urbanity; and the findings were flat, and no patterns were observed. However, when the data was cross-tabulated with individual questions, a few patterns were observed. Across educational levels of the respondents, those who are more educated are only marginally more likely to say that they never share an OTP with an unknown caller, compared to the non-literate and less educated respondents. Similarly, if an unknown person calls and asks the respondent to press a button or number, there is a slightly higher chance of a non-literate person doing so (22%) compared to a college graduate (18%).

Figure 8.3: One in ten people are highly vulnerable to responding to unsolicited calls or texts by an unknown person

Note: Please refer to Appendix 3 to see how the index was created.

Question asked: If you receive any of the following from an unknown person or number, will you do the following: a) Click on a link that you received c) Open a photo, video or other type of file d) Press a button or number if an unknown caller asks you to do that e) Share an OTP with the caller – yes, mostly; yes, sometimes; or never?

8.3 Analysing the Cybersecurity Awareness Landscape

On average, about a hundred people fall prey to cybercrime every hour in India (*The Economic Times,* 2026a). Against this background, creating awareness about cybercrime and motivating people to adopt protective behaviour becomes paramount. The central government has taken measures to spread awareness regarding cybercrime, such as the dissemination of awareness messages through SMS, social media handles of the Indian Cybercrime Coordination Centre (I4C), newspaper advertisements, radio campaigns, etc. (Press Information Bureau, 2024). In this section, we try to understand the level of exposure that the public has to these awareness campaigns.

The findings show that 21 percent of the respondents have received messages related to cybersecurity awareness, and a similar proportion (22%) has seen an advertisement on cybersecurity awareness (**Figure 8.4**). Forty-five percent of the respondents have both received a message and seen an advertisement related to cybersecurity awareness. Only a small minority, seven percent, have received none of them. From this, we can surmise that the dissemination process by the government usage of cyber hygiene practices quite robust when it comes to sending messages or displaying advertisements related to cybersecurity awareness.

Figure 8.4: Nearly half of the respondents have both received messages and seen advertisements on cybersecurity awareness

Note: The rest did not respond.

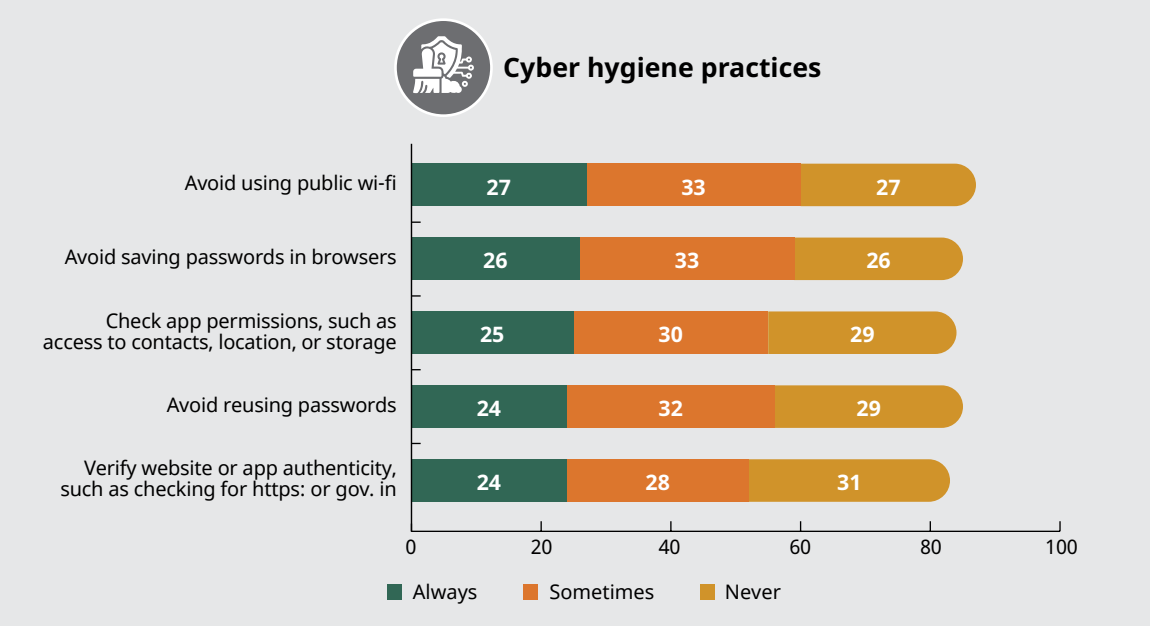
Question asked: These days, there are many advertisements and messages etc., to make people aware of the risks and cautions about cybersecurity. Have you received any such message or seen any such advertisement?

8.4 Extent of Digital Hygiene Practices

After every major cyber breach, security experts, government, and policymakers across the world call for the need to improve cyber hygiene. Cyber hygiene refers to the set of cybersecurity practices that online consumers are expected to adopt in order to safeguard the security and integrity of their personal information stored on internet-enabled devices from potential cyberattacks (Vishwanath et al., 2020). Some cyber hygiene practices include avoiding saving passwords in browsers, avoiding reusing passwords, regularly updating software, using antivirus and anti-malware software, etc. that one can take to protect personal information and devices from cyber threats.

Against this background, respondents were asked whether they practise the following cybersecurity measures regularly—avoiding using public Wi-Fi, avoiding saving passwords on browsers, checking app permissions before downloading, avoiding reusing passwords across platforms, and verifying website or

Figure 8.5: A quarter of respondents reported always following secure cyber practices



Note: All figures are in percentages. Rest did not respond.

Question asked: Do you take the following actions to protect your personal data: avoid saving passwords in browsers/ Avoid using public Wi-Fi/ Avoid reusing passwords/ Check app permissions such as access to contacts, location, or storage/Verify website or app authenticity such as checking for https: or gov.in – yes, always; yes, sometimes; no, never?

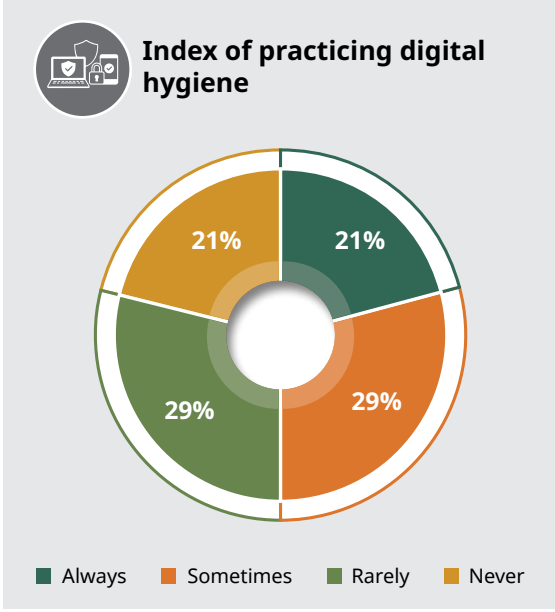
app authenticity before visiting the website or downloading the app. Nearly a quarter of the respondents said that they follow these practices "always" (**Figure 8.5**). Conversely, a marginally higher proportion of respondents said that they "never" follow such practices.

Over a quarter of the respondents said that they "always" avoid using public Wi-Fi (27%), and a third avoid using it "sometimes" (33%). Twenty-seven percent have "never" used this type of cyber hygiene practice. When it comes to avoiding saving passwords in browsers, a little over a quarter (26%) do it "always", and about one-third (33%) of the respondents do so "sometimes". In terms of checking app permissions, such as access to contacts, locations or storage, 25 percent of respondents said they do so "always", and about one-third (30%) do so "sometimes". A similar proportion (29%) have "never" checked their app permissions. A similar proportion of respondents reported "never" avoiding reusing passwords (29%) and "never" verifying the authenticity of a website or an app (31%) (**Figure 8.5**).

To get a deeper understanding, an index of digital hygiene was created, ranging from "never" using digital hygiene to "rarely", "sometimes" and "always" practising digital hygiene. For this, all the questions on cyber/digital hygiene were used, such as avoiding saving passwords in browsers, avoiding reusing passwords, checking app permissions, avoiding using public Wi-Fi and checking the authenticity of websites. After creating the index, the data shows that nearly a fifth (21%) have "never" practised any digital hygiene, whereas another comparable proportion (21%) said that they have "always" practised it. On the other hand, about three in ten said they practise it "rarely", and another corresponding proportion said they practise digital hygiene "sometimes" (29% both) (**Figure 8.6**).

The digital hygiene practices have been further analysed across various socio-demographic factors.

Figure 8.6: A fifth of the respondents have never practised digital hygiene



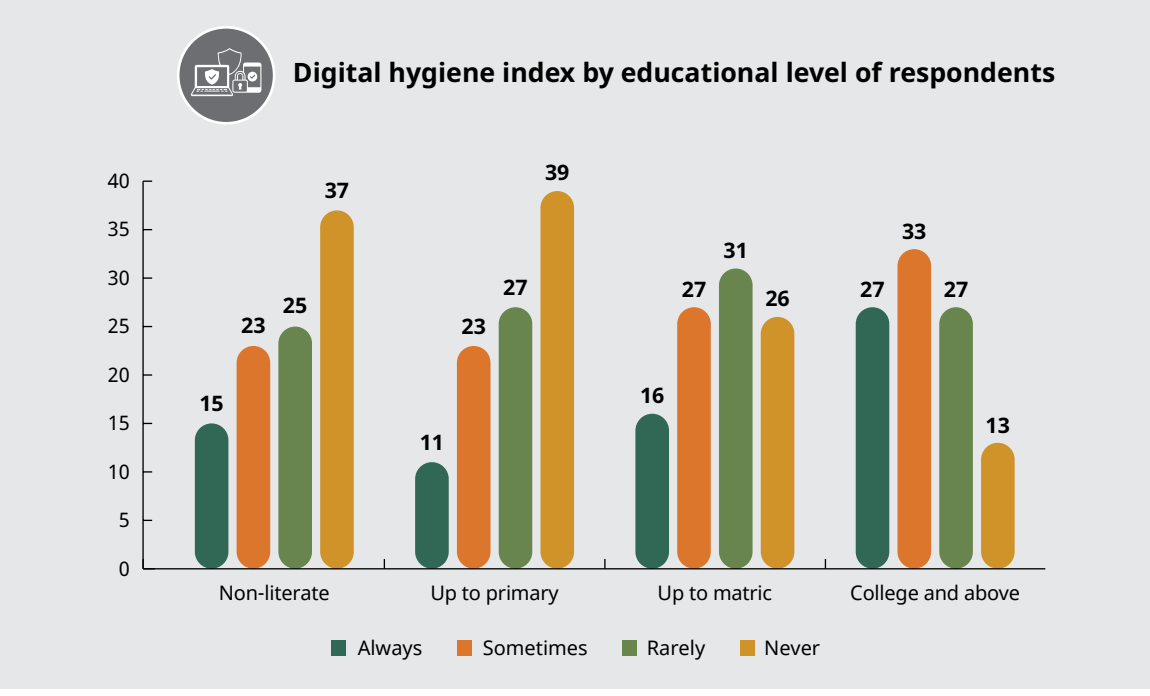
Note: Kindly refer to Appendix 3 for the details of this index.

Table 8.5: Younger respondents are most likely to always follow digital hygiene practises

Age group	Digital hygiene index			
	Always	Sometimes	Rarely	Never
Up to 25 years	25	33	29	13
26 to 35 years	22	33	28	17
36 to 45 years	22	28	29	21
46 to 55 years	17	26	30	26
56 years and above	15	22	27	36

Note: All figures are in percentages. Kindly refer to Appendix 3 for the details of this index.

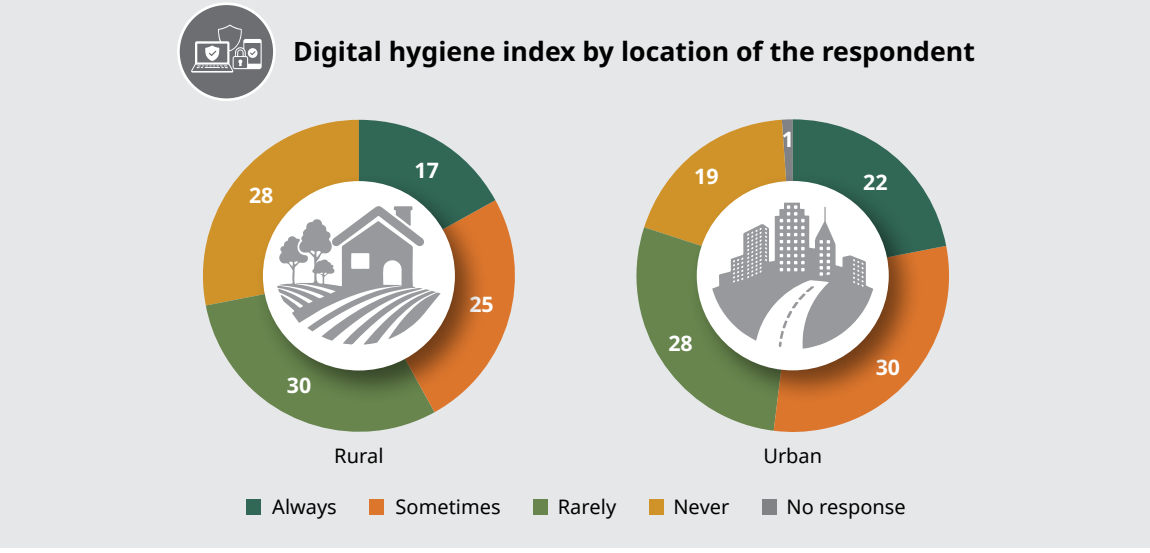
Figure 8.7: Educated respondents are more likely to follow digital hygiene



Note: All figures are in percentages. Kindly refer to Appendix 3 for the details of this index.

The analysis of data on the basis of age reveals that digital hygiene practices are most likely to be followed by the younger age cohorts compared to the older age groups, while the use of such precautionary practises decreases significantly amongst the older respondents. Amongst those aged up to 25 years, a quarter of the respondents (25%) reported always following digital hygiene measures, while 13 percent said that they never follow them. Among those who fall in the age bracket of 56 years and above, only 15 percent reported always following such practices, while over a third (36%) said that they never undertake such measures (**Table 8.5**).

Figure 8.8: Urban respondents are more likely to use digital hygiene practices



Note: All figures are in percentages. Kindly refer to Appendix 3 for the details of this index.

Further analysis of the data on the basis of education level suggests that the probability of usage of digital hygiene practices increases with an increase in education level. Among the non-literates, just 15 percent reported always following digital hygiene, while the corresponding figure amongst college graduates is 27 percent (**Figure 8.7**). Similarly, the data across urban and rural classifications show that those residing in rural areas are less likely to use digital hygiene practices in comparison to their urban counterparts. Nearly one in every four urban respondents (22%) "always" follow digital hygiene practises, as opposed to less than one in five among the rural respondents (17%) (**Figure 8.8**).

8.5 Conclusion

Adopting preventive measures to safeguard against digital threats is slowly but steadily becoming a reality for all digital users faced with the looming threat of cybercrimes. While these practices may not guarantee protection against all cybercrimes, a certain level of vigilance can go a long way in limiting exposure to such threats. The findings in this chapter show that while a significant proportion has adopted basic cybersecurity measures, the depth and consistency of this adoption are uneven and are strongly informed by education, income and age.

The data on 2-step verification paints a picture of security-conscious users, with more than a third using 2-step verification for internet banking apps and more than half using it for UPI apps. However, there is also a variation in the adoption of such measures across different socio-demographic groups. Data shows the adoption rate of the 2-step verification system by the younger, educated, affluent and urban respondents is significantly higher compared to the older population, less educated, economically marginalised and rural respondents. Moreover, the latter groups are also less likely to use either internet banking or UPI apps altogether.

The findings on unsolicited calls and messages add a more nuanced picture. While a majority of the respondents exercise caution around OTP sharing, unknown links, and unsolicited files, an important minority, about a third, report that they are sometimes or always likely to engage in these types of behaviours, such as opening files from unknown senders, or clicking on unverified links.

On awareness, the government's outreach appears to have had a rather broad effect, with a fifth either receiving messages or having seen advertisements and nearly half of them having both received messages and seen advertisements on cybersecurity.

On the other hand, digital hygiene practices are rather prevalent among a majority of the respondents. While half of respondents follow at least some digital hygiene practices, such as avoiding public Wi-Fi, not saving passwords in browsers, and checking app permissions, avoid reusing passwords and checking website authenticity, nearly a third have never followed any of them. As with other findings, the practise of digital hygiene is considerably higher among younger, educated, urban, and wealthier respondents, while older, non-literate, rural, and economically weaker respondents are far less likely to follow them.

In sum, this chapter indicates that specific socioeconomic and demographic groups are more vulnerable to cybercrime than others. Though awareness is widespread, its translation into consistent protective behaviours is strongly informed by age, education, and economic status. To bridge this gap, there is an urgent need to move beyond broad-based campaigns and focus on creating targeted awareness for vulnerable groups and enabling people to adopt digital hygiene measures.

References

- Bruce, M., Lusthaus, J., Kashyap, R., Phair, N., & Varese, F. (2024). Mapping the global geography of cybercrime with the World Cybercrime Index. *PLOS ONE, 19*(4), e0297312. https://doi.org/10.1371/journal.pone.0297312
- Livemint. (2026, January 3). ₹52,976,00,00,000 lost to cyber frauds in India in 6 years, says report – shocking

numbers explained. *Livemint*. https://www.livemint.com/news/india/529760000000-lost-to-cyber-frauds-in-india-in-6-years-says-report-shocking-numbers-explained-digital-arrest-mha-11767416448678.html

- McAfee. (2026). *State of Scamiverse*. https://www.mcafee.com/en-in/consumer-corporate/newsroom/press-releases/2026/20260204.html
- Press Information Bureau, Government of India. (2024, December 10). *Awareness campaign on cybercrimes* [Press release]. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2082765&reg=3&lang=2
- Press Information Bureau, Government of India (2026, January 23). *CERT-In: India's Frontline Defender against Cyber Threats* [Press release]
- Safer Internet India. (2025, November). Cybercrimes up 217% in the past five years: Insights from the NCRB report. *Safer Internet India*. https://saferinternetindia.com/cybercrimes-up-217-in-the-past-five-years-insights-from-the-ncrb-report/
- The Economic Times. (2025, October 23). Digital payments comprise 99.8% of total transactions volume in H1 2025: RBI. *The Economic Times*. https://economictimes.indiatimes.com/news/economy/finance/digital-payments-comprise-99-8-of-total-transactions-volume-in-h1-2025-upi-transactions-rbi/articleshow/124760861.cms
- The Economic Times. (2026a, February 11). Amit Shah asks CBI, I4C to develop ecosystem to counter cybercriminals, stay two steps ahead. *The Economic Times*. https://telecom.economictimes.indiatimes.com/news/policy/amit-shah-calls-for-stronger-cybersecurity-measures-against-cybercriminals/128184802
- The Economic Times. (2026b, May 5). India ranks 5th among world's most spam-affected nations: Truecaller report. *The Economic Times*. https://economictimes.indiatimes.com/news/india/india-ranks-5th-among-worlds-most-spam-affected-nations-truecaller-report/articleshow/130824683.cms
- Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems, 128,* Article 113160. https://doi.org/10.1016/j.dss.2019.113160

CHAPTER

09

Every Country is grappling with the issue of cybercrimes (Idaho, US - 2018).

Photo by: U.S. Department of Energy.

Public Evaluation of Institutional Competence and Digital Safety

Key Findings

- Nearly three out of four people feel that the police are equipped to deal with financial cybercrimes. Twenty-nine percent feel they are “well equipped”, while 44 percent feel they are “somewhat equipped”.
- Victims of cybercrimes are less likely to believe that police are well equipped to deal with cases of financial cybercrimes. However, among the victims, those who complained to the police are slightly more likely to believe that the police are well equipped to deal with financial cybercrimes.
- Respondents believe that police personnel are better trained to deal with cybercrimes (36% said ‘very much’ trained) than bank officials (26% said ‘very much’ trained)
- On the questions of whether banks and the police are well-trained to deal with cybercrimes, victims of cybercrimes are less likely to believe so, compared to those who have not been victims. However, amongst the victims, those who complained separately to the police and bank respectively are slightly more likely to believe that these institutions are well trained, compared to those who did not complain.
- Around half of the respondents (48%) are very likely to report cybercrime to the police in the future, if they become a victim. However, cybercrime victims are less likely to report a future incident of cybercrime to the police.
- One-third of the respondents (34%) feel that the government should launch an awareness campaign on cybersecurity.

Public Evaluation of Institutional Competence and Digital Safety

The preceding chapters paint a layered picture of India's ever-expanding digital ecosystem, one that presents unprecedented opportunities while also creating widespread vulnerability in trust, security, and privacy. While digital participation through social media, easier digital transactions and other online financial services has empowered people, it has also enabled routine encounters with scams, identity theft and privacy violations. As a result, users view digital platforms with increasing caution. While people remain actively engaged in the digital ecosystem, they are perpetually nudged by a sense of vigilance, shaped by the perception that cybercrimes are escalating and becoming more widespread.

In such a context, effective redressal mechanisms have become essential. India has developed a range of institutional systems to address cybercrime, and these have expanded over time. Under the Information Technology Act, 2000, the Indian Computer Emergency Response Team (CERT-In) was established to monitor threats within the system (Afzal and Singh, 2026). In January 2020, the Ministry of Home Affairs (MHA) launched the Indian Cyber Crime Coordination Centre (I4C)[1] which serves as a nodal point between various state police forces, other law enforcement agencies, as well as stakeholders such as banks. The I4C introduced the National Cybercrime Reporting Portal (NCRP), a centralised platform to register cybercrime complaints (Afzal and Singh, 2026). Further, the Central government initiated the Cyber Crime Prevention against Women and Children (CCPWC) scheme, under which it provides financial assistance to states and union territories for capacity-building to address cybercrimes against women and children. Since 2020, this scheme has funded cyber forensic and training labs in over 33 states and Union Territories (Kaushik, 2025). These measures in themselves reflect a growing recognition of the need for a coordinated institutional response.

However, an important question comes up: Are these systems truly accessible and effective in practice? Cybercrime redressal mechanisms involve different stakeholders, including police, bank officials, judges and magistrates. While these mechanisms offer formal accessibility via helplines, portals, complaint registration processes and investigations, data however shows that their functioning is uneven. Issues such as procedural complexities, significant delays, failures in timely account freezing, limited financial recovery, and, in some cases, reliance on personal networks to exert pressure on authorities continue to affect perceptions. Although the government aims to strengthen coordination through various mechanisms and address these gaps, only a small proportion of such cases reach courts, and even fewer are resolved. Such a condition reflects a clear gap between formal access to the redressal mechanism and citizens' actual experience, which ends up shaping public evaluation of these institutions.

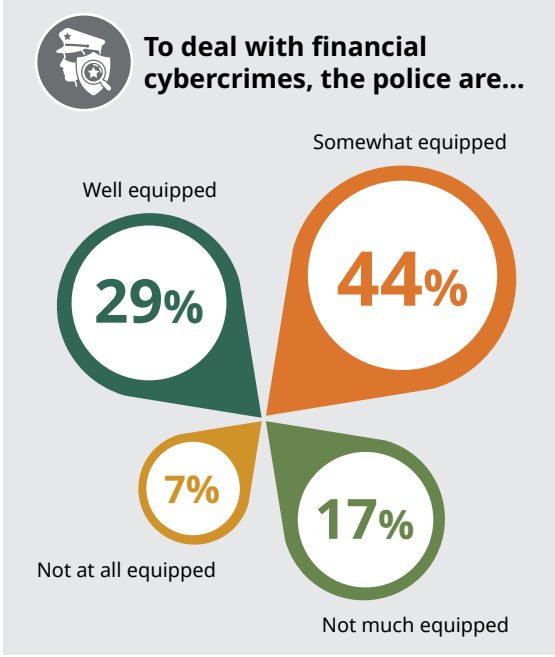
Against this background, the chapter aims to analyse public perceptions of the police, banks and courts and to assess whether they are perceived as capable enough to fight cybercrimes. In a similar vein, the chapter examines the likelihood of citizens reporting cybercrime in the future. It also explores how people assign responsibility for data protection – whether they view it as primarily the responsibility of individuals or of governments and banks. Lastly, it seeks to understand what citizens expect from the government when it comes to ensuring digital safety in a risk-prone digital environment.

9.1 Institutional Capacity

Looking at people's perceptions about the cybercrime redressal ecosystem is crucial to understanding whether services reach citizens adequately. The police are responsible for maintaining public order and handling crime, including cybercrime. Thus, the police are often the first point of contact in cases of cybercrimes.

The respondents were asked about their perceptions of how well equipped they think the police are to deal with financial cybercrimes. Overall, nearly three quarters (73%) perceived the police to be either very well or somewhat equipped to handle financial cybercrimes. While over four in every ten (44%) thought police are 'somewhat equipped', less than three in every ten (29%) considered them 'very' well equipped (**Figure 9.1**). On the other hand, about a quarter (24%) reported that the police are not equipped to deal with financial cybercrimes (17% said that the police are "not much equipped" and 7% said they are "not at all equipped").

Figure 9.1: Nearly three out of four people feel that the police are equipped to deal with financial cybercrimes



Note: All figures are in percentages. The rest did not respond.

Question asked: In your opinion, how equipped do you think the police is to deal with financial cybercrimes – very equipped, somewhat equipped, not much equipped, or not at all equipped?

Table 9.1: Nearly half of respondents from Bihar and Madhya Pradesh believe that the police are 'very well equipped' to deal with financial cybercrimes

State	To deal with cybercrime, police are...			
	Well equipped	Somewhat equipped	Not much equipped	Not at all equipped
Madhya Pradesh	46	35	11	3
Bihar	46	36	14	3
Kerala	43	38	12	4
Telangana	39	43	13	1
Gujarat	38	41	11	2
Odisha	33	56	9	2
Rajasthan	29	39	22	5
Karnataka	29	49	15	6
Jharkhand	27	38	19	9
Assam	27	53	15	3
Tamil Nadu	24	57	17	2
Haryana	23	29	19	20
West Bengal	18	52	15	12
Uttar Pradesh	17	41	23	13
Delhi	13	39	21	21
Maharashtra	11	50	29	9

Note: All figures are in percentages. The rest did not respond.

Question asked: In your opinion, how equipped do you think the police is to deal with financial cybercrimes – very equipped, somewhat equipped, not much equipped, or not at all equipped?

The data shows considerable state-wise variation among those who believe that police are well equipped to deal with financial cybercrimes. About half of the respondents from Bihar and Madhya Pradesh (46% each) expressed relatively high confidence in police being well equipped to deal with financial cybercrimes, followed by Kerala (43%) and Telangana (39%) (**Table 9.1**). Over one in three respondents from Gujarat (38%) and Odisha (33%) express the same, placing these states slightly above the national average of 29 percent. On the other end, confidence is remarkably lower in Uttar Pradesh (17%), Delhi (13%) and Maharashtra (11%), where only a small proportion perceives the police as well equipped to deal with financial cybercrimes. Also, about one in five respondents from Delhi (21%) and Haryana (20%) are of the opinion that the police are 'not at all equipped' to deal with financial cybercrimes.

When the perceptions of victims and those who aided the victim, were analysed and compared against the perceptions of those who were not victims of cybercrimes, it was found that victims were slightly less likely to believe that the police are well equipped to deal with cybercrimes. While 31 percent of the respondents who were not victims of cybercrimes said that the police are well equipped to deal with financial cybercrimes, the proportion drops to 23 percent amongst those who have been victims of cybercrimes or have aided the victims of cybercrimes (**Table 9.2**). Simultaneously, victims and those who assisted cybercrime victims are relatively more likely to perceive that the police are "not much equipped" (21% versus 15%) and "not at all equipped" (10% versus 6%) to deal with financial cybercrimes compared to non-victims.

As seen above, victims are relatively less likely to believe that the police are well equipped to deal with financial cybercrimes. However, among the victims, those who complained to the police are slightly more likely to believe that the police are well equipped to deal with financial cybercrimes, compared to those who did not complain to the police (**Figure 9.2**). This indicates that while the overall perceptions regarding police capacity to deal with cybercrimes is not very positive amongst the victims, there is a higher likelihood for those who engage with the police to have a more positive opinion about their capacity to deal with financial cybercrimes. However, the difference in these opinions is only marginal, and not very sharp.

Those who complained to the police were more likely to believe that the police are well equipped to deal with cybercrimes, compared to those who did not complain. Amongst those who complained to the police, a quarter of the respondents (25%) were likely to report that the police are "well equipped", compared to nearly one in five (18%) among those who did not complain. Conversely, the perception that the police are "not at all equipped" is marginally higher among those who did not complain

Table 9.2: Victims of cybercrimes are less likely to believe that police are well equipped to deal with cases of financial cybercrimes

	To deal with financial cybercrimes, the police are...			
	Well equipped	Somewhat equipped	Not much equipped	Not at all equipped
Overall	**29**	**44**	**17**	**7**
Victim/ Respondents who assisted	23	44	21	10
Non-victims	31	44	15	6

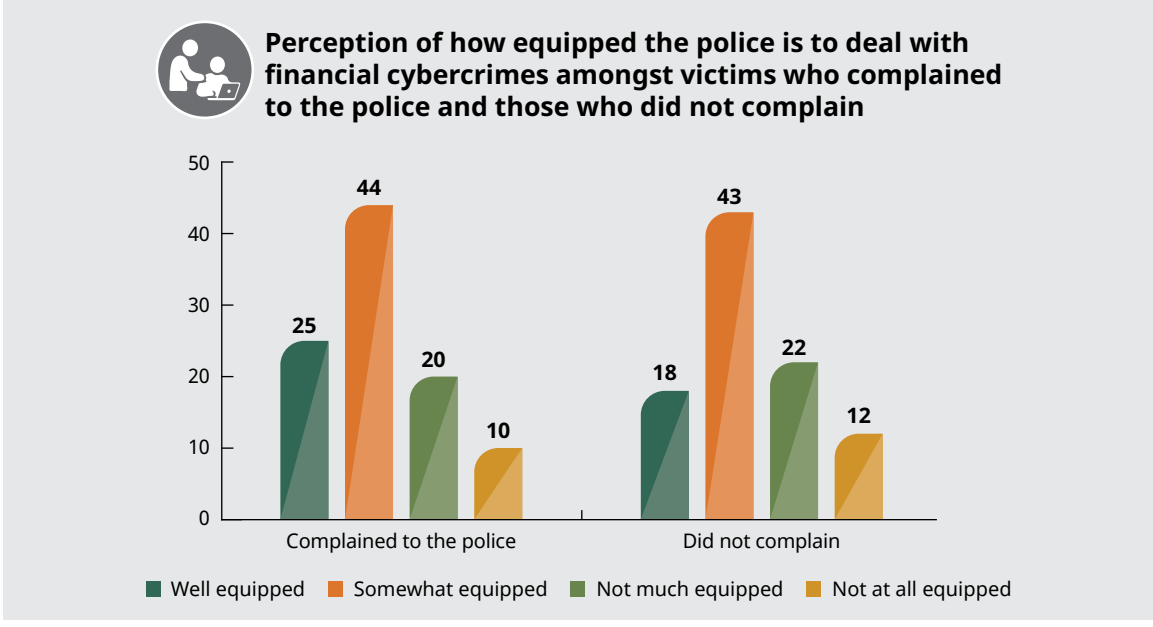
Note: All figures are in percentages. The figures show only the respondents who said "Yes" to being a victim of cybercrime and who aided the victims of cybercrime.

Question asked: In your opinion, how equipped do you think the police is to deal with financial cybercrimes – very equipped, somewhat equipped, not much equipped, or not at all equipped?

(12%), compared to those who complained to the police (10%) (**Figure 9.2**). These findings suggest that first-hand experience with police tends to have a slightly more favourable assessment of their competence.

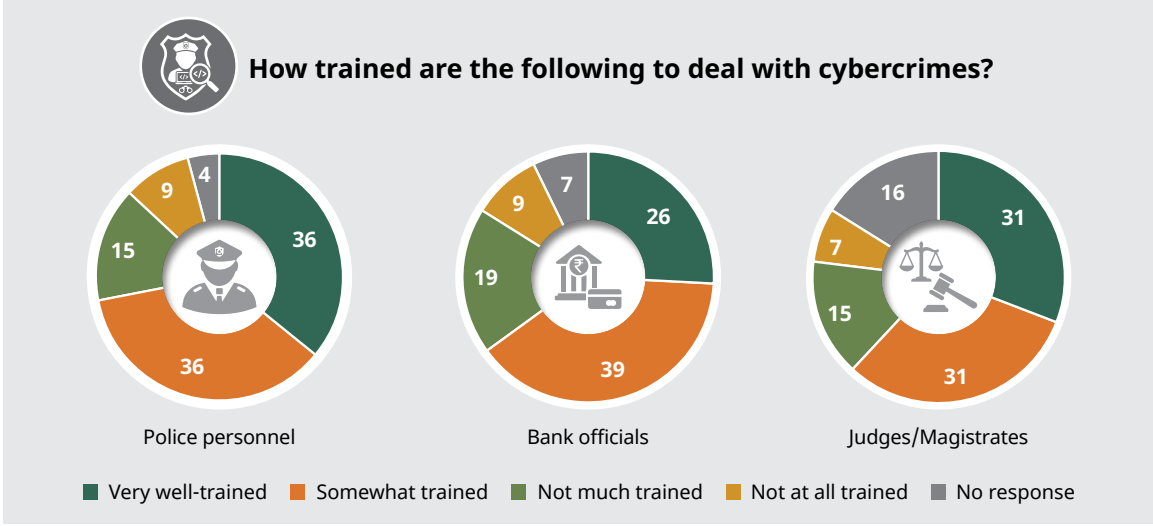
Since bank officials, judges and magistrates, along with police personnel, have a role in the cybersecurity ecosystem, the respondents were asked about their perceptions of whether the police, banks, and judges/magistrates are trained to deal with cybercrimes. Over seven in ten respondents (72%) report that the police are well-trained (combining 'very much' - 36% and 'somewhat' - 36%) (**Figure 9.3**).

Figure 9.2: Cybercrime victims who complained to the police are more likely to believe that police are well equipped to deal with financial cybercrimes



Note: All figures in percentages. The data includes perceptions of both the victims and respondents who assisted cybercrime victims.
Question asked: In your opinion, how equipped do you think the police is to deal with financial cybercrimes – very equipped, somewhat equipped, not much equipped, or not at all equipped?

Figure 9.3: Common people believe that police personnel are better trained to deal with cybercrimes than bank officials



Note: All figures are in percentages.
Question asked: In your opinion, how trained are these people to deal with cybercrimes - very much, somewhat, not much, or not at all?

Table 9.3: Victims are less likely to believe that the police are trained to deal with cybercrimes, compared to those who have not been victims

	To deal with cybercrimes, the police personnel are...			
	Very well trained	Somewhat trained	Not much trained	Not at all trained
Victims/respondents who assisted cybercrime victims	28	36	21	12
Non-victims	38	36	1	8
Whether they complained to the police*				
Victims who complained to the police	32	33	20	13
Victims who did not complain to the police	22	39	21	11

**The victims/respondents who assisted cybercrime victims who reported 'yes' to complaining to the police and 'went to the police but did not pursue the case' (complainants) and 'No' (non-complainants).*

Note: The rest did not respond. All figures are in percentages.

Question asked: In your opinion, how trained are police personnel to deal with cybercrimes - very much, somewhat, not much, or not at all?

A little over six in ten (62%) said that the judges/ magistrates are well-trained (combining 'very much' - 31% and 'somewhat' - 31%), and a corresponding proportion - 65 percent - also hold the same opinion about bank officials (combining 'very much' - 26% and 'somewhat' - 39%). In general, there seems to be a relatively higher level of confidence in the police and judges/ magistrates compared to bank officials. The latter are perceived relatively less well-trained and less adequately equipped to deal with cybercrimes.

In contrast, experts from the banking sector and other cybercrime experts who were interviewed for this study were of the opinion that banks have sufficient training to deal with cybercrimes, but often lack accountability (see **Chapter 2** for more details).

The perceptions of training and competence about police, banks or judges can vary depending on whether a person has experienced cybercrime or not. Moreover, this perception can differ more meaningfully depending upon whether the victims had a direct experience with these institutions (police, banks and judges).

At the broader level, perceptions about the police show a clear divide among the victims (including respondents who assisted victims) and non-victims. Non-victims (38%) hold a more favourable view of the police than the victims (28%), with a greater proportion citing them as "very well trained" (**Table 9.3**). Victims (12%), in turn, are relatively more likely to report that police are "not at all trained" to deal with cybercrime than the non-victims (8%). This pattern becomes more nuanced when the victims or those who assisted cybercrime victims are further disaggregated by whether they filed a complaint. Among those victims who complained to the police about the cybercrime, about one-third (32%) reported that the police are 'very much trained', as compared to about a quarter (22%) of those victims who did not complain to the police (**Table 9.3**). While cybercrime victimisation appears to lower confidence in the police's ability to deal with cybercrime relative to non-victims, engagement through complaint appears to partially restore it.

Broadly, a similar pattern is also observed when it comes to bank officials. Non-victims were more likely to report banks as 'very much trained' (27% versus 22% among victims), while victims were marginally more likely to view banks as 'not at all trained' (11% versus 8% among non-victims) (**Table 9.4**). However, among victims who separately complained to their bank, 26 percent reported officials as 'very much trained', compared to 18 percent among those who did not. This again shows a moderating effect of direct interaction with the institution.

The perception about the competence of judges or magistrates is also not very different. Non-victims (32%) were more likely to view judges as 'very much trained' to deal with cybercrime compared to victims or those who assisted them (27%), and the latter group is also more inclined to perceive judges as 'not much trained' (18% versus 15% among non-victims) (**Table 9.5**). Among those whose cases reached court, 31 percent of the victims said judges are 'very much trained', as opposed to 26 percent of those whose cases did not go to court.

Table 9.4: Victims who complained to the bank were more likely to perceive bank officials as well trained than those who did not complain

	To deal with cybercrimes, the bank officials are...			
	Very much trained	Somewhat trained	Not much trained	Not at all trained
Victims/respondents who assisted	22	42	21	11
Non-victims	27	38	19	8
Whether they complained to the bank*				
Victims who complained to the bank	26	41	18	13
Victims who did not complain to the bank	18	41	23	11

**The victims/respondents who assisted cybercrime victims who reported 'yes' to separately complaining to the bank (complainants) and 'No' (non-complainants).*

Note: The rest did not respond. All figures are in percentages.

Question asked: In your opinion, how trained are bank officials to deal with cybercrimes - very much, somewhat, not much, or not at all?

Table 9.5: Victims whose cases went to court were more likely to perceive judges/ magistrates as well trained than those whose cases did not go to court

	To deal with cybercrimes, the judges/magistrates are...			
	Very much trained	Somewhat trained	Not much trained	Not at all trained
Victims/respondents who assisted	27	32	18	9
Non-victims	32	31	15	7
Whether cases went to the court*				
Victims whose cases went to court	31	33	21	10
Victims whose cases did not go to court	26	32	17	10

**The victims/respondents who assisted cybercrime victims who reported 'yes' to their cases went to court (Litigated) and 'No' (non-litigated).*

Note: The rest did not respond. All figures are in percentages.

Question asked: In your opinion, how trained are judges/magistrates to deal with cybercrimes - very much, somewhat, not much, or not at all?

However, victims whose cases went to the court were also somewhat more likely to report judges as not adequately trained (31% combining 'not much trained' – 21% and 'not at all trained' – 10%) as compared to those whose cases did not reach the court (27% combining 'not much trained' – 17% and 'not at all trained' – 10%). Overall, non-victims and those with court experience hold similarly positive views of judicial competence, indicating that direct exposure to the legal process appears to produce a more polarised assessment.

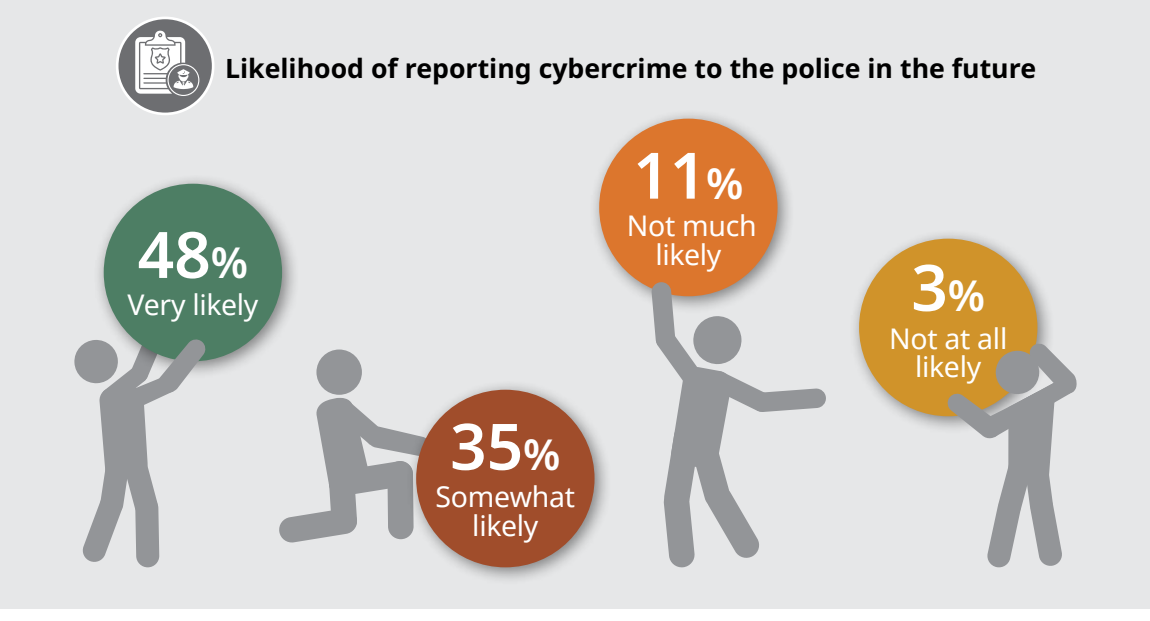
9.2 Likelihood of Reporting in the Future

Having examined perceptions about institutional (police, bank officials and judges) competence, it is equally important to understand how these experiences and perceptions translate into future behaviour. Specifically, whether victims or the general public would choose to report a cybercrime if they encountered one. This section explores how respondents assess their own likelihood of reporting such incidents to the police.

To understand future reporting behaviour, a scenario was presented to the respondents. They were asked about their likelihood of reporting a case of cybercrime to the police if they become a victim in the future. Approximately half the respondents (48%) reported a high likelihood (**Figure 9.4**). Thirty-five percent said they are "somewhat likely". Fourteen percent say they are not likely to report in the future (11% said "not much likely" and 3% said "not at all likely").

Cybercrime thrives on socioeconomic inequalities. Intersectional identities shape experiences of cybercrime victimisation among individuals. When the respondents are asked about their likelihood of reporting cybercrime to the police in the future, there is a notable variation across different socioeconomic groups. The most economically advantaged groups show the highest likelihood (58%) of reporting future instances as opposed to those belonging to the poor category (40%), with a difference of 18 percentage points between the two groups (**Figure 9.5**).

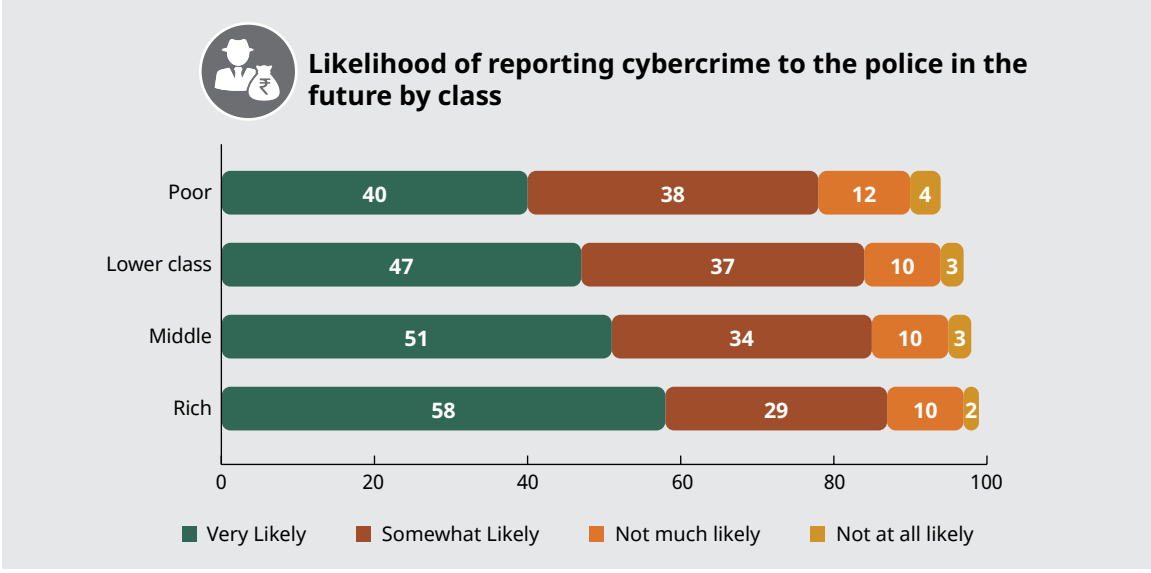
Figure 9.4: Around half of the respondents are very likely to report cybercrime to the police in the future, if they become a victim



Note: The rest did not respond.

Question asked: If you are a victim of a case of cybercrime in the future, how likely are you to report the case to the police - very likely, somewhat likely, not much likely, or not at all likely?

Figure 9.5: Rich respondents are most likely to report cybercrime in the future

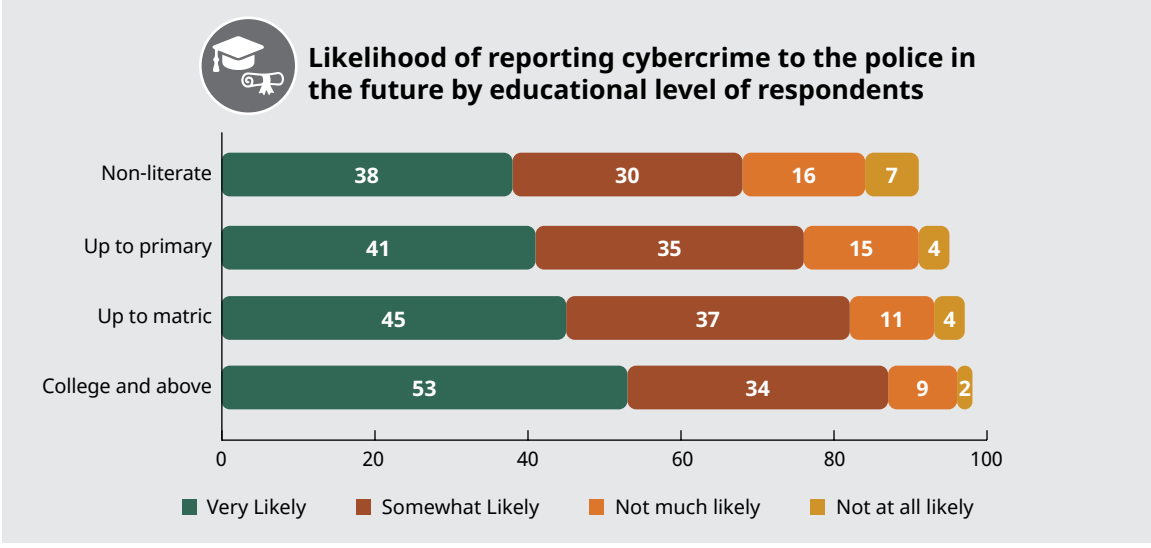


Note: The rest did not respond. All figures are in percentages.

Question asked: If you are a victim of a case of cybercrime in the future, how likely are you to report the case to the police - very likely, somewhat likely, not much likely, or not at all likely?

The responses were also analysed across different education levels. The findings indicated that the more educated respondents exhibited a higher likelihood of reporting a cybercrime case to the police in the future. The highest proportion, 53 percent of respondents with a college education or more report being "very likely" to report to the police in the future. Compared to this, only 38 percent of those without formal education are "very likely" to report (**Figure 9.6**). In contrast, 16 percent of the non-literate respondents said that they are "not much likely" to report, as opposed to only nine percent among those with college degrees. While the data was also analysed among different age groups and the gender of the respondents, no sharp patterns were observed.

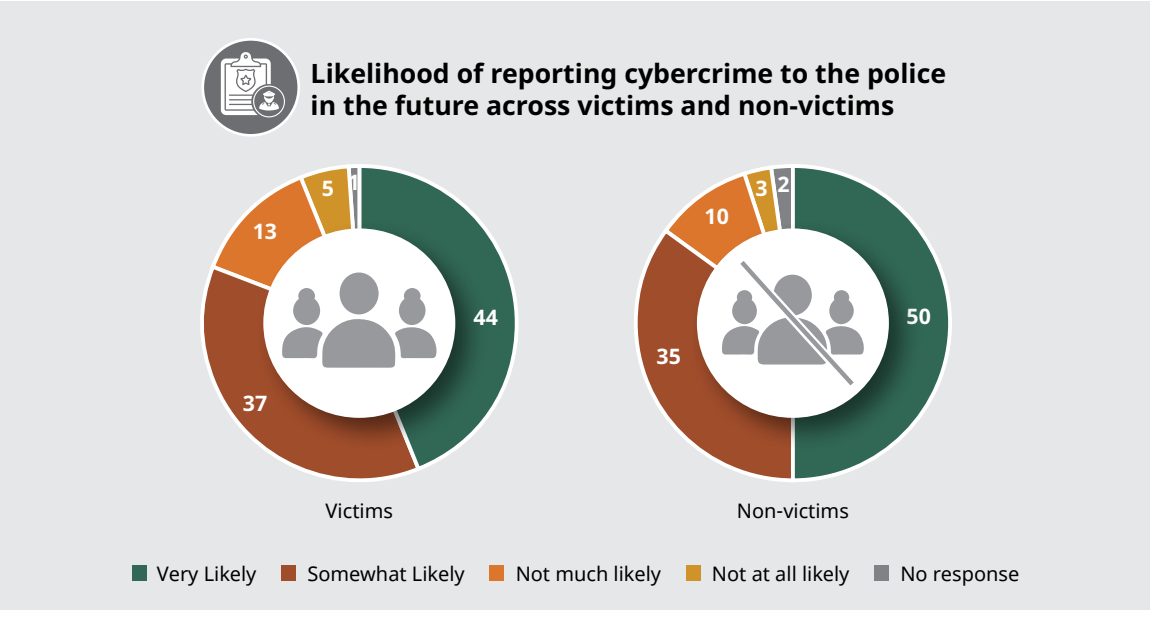
Figure 9.6: Educated people are more likely to report cybercrime to the police in the future



Note: The rest did not respond. All figures are in percentages.

Question asked: If you are a victim of a case of cybercrime in the future, how likely are you to report the case to the police - very likely, somewhat likely, not much likely, or not at all likely?

Figure 9.7: Cybercrime victims are less likely to say that, in case they face such a crime in the future, they will report it to the police



Note: All figures are in percentages. The victim category contains both the victims of cybercrime and those who helped cybercrime victims.

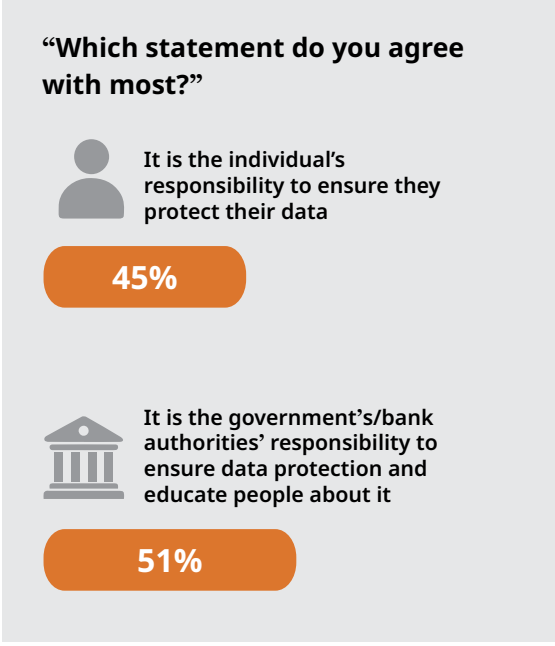
Question asked: If you are a victim of a case of cybercrime in the future, how likely are you to report the case to the police - very likely, somewhat likely, not much likely, or not at all likely?

The data was further analysed by comparing the responses of those who have already been victims of cybercrimes with those who have not been victims. The data highlights that those who have not been victims of cybercrime in the past are marginally more likely to say that in case they face such a crime in the future, they will report it to the police (50% said "very likely"), as compared to those who have been victims or those who have assisted victims of cybercrimes (44% said "very likely") (**Figure 9.7**). This indicates that while the overall satisfaction with the police investigation of cybercrimes may be high amongst the victims (as seen in Chapter 5), nonetheless, victims are less likely to trust the institution to be able to resolve their complaint in the future.

9.3 Steps Towards Digital Safety

Studying people's perceptions about who is responsible for data security and protection is important to hold institutions accountable. Responsibility for data protection is often shared between the individual and institutions, but how this balance is perceived by the public can influence people's behaviour.

Figure 9.8: A little over half of the respondents believe that the government/bank authorities are responsible for ensuring data protection



Note: The rest did not respond.

Question asked: I will now read two statements, please tell me which one do you agree with the most? Statement 1: It is the individual's responsibility to ensure they protect their data; Statement 2: It is the government's/bank authorities' responsibility to ensure data protection and educate people about it.

While individuals protect their own information through everyday practices like using strong passwords, verifying app permissions and staying alert to risks, government or financial institutions, on the other hand, are expected to create secure systems that enforce systematic regulations and ensure that people are informed about how their data is used and protected.

To understand this balance and how it shapes perceptions about data regulation, respondents were presented with two statements and asked which one they agreed with the most. The data indicates that perceptions are relatively divided, with nearly half (45%) saying it is the responsibility of the individual to protect their data, whereas another half (51%) thought it to be the responsibility of the government or the bank authorities to ensure data protection and build public awareness (**Figure 9.8**).

The data was further analysed across different education levels. The more educated respondents are, the more likely they are to agree with the statement that the government or bank authorities need to ensure data protection and educate people about it. Fifty-three percent of the respondents who hold a college degree or above are likely to hold the government or banks accountable, as compared to 39 percent of the respondents with no formal education (**Table 9.6**). There was no significant difference between the opinions of the urban and rural people.

While understanding where people place the burden of responsibility for digital safety offers valuable insight into public expectations, it raises a natural follow-up question: what do citizens expect the government to do? To this end, the respondents were asked what the most important step the government/authorities can take to ensure the citizens' digital safety. The majority (34%) said awareness campaigns on cybersecurity are the most important step that the government should undertake (**Figure 9.9**). This was followed by the need for the implementation of data protection regulations (18%) and improving the effectiveness of cybercrime reporting portals (14%). Only seven percent of the respondents felt that better training of cybersecurity personnel is the most important step that the government can undertake to ensure digital safety.

9.4 Conclusion

The data indicates that while the public is engaged with institutions tasked with ensuring their digital safety, they are also uncertain about their effectiveness. Over two in every three respondents are confident that police are equipped to deal with cybercrime, while about a quarter are not. States like Bihar, Madhya Pradesh and Kerala depict the highest level of confidence.

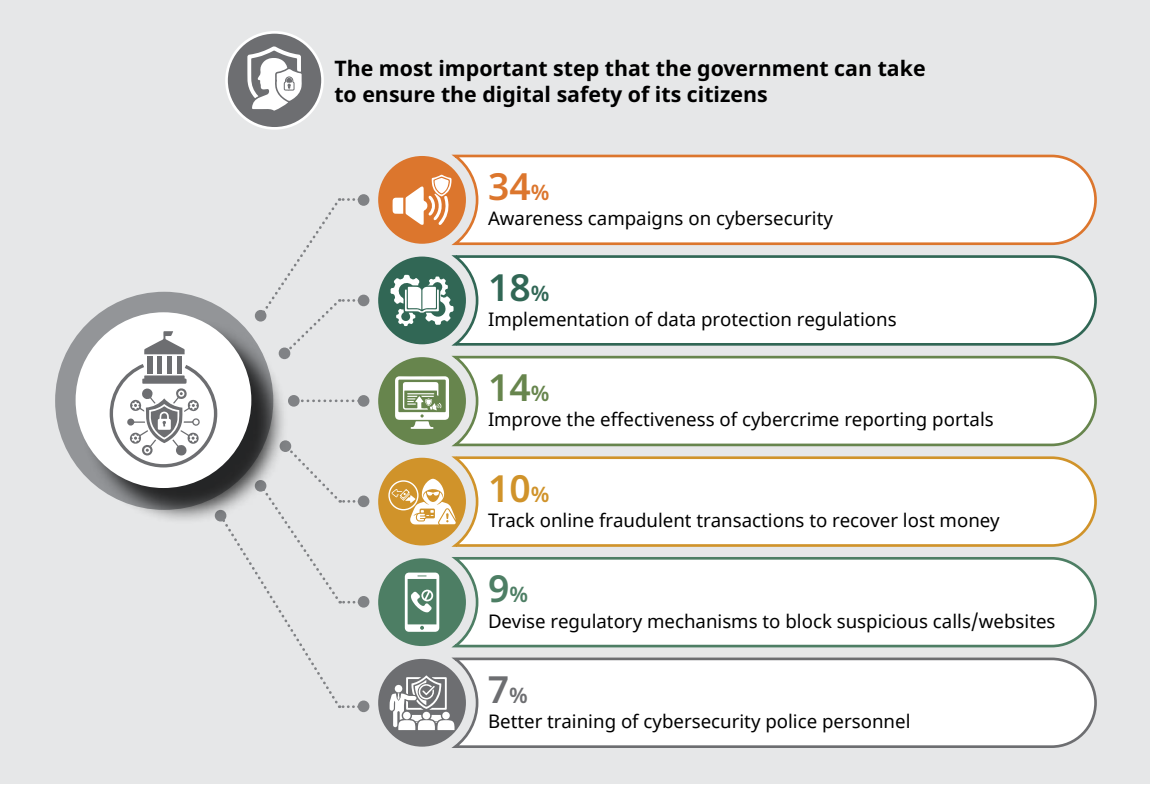
Table 9.6: Educated respondents are more likely to hold government/bank authorities accountable for data protection

Level of education of the respondents		Data protection is the responsibility of...	
		The individual	The government/bank authorities
	Non-literate	50	39
	Up to primary	45	46
	Up to matric	46	51
	College and above	45	53

Note: The rest did not respond. All figures are in percentages.

Question asked: I will now read two statements, please tell me which one do you agree with the most? Statement 1: It is the individual's responsibility to ensure they protect their data; Statement 2: It is the government's/bank authorities' responsibility to ensure data protection and educate people about it.

Figure 9.9: One-third of the respondents feel that the government should launch an awareness campaign on cybersecurity



Note: The rest either cited other steps or did not respond. This was an open-ended question, and the answer categories were not read out.

Question asked: In your opinion, what is the most important step that the government/authorities can take to ensure the digital safety of the citizens?

Moreover, the experience of cybercrime does not lead to a sharp difference in their view of police preparedness. Victims of cybercrimes or those who assisted victims of cybercrimes are less likely to believe that the police are well equipped to deal with cybercrimes, compared to those who have not been victims. Amongst victims, however, those who complained to the police are more likely to believe that the police are well equipped to deal with cybercrimes, indicating that engagement with the police tends to improve people's perceptions regarding its capacity to deal with cybercrimes.

The study also examines public confidence in key institutional actors involved in addressing cybercrime. Accounting for bank officials, judges, and magistrates, the study points to a higher level of confidence in the police, followed by judges and magistrates and finally the banks. Importantly, these perceptions are not static as they are shaped by lived experience. Direct contact with institutions, whether through filing a complaint, approaching a bank, or going through a court case, tends to produce more nuanced assessments. While victims of cybercrimes are less likely to believe that the police, banks, or courts are well trained to deal with cybercrimes, among the victims, those who complained to the police or bank, or whose cases went to court, are slightly more likely to believe that the respective institutions are well trained.

Confidence in reporting future cybercrimes is relatively strong, with over eight in ten respondents expressing a likelihood of approaching the police should they encounter cybercrime. This reporting varies systematically by socioeconomic status and education, with the more educated and the economically advantaged respondents being more likely to say that they will report such a case to the police in the future. Here again, however, there is a

slight variation in the responses of those who have been victims and those who have not, with victims of cybercrimes being less likely to report a future incident of cybercrime to the police.

Moreover, trust in digital financial infrastructure has emerged as a significant factor, as perceived safety with online banking channels declines, the burden of responsibility shifts decidedly from the individual towards the state. In terms of what citizens want for their digital safety, awareness campaigns are the most important step cited by a third of the respondents. This is followed by the implementation of data protection regulations and the improvement of the effectiveness of cybercrime portals.

Taken together, these findings suggest that confidence in the cybercrime security ecosystem is not at its best. To ensure that, the focus should not only be on strengthening the capacity of institutions that respond to cybercrime, but also on public confidence in those institutions. This implies that a lot of work needs to be done to satisfy citizens, which could be achieved by transparency, accessibility, and sustained outreach.

Endnotes

i Read more about the initiative here: https://i4c.mha.gov.in/about.aspx

References

- Afzal, A., & Singh, A. (2026). Cyber crimes in India: Challenges and legal reform. *International Journal of Social Science Research, 3*(1). https://doi.org/10.70558/IJSSR.2026.v3.i1.30820
- Kaushik, K. (2025, June 24). India's cyber forensics push since 2020: Building national capacity for digital investigations. *Observer Research Foundation*. https://www.orfonline.org/expert-speak/india-s-cyber-forensics-push-since-2020-building-national-capacity-for-digital-investigations

APPENDIX 1: Technical Details of Study Design and Sample

The latest edition of Status of Policing in India Report (SPIR) 2026 – Cybercrime: Victim Perspectives and Systemic Responses – is jointly conducted by Lokniti-CSDS and Common Cause. This edition of the report draws on a survey across 16 Indian states with 8,306 respondents, aiming to examine the rapidly changing nature of cybercrimes in India and the systems meant to respond to them. This study seeks to understand the nature and experiences of victims across offences such as online fraud, digital arrest scams, trolling and bullying, identity theft, and online sexual harassment. It also explored how victims navigate reporting processes, the role played by banks and other institutions, and the challenges they face in seeking redress.

1. Sampling Overview

This study had a target sample size of 8000 respondents, to be conducted across 16 Indian states. A target of 500 interviews was conducted across all states. In each state, these 500 interviews were spread across five districts, with a sample of 100 in each district. Furthermore, within each district, four locations were sampled, and 25 interviews were conducted in each of these four locations. These locations were selected as per economic class, starting from lower, middle, upper-middle and upper/rich levels of economic prosperity. The selection of locations was done in accordance with the local insights from the respective state teams, consisting of state coordinators and supervisors. The survey was conducted mainly in lower-income, middle class and upper-class localities. A minimum of three locations from each state were rural areas or villages.

2. Sample Selection

A multi-stage random sampling method was used to select the sample. The sampling was done at four stages.

Stage 1: Selection of sampled states

The selection of states was done with a few parameters in mind: primarily, the concentration of cybercrimes in each state and the possible cross-section of varying degrees of urbanity in these states.

To select these 15 states, official data on "State/UT-wise Number of Cases Registered under Cyber Crimes from 2018 to 2022" was taken [downloaded from: https://www.data.gov.in/resource/stateut-wise-number-cases-registered-under-cyber-crimes-2018-2022-0]. For each state, across five years, the average of cybercrime was calculated and arranged in descending order. The final list of the sampled states has thus been made, primarily on the basis of the highest number of registered cybercrimes, and secondly, the geographical spread of the states across the Indian geographical landscape. Andhra Pradesh was not selected even though it was the sixth highest in the registered number of cybercrimes, because of its proximity to Telangana, which is already selected due to being the third-highest in the list. In addition to these states, Delhi was selected due to it being the capital city and also having the highest number of registered cybercrimes among the Union Territories.

S. No.	State/UT	Category	2018	2019	2020	2021	2022	Average of all five years
Total (All India)	Total (All India)	Total (All India)	27248	44735	50035	52974	65893	48177
	Karnataka	State	5839	12020	10741	8136	12556	9858.4
	Uttar Pradesh	State	6280	11416	11097	8829	10117	9547.8
	Telangana	State	1205	2691	5024	10303	15297	6904
	Maharashtra	State	3511	4967	5496	5562	8249	5557
	Assam	State	2022	2231	3530	4846	1733	2872.4
	Odisha	State	843	1485	1931	2037	1983	1655.8
	Rajasthan	State	1104	1762	1354	1504	1833	1511.4
	Bihar	State	374	1050	1512	1413	1621	1194
	Gujarat	State	702	784	1283	1536	1417	1144.4
	Jharkhand	State	930	1095	1204	953	967	1029.8
	Tamil Nadu	State	295	385	782	1076	2082	924
	Madhya Pradesh	State	740	602	699	589	826	691.2
	Haryana	State	418	564	656	622	681	588.2
	West Bengal	State	335	524	712	513	401	497
	Kerala	State	340	307	426	626	773	494.4
	Delhi	Union Territory	189	115	168	356	685	302.6

Stage 2: Selection of sampled districts

To select the districts, district-wise data on cybercrimes was used. It is important to note that for this, the data from the year 2023 was used, which was the latest available data at the time of sampling. The criteria for selection of the state were the top five districts that had the highest number of cybercrimes. Keeping in mind that some of the police administrative districts have jurisdiction over multiple cities/districts, and therefore the main administrative district was selected, after which the Commissionerate is named (e.g., Lucknow district for the Lucknow Commissionerate). Moreover, wherever the district name within the police administrative district was repeated in the list (Bengaluru district and Bengaluru city), the one with higher cybercrime cases was chosen. Similarly, a few administrative districts in the 2023 cybercrime cases list did not have identifying district names (such as DCP BBSR in Odisha, Cybercrime cell in Madhya Pradesh, etc.), and hence the district next in line was chosen. Each district had a sample of 100 respondents, with a total of five districts across the state. The list of all the districts is given in Table 1.

Table 1: Sampled districts

S. No.	Sampled Districts	Total Cyber Crime Cases
1. Gujarat		
a.	Surat City	397
b.	Ahmedabad City	246
c.	Kheda	129
d.	Anand	108
e.	Vadodara City	61
2. Haryana		
a.	Gurugram	319
b.	Hissar	61
c.	Palwal	57
d.	Faridabad	49
e.	Karnal	34
3. Jharkhand		
a.	Ranchi	248
b.	Jamshedpur	107
c.	Dhanbad	102
d.	Deoghar	99
e.	Jamtara	75
4. Karnataka		
a.	Bengaluru City	17631
b.	Hubballi Dharwad City	465
c.	Chikkaballapura	262
d.	Tumakuru	252
e.	Mangaluru City	241
5. Kerala		
a.	Trivandrum Commr (Dist - Trivandrum)	584
b.	Thrissur Commr (Dist - Thrissur)	434
c.	Palakkad	208
d.	Kottayam	205
e.	Ernakulam Rural	188
6. Madhya Pradesh		
a.	Gwalior	91
b.	Indore Commissionarate (Dist - Indore)	86
c.	Bhopal Commissionarate (Dist - Bhopal)	75
d.	Rewa	33
e.	Sagar	28

S. No.	Sampled Districts	Total Cyber Crime Cases
7.	**Maharashtra**	
a.	Mumbai Commr (Dist - Mumbai)	4131
b.	Thane Commr (Dist - Thane)	639
c.	Pune Commr (Dist - Pune)	487
d.	Nagpur Commr (Dist - Nagpur)	309
e.	Pimpri Chinchwad City	244
8.	**Odisha**	
a.	Ganjam	140
b.	Jajpur	126
c.	Sambalpur	122
d.	Rourkela	121
e.	Baragarh	120
9.	**Rajasthan**	
a.	Jaipur Crime (Dist - Jaipur)	228
b.	Udaipur	157
c.	Kota City	113
d.	Jodhpur West	94
e.	Bharatpur	93
10.	**Tamil Nadu**	
a.	Chennai	1352
b.	Avadi	361
c.	Coimbatore City	207
d.	Cuddalore	185
e.	Chengalpattu	164
11.	**Telangana**	
a.	Hyderabad Commissionerate (Dist - Hyderabad)	4855
b.	Rachakonda Commissionerate (Dist - Rangareddy)	2947
c.	Warangal Commissionerate (Dist -Warangal)	1104
d.	Sangareddy	363
e.	Karimnagar Commissionerate (Dist - Karimnagar)	313
12.	**Uttar Pradesh**	
a.	Lucknow Commissionarate (Dist -Lucknow)	1453
b.	Ghaziabad	1097
c.	Gautambudh Nagar	582
d.	Kanpur Commissionarate (Dist - Kanpur)	481
e.	Prayagraj	399

S. No.	Sampled Districts	Total Cyber Crime Cases
13.	**West Bengal**	
a.	Purab Medinipur	37
b.	Bangaon	36
c.	Purba Bardhaman	28
d.	Kolkata	21
e.	Barasat	18
14.	**Assam**	
a.	Guwahati City	182
b.	Cachar	69
c.	Dhubri	69
d.	Kamrup	60
e.	Morigaon	36
15.	**Bihar**	
a.	Patna	917
b.	Nalanda	387
c.	Gaya	264
d.	Muzaffarpur	179
e.	Saran	174
16.	**Delhi**	
a.	West	83
b.	Outer North	69
c.	South	47
d.	Shahdara	41
e.	New Delhi	27

Stage 3: Selection of sampled locations

Within each district, four locations were chosen. In each of these locations, 25 respondents were interviewed. There were two important requirements in selecting these locations. Firstly, a minimum of three locations within 25 different locations within each state should be villages or in rural areas. Second, for economic diversity, the four locations selected should represent different income groups: one in lower income locality, one in middle income locality, one in upper middle-income locality and one in an affluent/rich locality.

Stage 4: Sampling of households

At the fourth stage, the Field investigators (FIs) were provided with a list of locations that were prepared in consultation with state teams. This list contained information about the locations, such as the state name, district name, nature of the locations, and their economic type. and village/ward name. The field investigators (FIs), while visiting these locations, employed a predetermined random walk procedure, taking into account the direction and pattern of the walk. This approach aimed to cover the village/ city area systematically. To determine the

starting point for the survey, FIs were instructed to identify a landmark, such as a school or public hospital, with the adjacent household as the starting point for data collection. From there, the FIs were instructed to add a predetermined random interval to select the next household for the interview. The specific interval varied based on the population size of the respective cities or villages. In cases where the locality was scattered, the FIs were asked to survey every 10th household that fell on their right-hand side. Conversely, if the locality was highly clustered, the FIs were instructed to survey every 20th household that was on their right. All interviews conducted by the FIs were strategically planned in a way to ensure that the location was covered in its entirety.

Stage 5: Selection of respondents

The selection of respondents was based on their gender and age. The field investigators (FIs) were instructed to follow a respondent's sheet with a prescribed quota for gender and age groups in mind. The quota ensured that the interviews covered the age bracket adequately and provided equal gender representation. All respondents were 18+ (adults). FIs were asked to conduct six interviews with youth in the age group of 18-25 years, seven in the age group of 26-40 years, six interviews in the age group of 41-59 years, and six among those older than 60+ years. An equal gender ratio was to be maintained in each age group while conducting the interviews. For instance, if the FI is to conduct six interviews in the age group of 18-25 years, three of them must be males and three females. To log the quota, the FIs were required to indicate the age group and gender of the respondent with a checkmark or tick (✓) provided in the respondent sheet.

A detailed sampling plan (targeted and achieved) for the study is shared in Table 2.

Table 2: Achieved sample from each state

States	Targeted sample	Achieved sample
Assam	500	526
Bihar	500	510
Gujarat	500	535
Haryana	500	512
Karnataka	500	521
Kerala	500	557
Madhya Pradesh	500	514
Maharashtra	500	520
Odisha	500	504
Rajasthan	500	498
Tamil Nadu	500	516
Uttar Pradesh	500	534
West Bengal	500	509
Delhi	500	521
Jharkhand	500	530
Telangana	500	499
Total	**8000**	**8306**

The profiles of the respondents are as follows:

Table 3: Profile of the respondents

	(%)
Age	
18 to 25 years	24
26 to 35 years	23
36 to 45 years	21
46 to 55 years	12
56 years and above	20
Gender	
Male	59
Female	41
Class	
Poor	26
Lower	36
Middle	23
Rich	15
Caste	
Scheduled Caste (SC)	15
Scheduled Tribe (ST)	5
Other Backward Class (OBC)	43
Other (General)	37
Religion	
Hindu	87
Muslim	8
Christian	3
Sikh	1
Other religious minorities	1
Educational level	
Non-literate	3
Up to primary	14
Up to matric	37
College and above	46
Location	
Rural	21
Urban	79

Note: All figures are in percentages, and are rounded off.

3. Research Instruments

Questionnaire

The English questionnaire was designed after a series of meetings and discussions with the research team comprising colleagues from Lokniti and Common Cause. The main objective of the survey was to understand the changing nature of cybercrime and explore how victims navigate reporting processes, the role played by banks and other institutions, and the challenges they face in seeking redress. Most questions in the questionnaire were structured, that is, they were closed-ended. However, there were some questions that were kept open-ended in order to find out the respondents' spontaneous feelings about an issue without giving him or her a pre-decided set of options.

Translation

After finalising the questionnaire, the translations were done for each state by the state teams. The questionnaire was translated into ten languages (Assamese, Bangla, Gujarati, Hindi, Kannada, Malayalam, Marathi, Odia, Tamil, Telugu).

Training workshops

To train the field investigator, a rigorous one-day training workshop was organised in each state before the fieldwork began. In the workshops, the trainers conducted an intensive and interactive workshop where field investigators underwent an orientation program and were trained rigorously on survey method interviewing techniques and communication with the respondent. They were also given a comprehensive and detailed understanding of the questionnaire, and the survey methodology was prepared for the interviewers. For a better understanding of the questionnaire, mock interviews were also conducted by the FIs so that they could understand the logic behind all the questions. Moreover, as the fieldwork was to be done on the app, they were taught about the installation of the app, and then how to feed the response and the mechanism for any challenges they face during fieldwork.

Fieldwork

The fieldwork for the study was conducted in the months of November and December, 2025. Field investigators were mainly students of social sciences belonging to colleges and universities in different parts of the country. They conducted face-to-face interviews with the respondents at the place of work or residence of the respondent, using a standardised questionnaire in the language spoken and understood by him or her. Our team was monitoring data quality during fieldwork, and whenever we found any discrepancies, we immediately contacted the concerned team to notify the FIs and warn them. In case of any doubt about the quality of the interview, the FIs were asked to do extra interviews.

Data processing and data cleaning

The data was saved on the server of the app used for the study. Once the fieldwork was over, the overall data was downloaded and then converted into SPSS format.

Data cleaning

Preliminary analysis was done to check whether there are any invalid entries or unexplained data points. If we located any such cases, we rectified and cleaned the file before the final analysis.

APPENDIX 2: Survey Questionnaire for Cybercrime Victims and Close Aides of Victims

Z1. State: _____

Z2. District: _____

Z3. Location Name: _____

Z4. Location Category ***(Do not ask, judge on your own):***

1. Village
2. Town (50,000 – 1 lakh population)
3. Small City (1 – 5 lakh population)
4. Big City (5 – 10 lakh population)

Z5. Type of location ***(Do not ask, follow the instructions given by the state team)***

1. Lower
2. Middle
3. Upper-middle
4. Upper/Rich

F1. Investigator Roll No.: _____

F1a. Investigator Name: _____

F2. Date of Interview: _____

INVESTIGATOR'S INTRODUCTION AND STATEMENT OF INFORMED CONSENT

My name is _____ and I am from Lokniti-CSDS (also mention the name of your university/college), a research institute based in Delhi. We are conducting a survey about people's experiences with various cybercrimes and measures of online safety, for which we are interviewing thousands of people across the country. The survey aims to understand the readiness of police system and banks in handling various incidents of cybercrime. This survey is an independent study and it is not linked to any political party or government agency. Any information you provide will be kept strictly confidential. The findings will be used for research purposes. It usually takes 25-30 minutes to complete the interview. Please take some time out and help me in completing this survey.

F3. Can I start the interview now?

1. Yes
2. No ***(Stop the discussion and go to some other person/house)***

F4. Name of the Respondent: _____

Z6. Age of the Respondent: _____ ***(in years)***

98. No response ***(If age is above 95 years, enter code 95)***

Z7. Gender ***(Do not ask, determine on your own)***

1. Male 2. Female 3. Others

INTERVIEW BEGINS

Q1. Do you own a mobile phone?

1. Yes, a smartphone
2. Yes, a basic/button phone
3. No, but I use another family member's phone
4. No

98. No response / Don't know

Q2. ***(If 1, 2 or 3 in Q1)*** Do you have access to an internet connection through data packs or Wi-Fi on this mobile?

1. Yes, always
2. Yes, sometimes
3. No, never

98. No response / Don't know

99. Not applicable

Q3. ***(If '4' or '98' in Q1 or '3' '98' in Q2)*** Do you use the internet on any other device?

1. Yes
2. No (Stop the survey and interview the next respondent)

98. No response / Don't know

Q4. ***(If '1' or '2' in Q2, or '1' in Q3)*** How often do you use the following – daily, once or twice a week, once or twice a month, or never?
(Read the following items one by one and mark the answer given by the respondent)

1. Daily
2. Once or twice a week
3. Once or twice a month
4. Never 98. No response

a. Social media apps/websites ***(WhatsApp, Instagram, Facebook, etc.)***

b. Mobile banking apps/net-banking websites

c. UPI

Q4a. ***(If '1' or '2' in Q2, or '1' in Q3)*** And how often do you use the following – often, sometimes, rarely, or never?

(Read the following items one by one and mark the answer given by the respondent)

1. Often 2. Sometimes 3. Rarely
4. Never 98. No response

a. Online investment or other financial services (FDs, mutual funds, stock trading, etc.)
b. Digital loan apps (LazyPay, MoneyTap, etc.)

Q5. ***(If '1' or '2' in Q2, or '1' in Q3)*** When making payments online, how frequently do you use the following – many times, sometimes, or never?

(Read the following items one by one and mark the answer given by the respondent)

1. Many times 2. Sometimes 3. Never
98. No response 99. I don't make any online payments

a. UPI
b. NEFT/RTGS
c. Debit/credit card payment
d. Payment wallets
e. Any other ***(Please specify):*** _____

Q6. ***(If '1' or '2' in Q2, or '1' in Q3)*** How frequently do you make online payments for the following purposes – regularly, sometimes, or never?

(Read the following items one by one and mark the answer given by the respondent)

1. Regularly 2. Sometimes 3. Never
98. No response 99. I don't use online payments

a. Bill payments (electricity, water, mobile recharge, etc.)
b. Rent, fees, or EMIs
c. Sending/receiving money to/from family
d. Online shopping for groceries and other items (Flipkart, Amazon, etc.)
e. Booking ticket or travel
f. International transactions

Q7. ***(If '1' or '2' in Q2, or '1' in Q3)*** Do you have a 2-step verification system, like using PIN and OTP, on the following apps?

(Read the following items one by one and mark the answer given by the respondent)

1. Yes 2. No 3. I don't know about this (silent option)
98. No response 99. I don't use any such apps

a. Internet banking apps
b. UPI apps (Phone Pe, Google Pay, BHIM UPI, etc.)
c. WhatsApp

Q8. ***(If '1' or '2' in Q2, or '1' in Q3)*** If you receive any of the following from an unknown person or number, will you do the following – yes, mostly; yes, sometimes; or never?

(Read the following items one by one and mark the answer given by the respondent)

1. Yes, mostly 2. Yes, sometimes 3. Never
4. I will do it only after verifying the source ***(silent option)*** 98. No response

a. Click on a link that you received
b. Pick up a phone call from an unsaved number
c. Open a photo, video or other type of file
d. Press a button or number if an unknown caller asks you to do that
e. Share an OTP with the caller

Q9. ***(If '1' or '2' in Q2, or '1' in Q3)*** In your opinion, how safe are the following modes of online banking – very safe, somewhat safe, somewhat unsafe, very unsafe?

(Read the following items one by one and mark the answer given by the respondent)

1. Very safe 2. Somewhat safe 3. Somewhat unsafe
4. Very unsafe 98. No response

a. UPI
b. Mobile banking apps
c. Internet banking websites
d. Debit/credit card payments
e. Digital loan apps/websites
f. Stock trading apps/websites
g. Wallet-based apps (Phone Pe, BHIM, Google Pay, PayTm, etc.)

Q10. ***(If '1' or '2' in Q2, or '1' in Q3)*** How much do you trust your telecom service provider to keep your number and related personal information safe – a lot, somewhat, not much, or not at all?

1. A lot
2. Somewhat
3. Not much
4. Not at all
98. No response

Q11. ***(If '1' or '2' in Q2, or '1' in Q3)*** How often do you receive the following – many times, sometimes, rarely, or never?

(Read the following items one by one and mark the answer given by the respondent)

1. Many times 2. Sometimes 3. Rarely
4. Never 98. No response

a. A call/text message for the delivery of a product you never ordered
b. A call/text message saying your phone number has been linked to illegal activities
c. A call from a bank official asking for personal or account details
d. A call/text message from an unknown number claiming to be your friend/relative who is in urgent need of money
e. A call/text message about an investment opportunity, guaranteeing a high return
f. A call from police or someone in authority claiming that your friend/relative is in danger or has committed some crime, etc.

Q12. ***(If '1' or '2' in Q2, or '1' in Q3)*** How safe do you feel about sharing or posting personal data on social media platforms – very safe, somewhat safe, somewhat unsafe, or very unsafe?

(Give examples of social media platforms ONLY if respondent asks – WhatsApp, Facebook, Instagram, YouTube, etc.)

1. Very safe
2. Somewhat safe
3. Somewhat unsafe
4. Very unsafe

98. No response

Q13. ***(If '1' or '2' in Q2, or '1' in Q3)*** On a scale of 1 to 5, where 1 means "not at all scared" and 5 means "very scared", how scared are you of the following things happening:

(Read the following items one by one and mark the answer given by the respondent)

1. Not at all scared 2. 3.
4. 5: Very scared 98. No response

a. Losing money through online frauds or scams
b. Someone pretending to be you online (using your name or photo, etc.)
c. Someone digitally stealing and misusing your personal IDs such as Aadhaar Card, etc.
d. Someone hacking your devices such as phone, laptop, etc.
e. Someone secretly recording your audio or video without your consent

Q14. ***(If '1' or '2' in Q2, or '1' in Q3)*** Compared to others, how likely are you to be targeted online because of your…

(Read the following items one by one and mark the answer given by the respondent)

1. Yes, very much 2. Yes, somewhat 3. Not at all

98. No response

a. Age
b. Gender
c. Religion
d. Caste
e. Profession 99. NA
f. Regional identity
g. Sexual orientation
h. Disability 99. NA

Q15. ***(If '1' or '2' in Q2, or '1' in Q3)*** In your opinion, have the following crimes increased a lot, increased somewhat, or remained the same, in the last two years?

(Read the following items one by one and mark the answer given by the respondent)

1. Increased a lot 2. Increased somewhat 3. Remained the same
4. Decreased (silent option) 98. No response

a. People losing money through online scams or frauds
b. Sextortion, or blackmail using sexual content over call/message/video
c. Digital arrest

d. Someone pretending to be you online (using your name or photo, etc.)

e. Online sexual harassment using real or fake photos/videos

f. Cyber bullying/harassment or abuse on social media

Q16. ***(If '1' or '2' in Q2, or '1' in Q3)*** Have you been a victim of a cybercrime in the last 2-3 years?

1. Yes
2. No

98. No response

Q17. ***(If '2' in Q16)*** Did you help the victim closely in registering the cyber complaint or in handling the overall issue?

1. Yes
2. No

98. No response/I don't know

QUESTIONS 18-43 FOR VICTIMS OF CYBERCRIMES

Q18. ***(If '1' in Q16)*** What type of crime did you face? ***(First, write the answer in the space provided, and then select the correct answer from the options given and click on it)***

_____

1. Digital financial frauds (like scam, fake money transfer, or digital arrest)
2. Hacking of phone or any other device without your knowledge
3. Someone stealing your personal data (e.g. name, photo, location, Aadhaar Card, Pan Card or other ID cards, etc.)
4. Online sexual harassment
5. Cyber bullying or harassment/abuse on social media, where someone targeted you with abusive messages

97. Any other ***(Please specify):*** _____

98. No response

Q19. ***(If '1' in Q16)*** If there was a financial loss, how much was it? _____ ***(in Rupees)***

00. No financial loss 98. No response

Q19a. ***(If 'incurred a loss' in Q19)*** If there was a financial loss, was it from a government or a private bank account?

1. Government bank account
2. Private bank account

97. Any other ***(Please specify):*** _____

98. No response

Q20. ***(If '1' in Q16)*** Did you complain to the police?

1. Yes
2. Went to the police initially, but did not pursue the case
3. No

98. No response / Don't know

Q21. ***(If '3' in Q20)*** Why did you not complain to the police? (First, write the answer in the space provided, and then select the correct answer from the options given and click on it.)

_____

1. It was not a big amount
2. I felt embarrassed/ashamed
3. The police would have asked for a bribe
4. The complaint procedure is difficult/complex
5. I was scared to go to the police

97. Any other ***(Please specify):*** _____

98. No response

Q22. ***(If '1' or '2' in Q20)*** What was the first step you took when you found out about the cybercrime?

(Do not read out the answer options)

1. Went to the local police station
2. Went to the cyber police station in my jurisdiction
3. Called the local police/cyber police station
4. Called the police helpline number for cybercrimes
5. Filed an online complaint
6. Complained to the bank

97. Any other ***(Please specify):*** _____

98. No response

Q23. ***(If '1' or '2' in Q20)*** Did your complaint get registered as an FIR?

1. Yes
2. No

98. No response/Don't know

Q24. ***(If '2' in Q23)*** What was the reason?

(Do not read out the answer options)

1. Because I did not want to pursue the case
2. Because the police refused to register

97. Any other reason ***(Please specify):*** _____

98. No response

Q25. ***(If '1' or '2' in Q20)*** Did you need to go to the police station in person?

1. Yes, to the local police station
2. Yes, to the cyber police station/cell
3. Yes, to both
4. No

98. No response

Q26. ***(If 'yes' in Q25)*** How long did you have to wait at the police station to get your complaint registered? _____ ***(in hours)***

98. No response

Q27. ***(If 'yes' in Q25)*** How many times did you have to visit the police station (local/cyber) during the investigation process? _____ ***(number of times)***

98. No response

Q28. ***(If '1' or '2' in Q20)*** Overall, how easy or difficult was it to register a police complaint about the cybercrime – very easy, somewhat easy, somewhat difficult, or very difficult?

1. Very easy
2. Somewhat easy
3. Somewhat difficult
4. Very difficult
98. No response

Q29. ***(If '1' or '2' in Q20)*** Did you have to make any payment to the police at any point?

1. Yes
2. No
98. No response

Q30. ***(If '1' in Q29)*** How much payment did you have to make? _____ ***(in Rupees)***

98. No response

Q31. ***(If '1' or '2' in Q20)*** Did you have to contact someone in your personal network to put pressure on the police to deal with your case properly?

1. Yes
2. No
98. No response

Q32. ***(If '1' in Q31)*** Who did you contact? ***(Do not read out the answer options)***

1. Senior police officers
2. Senior government officials
3. Local politician
4. Local person of influence
5. Media
6. NGO
7. External agencies such as NHRC, NCW, etc. ***(Specify which):*** _____

97. Any other ***(Please specify):*** _____

98. No response

Q33. ***(If '1' in Q16)*** Did you complain separately to the bank?

1. Yes
2. No
98. No response

Q34. ***(If '1' in Q33)*** How soon after the fraud did you report it? (Do not read out the answer options)

1. Within 24 hours 2. Within 48 hours 3. More than 48 hours

98. No response

Q35. ***(If '1' in Q33)*** Did the bank take any action such as freezing all your accounts, etc. after receiving the complaint?

1. Yes, completely
2. Yes, partially
3. No
98. No response

Q36. ***(If '1' in Q16)*** Did your case go to court?

1. Yes
2. No
98. No response

Q37. ***(If '1' in Q36)*** What is the current status of your case? (Do not read out the answer options)

1. The investigation is ongoing
2. The case has been resolved
3. The case has not been resolved but it is closed
4. I am not aware of the status as I did not follow up with the authorities
98. No response

Q38. ***(If '2' or '3' in Q37)*** How satisfied were you with the outcome – completely satisfied, somewhat satisfied, somewhat dissatisfied, or completely dissatisfied?

1. Completely satisfied
2. Somewhat satisfied
3. Somewhat dissatisfied
4. Completely dissatisfied
98. No response

Q39. ***(If '1' in Q16)*** Were you able to recover your lost money?

1. Yes, the whole amount
2. Yes, partial amount
3. No
98. No response

Q40. ***(If '1' or '2' in Q39)*** How long after the cyber fraud did you recover the money? _____ ***(in days)***

98. No response

Q41. ***(If '1' in Q16)*** How satisfied are you with the coordination between the bank and the police in resolving your cybercrime complaint – very satisfied, somewhat satisfied, somewhat unsatisfied, or very unsatisfied?

1. Very satisfied
2. Somewhat satisfied
3. Somewhat unsatisfied
4. Very unsatisfied
5. There has been no coordination so far (silent option)
98. No response
99. Did not complain to the bank/police

Q42. ***(If '1' in Q16)*** How satisfied were you with the following – very satisfied, somewhat satisfied, somewhat dissatisfied, or very dissatisfied?

(Read the following items one by one and mark the answer given by the respondent)

1. Very satisfied 2. Somewhat satisfied 3. Somewhat dissatisfied
4. Very dissatisfied 5. Never used this service ***(silent option)*** 98. No response

a. Police helpline number for cyber complaints

b. Online police portal for cyber crimes

c. The complaint registration process at the cyber police station

d. The investigation of cybercrimes by the police

e. The court dealing with your case of cybercrime

f. The bank's role in recovering the money

g. The RBI Banking Lokpal

Q43. **(If '1' in Q16)** Some victims of financial cybercrimes believe that their financial data was leaked by a bank insider because of which they were targeted by criminals. In your case, do you think the crime occurred due to a breach of your personal data by the bank or its personnel?

1. Yes, it occurred due to a breach of personal data
2. No, it didn't happen because of that

98. Don't know

FOR FAMILY MEMBER/CLOSE FRIEND OF CYBERCRIME VICTIMS

Q44. ***(If '1' in Q17)*** What type of crime did they face? (First, write the answer in the space provided, and then select the correct answer from the options given and click on it.) _____

1. Digital financial frauds (like scam, fake money transfer, or digital arrest)
2. Hacking of phone or any other device without their knowledge
3. Someone stealing their personal data (e.g. name, photo, location, Aadhaar Card, Pan Card or other ID cards, etc.)
4. Online sexual harassment
5. Cyber bullying or harassment/abuse on social media, where someone targeted them with abusive messages

97. Any other (Please specify): _____

98. No response/ I don't know

Q45. ***(If '1' in Q17)*** If there was a financial loss, how much was it? _____ ***(in Rupees)***

00. No financial loss

98. No response/ I don't know

Q45a. ***(If 'incurred a loss' in Q45)*** If there was a financial loss, was it from a government or a private bank account?

1. Government bank account
2. Private bank account

97. Any other (Please specify): ¬_____

98. No response/ I don't know

Q46. ***(If '1' in Q17)*** Did they complain to the police?

1. Yes
2. Went to the police initially, but did not pursue the case
3. No

98. No response/ I don't know

Q47. ***(If '3' in Q46)*** Why did they not complain to the police? (First, write the answer in the space provided, and then select the correct answer from the options given and click on it.)

_____

1. It was not a big amount
2. I/they felt embarrassed/ashamed
3. The police would have asked for a bribe
4. The complaint procedure is difficult/complex
5. I/they was/were scared to go to the police

97. Any other ***(Please specify):*** _____

98. No response/ I don't know

Q48. ***(If '1' or '2' in Q46)*** What was the first step they took when they found out about the cybercrime?

(Do not read out the answer options)

1. Went to the local police station
2. Went to the cyber police station in their jurisdiction
3. Called the local police/cyber police station
4. Called the police helpline number for cybercrimes
5. Filed an online complaint
6. Complained to the bank

97. Any other ***(Please specify):*** _____

98. No response/ I don't know

Q49. ***(If '1' or '2' in Q46)*** Did their complaint get registered as an FIR?

1. Yes
2. No

98. No response/ I don't know

Q50. ***(If '2' in Q49)*** What was the reason?

(Do not read out the answer options)

1. Because they did not want to pursue the case
2. Because the police refused to register

97. Any other reason (Please specify): _____

98. No response/ I don't know

Q51. ***(If '1' or '2' in Q46)*** Did they need to go to the police station in person?

1. Yes, to the local police station
2. Yes, to the cyber police station/cell
3. Yes, to both
4. No

98. No response/ I don't know

Q52. ***(If 'yes' in Q51)*** How long did they have to wait at the police station to get their complaint registered? _____ ***(in hours)***

98. No response/ I don't know

Q53. ***(If 'yes' in Q51)*** How many times did they have to visit the police station (local/cyber) during the investigation process? _____ ***(number of times)***

98. No response/ I don't know

Q54. ***(If '1' or '2' in Q46)*** Overall, how easy or difficult was it to register a police complaint about the cybercrime – very easy, somewhat easy, somewhat difficult, or very difficult?

1. Very easy
2. Somewhat easy
3. Somewhat difficult
4. Very difficult

98. No response/ I don't know

Q55. ***(If '1' or '2' in Q46)*** Did they have to make any payment to the police at any point?

1. Yes
2. No

98. No response/ I don't know

Q56. ***(If '1' in Q55)*** How much payment did they have to make? _____ ***(in Rupees)***

98. No response/ I don't know

Q57. ***(If '1' or '2' in Q46)*** Did they have to contact someone in their personal network to put pressure on the police to deal with their case properly?

1. Yes
2. No

98. No response/ I don't know

Q58. ***(If '1' in Q57)*** Who did they contact? ***(Do not read out the answer options)***

1. Senior police officers
2. Senior government officials
3. Local politician
4. Local person of influence
5. Media
6. NGO
7. External agencies such as NHRC, NCW, etc. ***(Specify which):*** _____

97. Any other ***(Please specify):*** _____

98. No response/ I don't know

Q59. ***(If '1' in Q17)*** Did they complain separately to the bank?

1. Yes
2. No
98. No response/ I don't know

Q60. ***(If '1' in Q59)*** How soon after the fraud did they report it? ***(Do not read out the answer options)***

1. Within 24 hours
2. Within 48 hours
3. More than 48 hours
98. No response/ I don't know

Q61. ***(If '1' in Q59)*** Did the bank take any action such as freezing all their accounts, etc. after receiving the complaint?

1. Yes, completely
2. Yes, partially
3. No
98. No response/ I don't know

Q62. ***(If '1' in Q17)*** Did their case go to court?

1. Yes
2. No
98. No response/ I don't know

Q63. ***(If '1' in Q62)*** What is the current status of their case? ***(Do not read out the answer options)***

1. The investigation is ongoing
2. The case has been resolved
3. The case has not been resolved but it is closed
4. I/they did not follow up with the authorities
98. No response/ I don't know

Q64. ***(If '2' or '3' in Q63)*** How satisfied were you with the outcome – completely satisfied, somewhat satisfied, somewhat dissatisfied, or completely dissatisfied?

1. Completely satisfied
2. Somewhat satisfied
3. Somewhat dissatisfied
4. Completely dissatisfied
98. No response/ I don't know

Q65. ***(If '1' in Q17)*** Were they able to recover their lost money?

1. Yes, the whole amount
2. Yes, partial amount
3. No
98. No response/ I don't know

Q66. ***(If '1' or '2' in Q65)*** How long after the cyber fraud did they recover the money? _____ ***(in days)***

98. No response/ I don't know

Q67. ***(If '1' in Q17)*** How satisfied are you with the coordination between the bank and the police in resolving their cybercrime complaint – very satisfied, somewhat satisfied, somewhat unsatisfied, or very unsatisfied?

1. Very satisfied
2. Somewhat satisfied
3. Somewhat unsatisfied
4. Very unsatisfied
5. There has been no coordination so far (silent option)
98. No response
99. Did not complain to the bank/police

Q68. ***(If '1' in Q17)*** How satisfied were you with the following – very satisfied, somewhat satisfied, somewhat dissatisfied, or very dissatisfied?

(Read the following items one by one and mark the answer given by the respondent)

1. Very satisfied 2. Somewhat satisfied 3. Somewhat dissatisfied
4. Very dissatisfied 5. Never used this service (silent option)
98. No response/ I don't know

a. Police helpline number for cyber complaints
b. Online police portal for cyber crimes
c. The complaint registration process at the cyber police station
d. The investigation of cybercrimes by the police
e. The court dealing with your case of cybercrime
f. The bank's role in recovering the money
g. The RBI Banking Lokpal

Q69. ***(If '1' in Q17)*** Some victims of financial cybercrimes believe that their financial data was leaked by a bank insider, because of which they were targeted by criminals. In your case, do you think the crime occurred due to a breach of your personal data by the bank or its personnel?

1. Yes, it occurred due to a breach of personal data
2. No, it didn't happen because of that
98. Don't know

QUESTIONS 70-76 TO BE ASKED FROM ALL THE RESPONDENTS

Q70. In your opinion, how equipped do you think the police is to deal with financial cybercrimes – very equipped, somewhat equipped, not much equipped, or not at all equipped?

1. Very equipped
2. Somewhat equipped
3. Not much equipped
4. Not at all equipped
98. No response

Q71. In your opinion, how trained are these people to deal with cybercrimes - very much, somewhat, not much, or not at all?

(Read the following items one by one and mark the answer given by the respondent)

1. Very much 2. Somewhat 3. Not much
4. Not at all 98. No response

a. Police personnel

b. Bank officials

c. Judges/Magistrates

Q72. If you are a victim of a case of cybercrime in the future, how likely are you to report the case to the police - very likely, somewhat likely, not much likely, or not at all likely?

1. Very likely
2. Somewhat likely
3. Not much likely
4. Not at all likely
98. No response

Q73. I will now read two statements, please tell me which one do you agree with the most?

(Read out both the statements)

Statement 1: It is the individual's responsibility to ensure they protect their data.

Statement 2: It is the government's/bank authorities' responsibility to ensure data protection and educate people about it.

1. Agree with statement 1
2. Agree with statement 2
98. No response

Q74. In your opinion, what is the most important step that the government/authorities can take to ensure the digital safety of the citizens? ***(Do not read out the answer options)***

1. Awareness campaigns on cybersecurity
2. Improve the effectiveness of cybercrime reporting portals
3. Implementation of data protection regulations
4. Devise regulatory mechanisms to block suspicious calls/websites
5. Track online fraudulent transactions to recover lost money
6. Better training of cybersecurity police personnel

97. Any other (Please specify): _____

98. No response

Q75. These days, there are many advertisements and messages etc. to make people aware of the risks and cautions about cybersecurity. Have you received any such message or seen any such advertisement?

1. Received message
2. Seen advertisement
3. Both
4. Neither/none of them
98. No response

Q76. Do you take the following actions to protect your personal data?

(Read the following items one by one and mark the answer given by the respondent)

1. Yes, always 2. Yes, sometimes 3. No, never 98. No response

a. Avoid saving passwords in browsers

b. Avoid using public Wi-Fi

c. Avoid reusing passwords

d. Check app permissions such as access to contacts, location, or storage

e. Verify website or app authenticity such as checking for https: or gov.in

BACKGROUND INFORMATION

Z8. Are you married?

1. No
2. Yes
3. Divorced
4. Widow/Widower
5. Separated

98. Did not answer/No response

Z9. What is your educational level?

1. Illiterate (Can't read or write at all)
2. Below primary school
3. Primary pass (5th class)
4. Middle pass (8th class)
5. Matric pass (10th class)
6. Studying in 11th or 12th or junior college
7. Inter pass (12th class)
8. Diploma (After 10th or 12th class)
9. Graduate/pursuing graduation/in college
10. Post graduate/pursuing post graduation
11. Higher degree (MPhil, PhD)
12. Professional degree/course (Law, BTech, etc.)

97. Any other ***(Please specify):*** _____

98. Did not answer/No response

Z10a. What is your main occupation? ***(If retired, find out previous job.)***

(First note down the response in the space given below and then click on the right/most suitable option from the menu provided) _____

1. **Higher Professionals:** Engineers, Doctors, Lawyers, Chartered Accountants/Financial Experts, Professors, Corporate Managers/Chief Executives (CEO), Company secretaries, Production and operation managers, Scientists, Architects, Statisticians/Mathematicians, Writer, Creative or Performing Artists, etc.

2. **Lower Professionals:** Science technicians, Computer Operator, Data Entry, Finance and Sales Associate Professionals, Traditional Medicine practitioners (Ayurvedic/ Homeopathic Doctor, Faith Healer), Nurse, Compounder, School Teacher, Tutor, Priest, Astrologer, NGO worker/Social worker, librarians, etc.
3. **Government Managerial job:** Manager, Director, Executive, MP, MLA etc.
4. **Government Administrative job:** Administrators (First-Second Class Officer), Major in Army, Colonel, Brigadier, Police Inspector, Safety and Quality Inspectors
5. **Government Clerical Jobs:** Class III Officers, Clerk, Cashiers/Tellers, Typists, Army Jawan, Police Constable
6. **Government Class IV:** Peon, Postman, Gram Sevak, Amin, Safai Karamchari, Library Assistants, etc.
7. **Big and Medium Traders:** Big Shopkeepers, Factory Owners, Hotel Owners, Petrol Pumps, Taxi Owners, Big Travel Agency, Small Hotels, Property Dealers, Jewellers etc.
8. **Small Trader:** Grocery Shop, Small Travel Agency, Phone Booth, Broker, Parlour, Rickshaw Owner, Landlord, etc.
9. **Small/Temporary Business:** Temporary Shopkeeper, Sales Man, Delivery Boy, Shop Assistant, Small Shopkeepers, etc.
10. **Service/Service Area:** Cook, Waiter, Washerman, Barber, Domestic Servant/ Personal Care Workers, Chowkidar, Travel Attendants/Guides, Shop Sales Persons and Demonstrators, Delivery Boy, Private Guard, Safai Karamchari etc.
11. **Skilled Workers:** Driver, Mechanic, Electrician, Plumber, Tailor, Cobbler, Carpenter, Sailor, Gardeners, Fishery Workers, Miners, Stone Cutter and Carvers, Sculptors, Painters, Welders, Sheet metal workers, Blacksmith, Goldsmith, Glass makers, Handicraft workers, Printing and related workers, etc.
12. **Semi-skilled workers:** Artisans, bricklayers, potters, stone cutters, furniture, basketry, mat makers, Food processing workers, etc.
13. **Wage labourer (non-agriculture):** Rickshaw pullers, loaders, construction workers, street vendors, garbage collectors, mining and manufacturing labourers, etc.
14. **Farmer:** tilling own land or someone else's land
15. **Agricultural Labourer:** Landless farm labourers
16. Dairy/Fish/Poultry/Animal Husbandry work
17. Student but doing part time job
18. Housewife/househusband but doing part time job
19. Student
20. Housewife/househusband
21. Unemployed or looking for employment

97. Any other work (Please specify): _____
98. Did not answer/No response

Z10b. Are you the main earner of your household?

1. No
2. Yes

98. Don’t Know/No response

Z10c. ***(If 1 in Z10b)*** What is the occupation of the main earner of your household? (If retired, find out previous job.)

(First note down the response in the space given below and then click on the right/most suitable option from the menu provided) _____

_____

01. **Higher Professionals:** Engineers, Doctors, Lawyers, Chartered Accountants/Financial Experts, Professors, Corporate Managers/Chief Executives (CEO), Company secretaries, Production and operation managers, Scientists, Architects, Statisticians/Mathematicians, Writer, Creative or Performing Artists, etc.
02. **Lower Professionals:** Science technicians, Computer Operator, Data Entry, Finance and Sales Associate Professionals, Traditional Medicine practitioners (Ayurvedic/ Homeopathic Doctor, Faith Healer), Nurse, Compounder, School Teacher, Tutor, Priest, Astrologer, NGO worker/Social worker, librarians, etc.
03. **Government Managerial job:** Manager, Director, Executive, MP, MLA etc.
04. **Government Administrative job:** Administrators (First-Second Class Officer), Major in Army, Colonel, Brigadier, Police Inspector, Safety and Quality Inspectors
05. **Government Clerical Jobs:** Class III Officers, Clerk, Cashiers/Tellers, Typists, Army Jawan, Police Constable
06. **Government Class IV:** Peon, Postman, Gram Sevak, Amin, Safai Karamchari, Library Assistants, etc.
07. **Big and Medium Traders:** Big Shopkeepers, Factory Owners, Hotel Owners, Petrol Pumps, Taxi Owners, Big Travel Agency, Small Hotels, Property Dealers, Jewellers etc.
08. **Small Trader:** Grocery Shop, Small Travel Agency, Phone Booth, Broker, Parlour, Rickshaw Owner, Landlord, etc.
09. **Small/Temporary Business:** Temporary Shopkeeper, Sales Man, Delivery Boy, Shop Assistant, Small Shopkeepers, etc.
10. **Service/Service Area:** Cook, Waiter, Washerman, Barber, Domestic Servant/ Personal Care Workers, Chowkidar, Travel Attendants/Guides, Shop Sales Persons and Demonstrators, Delivery Boy, Private Guard, Safai Karamchari etc.
11. **Skilled Workers:** Driver, Mechanic, Electrician, Plumber, Tailor, Cobbler, Carpenter, Sailor, Gardeners, Fishery Workers, Miners, Stone Cutter and Carvers, Sculptors, Painters, Welders, Sheet metal workers, Blacksmith, Goldsmith, Glass makers, Handicraft workers, Printing and related workers, etc.
12. **Semi-skilled workers:** Artisans, bricklayers, potters, stone cutters, furniture, basketry, mat makers, Food processing workers, etc.
13. **Wage labourer (non-agriculture):** Rickshaw pullers, loaders, construction workers, street vendors, garbage collectors, mining and manufacturing labourers, etc.
14. **Farmer:** tilling own land or someone else's land
15. **Agricultural Labourer:** Landless farm labourers
16. Dairy/Fish/Poultry/Animal Husbandry work
17. Student but doing part time job
18. Housewife/househusband but doing part time job
19. Student

20. Housewife/househusband
21. Unemployed or looking for employment
97. Any other work (Please specify): _____
98. Did not answer/No response

Z11. What is your religion?

1. Hindu
2. Muslim
3. Christian
4. Sikh
5. Buddhist/Neo-Buddhist
6. Jain
7. Parsi
8. No religion (Atheist)
97. Any other (Please specify): _____
98. No response

Z12. What is your caste category?

1. Scheduled Caste (SC)
2. Scheduled Tribe (ST)
3. Other Backward Classes (OBC)
4. General
98. Did not answer/ No response

Z13. What is your caste/community? (First note down the given answer and then find the relevant option from the list below) _____

Z14a. (If Town/City) Type of house where Respondent lives (own or rented)

1.	House/Flat/Bungalow (5+ bedrooms)
2.	House/Flat (3 or 4 bedrooms)
3.	House/Flat with 2 bedrooms
4.	House/Flat with 2 pucca rooms
5.	House with 1 pucca room
6.	Mainly kutcha house
7.	Slum/Jhuggi Jhopri

Z14b. (If Village) Type of house where Respondent lives (own or rented)

1.	Pucca (both wall and roof made of pucca material)
2.	Pucca-Kutcha (either wall or roof made from pucca material and other of kutcha material)
3.	Kutcha (both wall and roof made from kutcha material other than mentioned in category 4)
4.	Hut (both wall and roof made from grass, leaves, mud, un-burnt brick or bamboo)

Z15. Do you or your family own these things?

	Yes	No
a. Car/jeep/van	1	2
b. Scooter / motorcycle/ moped	1	2
c. Air conditioner	1	2
d. Computer/laptop/iPad	1	2
e. Electric fan/cooler	1	2
f. Washing Machine	1	2
g. Fridge	1	2
h. Television	1	2
i. Bank/Post Office Account	1	2
j. ATM/Debit Card	1	2
k. LPG Gas	1	2
l. Internet connection in the house (besides mobile phone)	1	2
m. Toilet in the house	1	2
n. Pumping set (If the respondent lives in village)	1	2
o. Tractor (If the respondent lives in village)	1	2

Z16. Keeping in mind everyone in the family, how much is the family monthly income? ***(First, note down the given answer and then find the relevant option from the list below)***

1. Rs. 1000 to 2000
2. Rs. 2001 to 3000
3. Rs. 3001 to 5000
4. Rs. 5001 to 7500
5. Rs. 7501 to 10,000
6. Rs. 10,001 to 15,000
7. Rs. 15,001 to 20,000
8. Rs. 20,001 to 30,000
9. Rs. 30,001 to 50,000
10. Rs. 50,000 to 1 lakh
11. More than Rs. 1 lakh

98. Did not answer/No response

Z17. Could you give me your mobile/telephone no.? We may want to get in touch with you later if we have any queries. ***(If mobile number is not provided, please type 'zero' ten times)***

Mobile no.: _____

Z18. GPS: _____

APPENDIX 3: Details of How the Indices were Constructed

Index 1: Safety Index

The index was constructed by taking into account five sub-questions of Q9, which are:

Q9. In your opinion, how safe are the following modes of online banking – very safe, somewhat safe, somewhat unsafe, very unsafe?

a. UPI
b. Mobile banking apps
c. Internet banking websites
d. Debit/credit card payments
g. Wallet-based apps (Phone Pe, BHIM, Google Pay, PayTm, etc.)

In each sub-question, the response offered to the respondents was:

- Very safe
- Somewhat safe
- Somewhat unsafe
- Very unsafe
- No response

Step 1: An answer that was 'very safe' was assigned the value of 4. An answer that was 'somewhat safe' was assigned the score of 3. An answer that was 'somewhat unsafe' was assigned the score of 2. The answer 'very unsafe' was assigned the score of 1, and 'No response' to the sub-questions was assigned a score of 0.

Step 2: The scores of all five sub-questions were summed up. The result, summated scores range from 0 to 20.

Step 3: The summated scores were distributed across four newly created categories that indicated different degrees of perceived safety in online banking. Summated scores that ranged from 17 to 20 were categorized as very safe. Summated scores that ranged from 13 to 16 were categorized as somewhat safe. Summated scores ranging from 8 to 12 were categorized as somewhat unsafe, and summated scores that totalled 1 to 7 were categorized as very unsafe. The non-responses were set as missing.

Index of perceived safety of online banking

	Summated scores	Weighted distribution (%)
Very unsafe	1-7	11.6
Somewhat unsafe	8-12	24.6
Somewhat safe	13-16	40.5
Very safe	17-20	23.3

Index 2: Online Usage Index

The index was constructed by taking into account three sub-questions of Q4, which are:

Q4. How often do you use the following – daily, once or twice a week, once or twice a month, or never?

a. social media apps/websites (WhatsApp, Instagram, Facebook, etc.)
b. Mobile banking apps/net-banking websites
c. UPI

In each sub-question, responses offered to the respondents were:

- Daily
- Once or twice a week
- Once or twice a month
- Never
- No response

Step 1: An answer that was 'Daily' was assigned the value of 4. An answer that was 'once or twice a week' was assigned the score of 3. An answer that was 'once or twice a month' was assigned the score of 2. The answer 'never' was assigned the score of 1, and 'No response' to the sub-questions was assigned a score of 0.

Step 2: The scores of all three sub-questions were summed up. The result, summated scores range from 0 to 12.

Step 3: The summated scores were distributed across four newly created categories that indicated different degrees of usage of online services. Summated scores that ranged from 10 to 12 were categorised as High. Summated scores that ranged from 7 to 9 were categorized as Moderate. Summated scores ranging from 4 to 6 were categorised as low, and summated scores that totalled 1 to 3 were categorised as not used. The non-responses were set as missing.

Index of usage of online services

	Summated scores	Weighted distribution (%)
Not used	1-3	5.0
Low	4-6	15.5
Moderate	7-9	34.1
High	10-12	45.3

Index 3: Payment Index

The index was constructed by taking into account four sub-questions of Q5, which are:

Q5. When making payments online, how frequently do you use the following – many times, sometimes, or never?

a. UPI
b. NEFT/RTGS
c. Debit/credit card payment
d. Payment wallets

In each sub-question, the response offered to the respondents was:

- Many times
- Sometimes
- Never
- I don't make any online payments
- No response

Step 1: An answer that was 'many times' was assigned the value of 2. An answer that was 'sometimes' was assigned the score of 1. An answer that was 'never' and 'I don't make online payments' was assigned the value of 0.

Step 2: The scores of all four sub-questions were summed up. The result, summated scores range from 0 to 8.

Step 3: The summated scores were distributed across four newly created categories that indicated different degrees of usage of online payment. Summated scores that ranged from 5-8 were categorized as High. Summated scores that ranged from 3-4 were categorized as Moderate. Summated scores ranging from 1-2 were categorized as low, and summated scores that totalled 0 were categorized as Not used. The non-responses were set as missing.

Index of usage in online payments

	Summated scores	Weighted distribution (%)
Not used	0	16.0
Low	1-2	26.2
Moderate	3-4	31.1
High	5-8	26.7

Index 4: Fraudulent Index

The index was constructed by taking into account six sub-questions of Q11, which are:

Q11. How often do you receive the following – many times, sometimes, rarely, or never?

a. A call/text message for the delivery of a product you never ordered
b. A call/text message saying your phone number has been linked to illegal activities
c. A call from a bank official asking for personal or account details
d. A call/text message from an unknown number claiming to be your friend/relative who is in urgent need of money
e. A call/text message about an investment opportunity, guaranteeing a high return
f. A call from police or someone in authority claiming that your friend/relative is in danger or has committed some crime, etc.

In each sub-question, the response offered to the respondents was:

- Many times
- Sometimes

- Rarely
- Never
- No response

Step 1: An answer that was 'many times' was assigned the value of 4. An answer that was 'sometimes' was assigned the score of 3. An answer that was 'rarely' was assigned the score of 2. The answer 'never' was assigned the score of 1, and 'No response' to the sub-questions was assigned a score of 0.

Step 2: The scores of all four sub-questions were summed up. The result, summated scores range from 0 to 24.

Step 3: The summated scores were distributed across four newly created categories that indicated different degrees of receiving fraud text messages or calls. Summated scores that ranged from 18-24 were categorized as High. Summated scores that ranged from 12-17 were categorized as Moderate. Summated scores ranging from 7-11 were categorized as low, and summated scores that totalled 1-6 were categorized as No. The non-responses were set as missing.

Index of receiving fraud text messages or calls

	Summated scores	Weighted distribution (%)
No	1-6	29.7
Low	7-11	32.6
Moderate	12-17	25.5
High	18-24	12.2

Index 5: Digital Hygiene Index

The index was constructed by taking into account five sub-questions of Q76, which are:

Q76. Do you take the following actions to protect your personal data?

a. Avoid saving passwords in browsers
b. Avoid using public Wi-Fi
c. Avoid reusing passwords
d. Check app permissions such as access to contacts, location, or storage
e. Verify website or app authenticity, such as checking for https: or gov. in

In each sub-question, the response offered to the respondents was:

- Yes, always
- Yes, sometimes
- No, never
- No response

Step 1: An answer that was 'yes, always' was assigned the score of 3. An answer that was 'yes, sometimes' was assigned the score of 2. The answer 'no, never' was assigned the score of 1, and 'No response' to the sub-questions was assigned a score of 0.

Step 2: The scores of all five sub-questions were summed up. The result, summated scores range from 0 to 15.

Step 3: The summated scores were distributed across four newly created categories that indicated different degrees of measures taken to protect personal data. Summated scores that ranged from 13-15 were categorized as High. Summated scores that ranged from 10-12 were categorized as Moderate. Summated scores ranging from 6-9 were categorized as low, and summated scores that totalled 1-5 were categorized as Not used. The non-responses were set as missing.

Index of measures taken to protect personal data

	Summated scores	Weighted distribution (%)
Not used	1-5	21.1
Low	6-9	28.6
Moderate	10-12	29.3
High	13-15	21.0

Index 6: Unsolicited Call/Text Index

The index was constructed by taking into account four sub-questions of Q8, which are:

Q8. If you receive any of the following from an unknown person or number, will you do the following – yes, mostly; yes, sometimes; or never?

a. Click on a link that you received
c. Open a photo, video or other type of file

d. Press a button or number if an unknown caller asks you to do that

e. Share an OTP with the caller

In each sub-question, the response offered to the respondents was:

- Yes, mostly
- Yes, sometimes
- Never
- I will only do it after verifying the source (silent option)
- No response

Step 1: An answer that was 'yes, mostly' was assigned the score of 4. An answer that was 'yes, sometimes' was assigned the score of 3. An answer of 'I will only do it after verifying the source' was assigned the score of 2. The answer 'no, never' was assigned the score of 1, and 'No response' to the sub-questions was assigned a score of 0.

Step 2: The scores of all four sub-questions were summed up. The result, summated scores range from 0 to 16.

Step 3: The summated scores were distributed across four newly created categories that indicated different degrees of unsolicited calls or texts by an unknown person. Summated scores that ranged from 12-16 were categorized as High. Summated scores that ranged from 8-11 were categorized as Moderate. Summated scores ranging from 5-7 were categorized as low, and summated scores that totalled 1-4 were categorized as Not used. The non-responses were set as missing.

Index of vulnerability to unsolicited calls or texts by an unknown person

	Summated scores	Weighted distribution (%)
No vulnerability	1-4	44.0
Low vulnerability	5-7	22.6
Moderate vulnerability	8-11	23.3
High vulnerability	12-16	10.1

Index 7: Victim Index

The index was constructed by taking into account two separate questions, i.e., Q16 and Q17, which are:

Q16. Have you been a victim of a cybercrime in the last 2-3 years?

1. Yes
2. No

98. No response

Q17. Did you help the victim closely in registering the cyber complaint or in handling the overall issue?

1. Yes
2. No

98. No response

Step: An answer that was yes in both questions was summed up as 'yes' and merged to form the 'Victims' category, and 'No' and 'No responses' were merged separately.

Index of cybercrime victims

In the last two to three years	Weighted Distribution (%)
Victims/Those who assisted cybercrime victims	22.9
No	71.0
No response	6.1

Index 8: Complained to the police

The index was constructed by taking into account two separate questions, i.e., Q20 and Q46, which are:

Q20. (victims) Did you complain to the police?

1. Yes
2. Went to the police initially, but did not pursue the case
3. No

98.No response

Q46. (Respondents who assisted) Did you complain to the police?

1. Yes

2. Went to the police initially, but did not pursue the case
3. No

98.No response

Step: An answer of 'yes' in both questions were merged to form the first category. Response of 'went to the police initially, but did not pursue the case' in both questions was merged to form the second category. Response of 'No' in both questions was merged to form the third category. Similarly, "No response' answers were merged in both the questions to form the 'No response' category in the index.

Index those who complained to the police

Complained to the police	Weighted Distribution (%)
Yes	50.6
Went to the police initially, but did not pursue the case	10.8
No	34.4
No response	4.3

Index 9: Reasons for not complaining to the police

The index was constructed by taking into account two separate questions, i.e., Q21 and Q47, which are:

Q21. (victims) Why did they not complain to the police?

1. It was not a big amount
2. I felt embarrassed/ashamed
3. The police would have asked for a bribe
4. The complaint procedure is difficult/complex
5. I was/were scared to go to the police

97. Any other (Please specify): _____

98. No response/ I don't know

Q47. (Respondents who assisted) Why did they not complain to the police?

1. It was not a big amount
2. I/they felt embarrassed/ashamed
3. The police would have asked for a bribe
4. The complaint procedure is difficult/complex
5. I/they was/were scared to go to the police

97. Any other (Please specify): _____

98. No response/ I don't know

Step: Responses of 'It was not a big amount' to both questions were merged to form the first category. Responses of 'I/they felt embarrassed/ashamed' to both questions were merged to form the second category. Responses of 'The police would have asked for a bribe' to both questions were merged to form the third category. Responses of 'The complaint procedure is difficult/complex' to both questions were merged to form the fourth category. Responses of 'I/they was/were scared to go to the police' to both questions were merged to form the fifth category. Responses of 'Any other' to both questions were merged to form the sixth category. Responses of 'No response' to both questions were merged to form the last category in the index.

Index of reasons for not complaining to the police

Reasons for not complaining to the police	Weighted Distribution (%)
It was not a big amount	27.7
I felt embarrassed/ashamed	9.3
The police would have asked for a bribe	2.9
The complaint procedure is difficult/complex	13.8
I was scared to go to the police	10.4
Any other	20.7
No response	15.2

Index 10: First step after finding out about the cybercrime

The index was constructed by taking into account two separate questions, i.e., Q22 and Q48, which are:

Q22. (Victims) What was the first step you took when you found out about the cybercrime? (Do not read out the answer options)

1. Went to the local police station
2. Went to the cyber police station in my jurisdiction
3. Called the local police/cyber police station
4. Called the police helpline number for cybercrimes
5. Filed an online complaint
6. Complained to the bank

97. Any other (Please specify): _____

98. No response

Q48. (Respondents who assisted) What was the first step you took when you found out about the cybercrime? (Do not read out the answer options)

1. Went to the local police station
2. Went to the cyber police station in my jurisdiction
3. Called the local police/cyber police station
4. Called the police helpline number for cybercrimes
5. Filed an online complaint
6. Complained to the bank

97. Any other (Please specify): _____

98. No response

Step: Responses of 'Went to the local police station' to both questions were merged to form the first category. Responses of 'Went to the cyber police station in my jurisdiction' to both questions were merged to form the second category. Responses of 'Called the local police/ cyber police station' to both questions were merged to form the third category. Responses of 'Called the police helpline number for cybercrimes' to both questions were merged to form the fourth category. Responses of 'Filed an online complaint' to both questions were merged to form the fifth category. Responses of 'Complained to the bank' to both questions were merged to form the sixth category. Responses of 'Any other' to both questions were merged to form the seventh category. Responses of 'No response' to both questions were merged to form the last category in the index.

First step after finding out about the cybercrime Weighted Distribution (%)

First step after finding out about the cybercrime	Weighted Distribution (%)
Went to the local police station	50.1
Went to the cyber police station in my jurisdiction	18.0
Called the local police/cyber police station	10.0
Called the police helpline number for cybercrimes	8.8
Filed an online complaint	5.1
Complained to the bank	5.2
Any other	.4
No response	2.5

Index 11: Need to go to the police in person

The index was constructed by taking into account two separate questions, i.e., Q25 and Q51, which are:

Q25. (Victims) Did they need to go to the police station in person?

1. Yes, to the local police station
2. Yes, to the cyber police station/cell
3. Yes, to both
4. No

98. No response/ I don't know

Q25. (Respondents who assisted) Did they need to go to the police station in person?

1. Yes, to the local police station
2. Yes, to the cyber police station/cell
3. Yes, to both
4. No

98. No response/ I don't know

Step: Responses of 'Yes, to the local police station' to both questions were merged to form the first category. Responses of 'Yes, to the

cyber police station/cell' to both questions were merged to form the second category. Responses of 'Yes, to both' to both questions were merged to form the third category. Responses of 'No' to both questions were merged to form the fourth category. Responses of 'No response' to both questions were merged to form the last category in the index.

Index of need to go to the police in person

Went to these places in person	Weighted Distribution (%)
Yes, to the local police station	49.8
Yes, to the cyber police station/cell	25.6
Yes, to both	10.4
No	10.0
No response	4.2

Index 12: Person contacted to put pressure on the police

The index was constructed by taking into account two separate questions, i.e., Q32 and Q58, which are:

Q32. (Victims) Who did you contact?

1. Senior police officers
2. Senior government officials
3. Local politician
4. Local person of influence
5. Media
6. NGO
7. External agencies such as NHRC, NCW, etc.

97. Any other (Please specify): _____

98. No response

Q58. (Respondents who assisted) Who did you contact?

1. Senior police officers
2. Senior government officials
3. Local politician
4. Local person of influence
5. Media
6. NGO
7. External agencies such as NHRC, NCW, etc.

97. Any other (Please specify): _____

98. No response

Step: Responses of 'Senior police officers' to both questions were merged to form the first category. Responses of 'Senior government officials' to both questions were merged to form the second category. Responses of 'Local politician' to both questions were merged to form the third category. Responses of 'Local person of influence' to both questions were merged to form the fourth category. Responses of 'Media' to both questions were merged to form the fifth category. Responses of 'NGO' to both questions were merged to form the sixth category. Responses of 'External agencies such as NHRC, NCW, etc.' and 'Any other' to both questions were merged to form the seventh category. Responses of 'No response' to both questions were merged to form the last category in the index.

Index of person contacted to put pressure on the police

Person contacted	Weighted Distribution (%)
Senior police officers	47.4
Senior government officials	16.1
Local politician	12.8
Local person of influence	11.5
Media	5.3
NGO	.3
Any other	2.3
No response	4.3

Index 13: Contacting someone to put pressure on police

The index was constructed by taking into account two separate questions, i.e., Q31 and Q57, which are:

Q31. (Victims) Did you have to contact someone in your personal network to put pressure on the police to deal with your case properly?

1. Yes
2. No

98. No response

Q57. (Respondents who assisted) Did you have to contact someone in your personal network to put pressure on the police to deal with your case properly?

1. Yes
2. No

98. No response

Step: Responses of 'Yes' to both questions were merged to form the first category. Responses of 'No' to both questions were merged to form the second category. Responses of 'No response' to both questions were merged to form the last category in the index.

Index of whether a personal contact was used to put pressure on the police

Ask someone to put pressure on the police	Weighted Distribution (%)
Yes	26.1
No	65.9
No response	8.0

Index 14: Complained to the bank

The index was constructed by taking into account two separate questions, i.e., Q33 and Q59, which are:

Q33. (Victims) Did they complain separately to the bank?

1. Yes
2. No

98. No response

Q59. (Respondents who assisted) Did they complain separately to the bank?

1. Yes
2. No

98. No response

Step: An answer of 'yes' was merged for both questions and then merged to form the category 'yes'. Similarly, 'No' and "No response' answers were merged in both the questions to form the 'No' and 'No response' category in the index.

Index about complaining to the bank

Complained to the bank	Weighted Distribution (%)
Yes	53.1
No	41.6
No response	5.3

Index 15: Case went to the Court

The index was constructed by taking into account two separate questions, i.e., Q36 and Q62, which are:

Q36. (Victims) Did their case go to court?

1. Yes
2. No

98. No response

Q62. (Respondents who assisted) Did their case go to court?

1. Yes
2. No

98. No response

Step: An answer of 'yes' was merged for both questions and then merged to form the category 'yes'. Similarly, 'No' and "No response' answers were merged in both the questions to form the 'No' and 'No response' category in the index.

Index of cases going to the court

Cases went to court	Weighted Distribution (%)
Yes	22.5
No	70.5
No response	7.0

Index 16: Data leak by bank insider

The index was constructed by taking into account two separate questions, i.e., Q43 and Q69, which are:

Q43. (victims) Some victims of financial cybercrimes believe that their financial data was leaked by a bank insider because of which they were targeted by criminals. In your case, do you think the crime occurred due to a breach of your personal data by the bank or its personnel?

1. Yes, it occurred due to a breach of personal data
2. No, it didn't happen because of that

98. Don't know

Q69. (Respondents who assisted) Some victims of financial cybercrimes believe that their financial data was leaked by a bank insider because of which they were targeted by criminals. In your case, do you think the crime occurred due to a breach of your personal data by the bank or its personnel?

1. Yes, it occurred due to a breach of personal data
2. No, it didn't happen because of that

98. Don't know

Step: Responses of 'Yes, it occurred due to breach of personal data' to both questions were merged to form the first category. Responses of 'No, it did not happen because of that' to both questions were merged to form the second category. Responses of 'No response' to both questions were merged to form the last category in the index.

Index of data leak by bank insider

	Weighted Distribution (%)
Yes, cybercrime occurred due to a breach of personal data	31.1
No, it didn't happen because of that	44.6
Don't know	24.3

Index 17: Satisfaction with police handling of cybercrime

The index was constructed by taking into account four sub-questions of Q42, which are:

Q42. How satisfied were you with the following – very satisfied, somewhat satisfied, somewhat dissatisfied, or very dissatisfied?

a. Police helpline number for cyber complaints
b. Online police portal for cyber crimes
c. The complaint registration process at the cyber police station
d. The investigation of cybercrimes by the police

In each sub-question, the response offered to the respondents was:

- Very satisfied
- Somewhat satisfied
- Somewhat dissatisfied
- Very dissatisfied
- Never used this service (silent option)
- No response

Step 1: An answer that was 'very satisfied' was assigned the value of 4. An answer that was 'somewhat satisfied' was assigned the score of 3. An answer that was 'somewhat unsatisfied' was assigned the score of 2. The answer 'very unsatisfied' was assigned the score of 1, and 'No response' and 'Never used this service' to the sub-questions were assigned a score of 0.

Step 2: The scores of all five sub-questions were summed up. The result, summated scores range from 0 to 16.

Step 3: The summated scores were distributed across four newly created categories that indicated overall satisfaction with the police's handling of cybercrime. Summated scores that ranged from 14 to 16 were categorised as very satisfied. Summated scores that ranged from 9 to 13 were categorised as somewhat satisfied. Summated scores ranging from 5 to 8 were categorised as somewhat unsatisfied, and summated scores that totalled 1 to 4 were categorised as very unsatisfied. The non-responses and 'never used this service' were set as missing.

Index of satisfaction with police's handling of cybercrime

	Summated scores	Weighted distribution (%)
Very satisfied	1-4	17.4
Somewhat satisfied	5-8	19.4
Somewhat dissatisfied	9-13	42.1
Very dissatisfied	14-16	21.1

Index 18: Time of fraud reporting

The index was constructed by taking into account two separate questions, i.e., Q34 and Q60, which are:

Q34. (Victims) How soon after the fraud did you report it?

1. Within 24 hours
2. Within 48 hours
3. More than 48 hours

98. No response

Q60. (Respondents who assisted) How soon after the fraud did you report it?

1. Within 24 hours
2. Within 48 hours
3. More than 48 hours

98. No response

Step: Responses of 'Within 24 hours' to both questions were merged to form the first category. Responses of 'Within 48 hours' to both questions were merged to form the second category. Responses of 'More than 48 hours' to both questions were merged to form the second category. Responses of 'No response' to both questions were merged to form the last category in the index.

Index about time of fraud reporting

Time of fraud reporting	Weighted Distribution (%)
Within 24 hours	62.6
Within 48 hours	21.2
More than 48 hours	11.0
No response	5.2

Index 19: Freezing accounts

The index was constructed by taking into account two separate questions, i.e., Q35 and Q61, which are:

Q35. (Victims) Did the bank take any action such as freezing all your accounts, etc. after receiving the complaint?

1. Yes, completely
2. Yes, partially
3. No

98. No response

Q61. (Respondents who assisted) Did the bank take any action such as freezing all your accounts, etc. after receiving the complaint?

1. Yes, completely
2. Yes, partially
3. No

98. No response

Step: Responses of 'Yes, completely' to both questions were merged to form the first category. Responses of 'Yes, partially' to both questions were merged to form the second category. Responses of 'No' to both questions were merged to form the third category. Responses of 'No response' to both questions were merged to form the last category in the index.

Index of freezing accounts by the bank

Account frozen by the bank	Weighted Distribution (%)
Yes, completely	47.1
Yes, partially	26.8
No	18.6
No response	7.6

Index 20: Lost money recovery

The index was constructed by taking into account two separate questions, i.e., Q39 and Q65, which are:

Q39. (victims) Were you able to recover your lost money?

1. Yes, the whole amount
2. Yes, partial amount
3. No

98. No response

Q65. (Respondents who assisted) Were you able to recover your lost money?

1. Yes, the whole amount

2. Yes, partial amount

3. No

98. No response

Step: Responses of 'Yes, the whole amount' to both questions were merged to form the first category. Responses of 'Yes, partial amount ' to both questions were merged to form the second category. Responses of 'No' to both questions were merged to form the third category. Responses of 'No response' to both questions were merged to form the last category in the index.

Index about the recovery of lost money

Amount recovered	Weighted Distribution (%)
Yes, the whole amount	10.4
Yes, partial amount	7.4
No	71.6
No response	10.6

Index 21: Time of fraud recovery

The index was constructed by taking into account two separate questions, i.e., Q40 and Q66, which are:

Q40. How long after the cyber fraud did you recover the money? _____ (in days)

98. No response

Q66. How long after the cyber fraud did you recover the money? _____ (in days)

98. No response

Step: Responses of 'Up to 15 days' to both questions were merged to form the first category. Responses of '16 to 30 days' to both questions were merged to form the second category. Responses of '31 to 60 days' to both questions were merged to form the third category. Responses of '61 to 90 days' to both questions were merged to form the fourth category. Responses of 'No response' to both questions were merged to form the last category in the index.

Index about the time of fraud money recovery

Time taken to recover the money	Weighted Distribution (%)
Upto 15 days	32.2
16 days to a month	17.2
1 month to 2 months	24.1
More than 2 months	9.8
No response	16.7

Index 22: Level of satisfaction with bank's role in recovering money

The index was constructed by taking into account two separate sub question of two different questions, i.e., Q42 (f) and Q68 (f), which are:

Q42. (victims) How satisfied were you with the following – very satisfied, somewhat satisfied, somewhat dissatisfied, or very dissatisfied?

f. The bank's role in recovering the money

Q68. (Respondents who assisted) How satisfied were you with the following – very satisfied, somewhat satisfied, somewhat dissatisfied, or very dissatisfied?

f. The bank's role in recovering the money

In each sub-question, the response offered to the respondents was:

- Very satisfied
- Somewhat satisfied
- Somewhat dissatisfied
- Very dissatisfied
- Never used this service (silent option)
- No response

Step: Responses of 'Very satisfied' to both questions were merged to form the first category. Responses of 'Somewhat satisfied' to both questions were merged to form the second category. Responses of 'Somewhat dissatisfied' to both questions were merged to form the third category. Responses of 'Very dissatisfied' to both questions were merged to form the fourth category.

Responses of 'Never used this service' to both questions were merged to form the fifth category. Responses of 'No response' to both questions were merged to form the last category in the index.

Index about satisfaction with bank's role in recovering money

Level of satisfaction	Weighted Distribution (%)
Very satisfied	10.7
Somewhat satisfied	21.3
Somewhat dissatisfied	16.2
Very dissatisfied	22.1
Never used this service (silent option)	23.8
No response	5.8

Index 23: Level of satisfaction with RBI banking Lokpal

The index was constructed by taking into account two separate sub-questions of two different questions, i.e., Q42 (g) and Q68 (g), which are:

Q42. (victims) How satisfied were you with the following – very satisfied, somewhat satisfied, somewhat dissatisfied, or very dissatisfied?

f. The RBI Banking Lokpal

Q68. (Respondents who assisted) How satisfied were you with the following – very satisfied, somewhat satisfied, somewhat dissatisfied, or very dissatisfied?

f. The RBI Banking Lokpal

Step: Responses of 'Very satisfied' to both questions were merged to form the first category. Responses of 'Somewhat satisfied' to both questions were merged to form the second category. Responses of 'Somewhat dissatisfied' to both questions were merged to form the third category. Responses of 'Very dissatisfied' to both questions were merged to form the fourth category.

Responses of 'Never used this service' to both questions were merged to form the fifth category. Responses of 'No response' to both questions were merged to form the last category in the index.

Index about satisfaction with RBI Banking Lokpal

Level of satisfaction	Weighted Distribution (%)
Very satisfied	8.7
Somewhat satisfied	17.7
Somewhat dissatisfied	10.6
Very dissatisfied	8.6
Never used this service (silent option)	46.4
No response	8.1

APPENDIX 4: Qualitative Tools Methodology

The qualitative component of this study aimed to capture in-depth: the lived experiences, institutional interactions, and perceptions of those who navigate India's cybercrime redressal system as both victims and professionals. Semi-structured in-depth interviews (IDIs), a focus group discussion (FGD), and visits to a cybercrime cell and court were used to draw out detailed, first-person accounts of engagement with the police, banks, courts, and social media platforms, alongside expert perspectives on systemic gaps and possible reforms. A total of 37 respondents were interviewed through one-on-one interviews and a focus group discussion (FGD). The findings are presented in Chapters 1 & 2 of this study.

A detailed methodology of the qualitative interviews and FGD is given here.

Types of Victims and Experts

The total number of In-depth Interview and FGD respondents is given in Table 1 below, disaggregated by the category of respondents:

Table 1: Types of Respondents

Category of Respondents	Number of Respondents
Victims of cybercrimes	16
Family members of victims of cybercrimes	2
Domain experts	15
Family members of accused persons in cybercrime cases	2
Persons whose bank accounts were frozen due to cybercrime investigations	2
Total	**37**

The break-down of the cybercrime victims who were interviewed, by the type of cybercrime faced by them, is given below:

Table 2: Number of Cybercrime victims

Type of Cybercrime	Number of Victims
Digital financial frauds	
Digital Arrest	3
Sextortion	1
Other types of financial frauds	9
Other types of cybercrimes	
Hacking	1
Online gender-based violence (bullying/harassment)	2
Total	**16**

The respective background profiles of all of the domain-experts who were interviewed, both through In-depth Interview method as well as those participated in the Focused Group Discussion, is given in Table 3.

Table 3: Profile of Experts

Field of Expertise	Background Information	Number of Experts
Cyberbullying	A psychologist and founder of an anti-cyberbullying organisation that aids victims of online bullying and harassment with both psychological and legal support.	1
Online-gender based violence	Through their organisation they aid victims of non-consensual intimate image abuse by helping them take down the content from online platforms, and coordinating with the police to report and resolve their cases.	3
	Through their organisation they aid victims of non-consensual intimate image abuse by helping them take down the content from online platforms, and coordinating with the police to report and resolve their cases.	
	Researcher and policy advocate on issues related to social media regulation, algorithmic implications, and online gender-based violence.	
Cyber policing	A retired IPS officer, with tenures as head of cyber security and fraud prevention in the public sector and banks respectively.	5
	A retired IPS officer and renowned as one of India's leading cybersecurity experts. Lead major State projects on cybersecurity infrastructure for the police.	
	Investigating officer at a cybercrime cell in Delhi	
	A senior IPS officer working in the government's cybercrime and artificial intelligence division	
	One of India's leading national security and cybercrime experts who investigates complex high-profile cybercrime cases, trains police officers on the evolving nature of cybercrime, and works closely with all of India's law enforcement and intelligence bodies.	
Digital Rights	Well-renowned advocate, author, and founder of a digital rights organisation.	4
	Lawyer and global cybersecurity lead of a digital rights organisation.	
	Head of regional policy and advocacy on digital rights & governance, and technology policy.	
	Researcher working on issues of artificial intelligence, digital rights, and online gendered experiences.	
Banking	Career banker and retired fraud investigator from a major private bank.	1
Journalist	Experienced field journalist covering issues of cybercrime and cybercriminals.	1
Total		**15**

Table 4: Mode of Interview of Experts

Type of Qualitative Research Tool Used	Number of Participants/Respondents
In-depth Interviews	10
Focused Group Discussion	5
Total number of domain experts interviewed	**15**

Sampling and mode of interviews

The participants for the interviews and focus group discussion were sampled using the following methods:

- Focus Group Discussion: Experts were purposively sampled.
- Victims and those who assisted them:
  - > Publicly circulated Google form that was shared on Common Cause's social media handles (Instagram, Facebook, LinkedIn, and X), its website and on WhatsApp.
  - > Snowball sampling.
  - > Visits to a cybercrime police station and cybercrime court in Delhi
- The family members of accused persons were interviewed at the cybercrime court.
- One person whose bank account was frozen due to an ongoing cybercrime investigation was interviewed outside a cybercrime cell in Delhi

One-on-one interviews were conducted primarily online via Zoom, between November 2025 and February 2026. In-person interviews were conducted with two family members of accused persons and one victim at a cybercrime court. One expert (investigating officer) was interviewed in-person at a cybercrime cell. Prior consent was obtained from all interviewees for their participation in the study. All interviews were recorded with participants' consent, except one involving a family member who had helped a victim and declined recording.

Interview Guides and Analysis

Multiple interview guides were used, tailored to the type of cybercrime experienced (for victims) and the expert's field of work (Refer to Appendix 5 for interview guides). Interviews with victims were focused on the nature and circumstances of cybercrime; their interactions and experience of redressal with institutional actors – namely the police, banks, courts, and social media platforms; their perceptions and satisfaction with these actors; and the psycho-social and financial impact of the crime. Interviews with the experts focused on the broader landscape of cybercrime, their experiences working with victims and the support extended to them, their engagement with other institutional actors, their perceptions of the overall redressal system, and recommendations for reform. All the interviews, including the FGD were transcribed and underwent a rigorous quality check before being coded and analysed in ATLAS.ti.

ATLAS.ti was used to code the transcripts and specific codes were assigned under different thematic areas to identify patterns across both victims' experiences and experts' perspectives. The codes were then further grouped into broader themes that allowed specific analyses of different aspects of cybercrimes and respondent experiences. Each type of cybercrime experienced by the victims were also analysed separately as one category to identify similarities within the same category of cybercrime.

The systematic coding and analysis procedure allowed the research team to frame the findings, and throughout the analysis stage the team was able to constantly review and cross-check codes and quotations for consistency and accuracy.

APPENDIX 5: Qualitative Interview Guides

The introductory section and questions on demographic details of respondents are common across all interview guides.

Introduction

I am XXX from Common Cause. We have been conducting studies on policing aimed towards systemic reforms under a series of reports titled the Status of Policing in India Reports. In the current issue of SPIR, we are focusing on cybercrimes in India and the preparedness of the police and other agencies to deal with such cases.

Through this research, we aim to understand people's experiences with cybercrime and the processes of complaint and redressal, to identify what works well and what challenges/gaps exist in the current system.

As part of this study, we would like to interview you about your experience of cybercrime and your interactions with relevant authorities. This interview will take about 40–50 minutes. Participation is entirely voluntary, and you may choose to skip any question you feel uncomfortable answering.

We would also like to ask your permission to record this conversation. This recording will only be used for our internal purposes of transcription and analysis. All personally identifiable information that you give will be kept anonymous and confidential. If there is any part of the interview that you would prefer to keep off the record, please let us know.

Z. Demographic Details

1. Name (only if you are comfortable with sharing your name. It will not be used for reporting or analysis at any stage):
2. Age:
3. Gender:
4. Profession (optional)
5. Where did the crime occur (city/town/village and state)?
6. When did the incident occur?
7. Which language will you be comfortable in?

INTERVIEW GUIDE 1: FOR VICTIMS OF FINANCIAL CYBERCRIMES

I. Crime details

1. Can you tell me a little bit about what type of crime you faced?
2. Can you describe the incident?

a. How did the fraudster contact you?

b. Did you notice any warning signs or suspicious behaviour before or during the transaction?

c. How do you think the fraudster got access to your account/data? (OTP/password/link etc.)

d. Which platform or medium was used for the fraud?

3. When did you find out that it was a fraud? / How soon after the crime did you find out about the fraud?
4. How much money was lost due to the fraud?

II. Reporting and Registration: Police

1. What was the first thing that you did when you found out?
2. How soon after finding out about the fraud did you approach the police?
3. Did you know which authority to contact when you found out about the fraud?
4. How did you first complain to the police – helpline, online portal, physical visit or any other way?
5. Did you face any difficulty in using the online reporting portal (if used) or understanding its language?
6. Registration
7. Did the police register a complaint immediately? If no, why not? How long did it take?
8. Did you face any other problems in the complaint's registration process?
9. Were you given a complaint or FIR number?
10. What information/details did the police ask for?
11. Did the police or the cyber cell take any immediate action, such as tracing the transaction?
12. Did you have to pay a bribe or make any other payment?
13. How many times did you have to visit the police?
14. After the complaint was registered, did you get any updates from the police on your case proactively?
15. How did you feel the police handled your case? What do you think the police could've done better here?
16. Do you think cybercrime units or specialised police cells are effective?
17. Do you think the police have the capacity to deal with cases of cybercrimes?

III. Reporting: Banks

1. Did you approach the bank? If so, when? How easy or difficult was it to approach the bank? How did you contact the bank?
2. What was the response that you got from the bank?
3. Did they explain the grievance redressal process or timelines?
4. What did they do with your transaction (e.g., freeze it, inform the recipient's bank, cancel it, etc.)
5. To your knowledge, did the banks coordinate with the police to investigate and/or resolve your case?
6. How long did it take to receive a response or closure from the bank? (How frequently did you have to check in with your bank? Did you get regular updates on your case)
7. Do you think the bank staff was helpful in dealing with your case?

8. Do you think the banks have the capacity to deal with cases of cybercrimes?
9. Did you need to reach out to the banking ombudsman? If yes, how did you do so? what was the response that you received from the ombudsman?

IV. Reporting/resolution: Court

1. Did your case reach the court or did you have to approach any court officer at any point during the case?

a. If your case did not reach court, could you tell us why (e.g., lack of follow-up, high cost, small amount, etc.)?

2. Which court was your case taken to? was the case handled by a special cyber court or regular court?
3. What was the process in the court?
4. What documents/evidence did you have to submit to the court? (optional)
5. How long was your case in the court? How many times did you have to visit?
6. Did you have to engage a lawyer? Was it a private lawyer or a government lawyer?
7. Did the case reach any resolution in the court? If yes, please give details-
    a. Did you get any of the money back? How much?
    b. Was any person arrested or convicted?
    c. Any other resolution?
8. If the case is still ongoing, what stage is it at now?
9. Roughly how much did you have to spend in the legal process?
10. Do you think the courts have the capacity to deal with cases of cybercrimes?

V. Other experiences

1. In your opinion, what could have made it easier to report your case?
2. Did you have to approach someone to put pressure on the agencies to look into your case? You don't have to tell us their name, just their profession, such as if it was a local politician, a police officer, some other government official, media, NGO, or any other? Do you think their intervention helped?
3. Do you think your personal details were leaked by any person or agency because of which you were targeted for this crime? If yes, then who do you think leaked it?
4. Do you think the crime and the subsequent complaints process impacted you professionally, emotionally or socially? If so, can you please describe how?
5. Did you suffer from any further financial loss because of this crime and the case?
6. Did you seek any legal or financial help due to the case?

VI. Systemic preparedness, trust and satisfaction

1. Overall, were you satisfied with your experience with the:
    a. Police
    b. Banks
    c. Courts
2. How do you think the systems can be improved to:

a. Prevent such cases of cybercrimes

b. Ensure better response to complaints of cybercrimes

3. What kind of training or resources do you think police and banks need to handle such crimes better?
4. What changes would you recommend in government policy or law to make cybercrime redressal more effective?
5. Do you think telecom companies, fintech apps like PayTM, or social media platforms should play a bigger role in prevention or resolution? (optional)
6. What kind of awareness campaigns or public education could have helped you avoid the fraud?
7. ls there anything else you'd like to share about your experience that we haven't discussed?

INTERVIEW GUIDE 2: FOR VICTIMS OF CYBERBULLYING

I. Crime details

1. Can you tell me a little bit about what happened? When did the incident occur?
2. What type of cyber harassment or abuse did you face? (e.g., online stalking, threatening, morphing, deepfakes, unsolicited sexual images, blackmail, revenge porn, obscene comments or gestures, etc.)
3. Could you describe the incident(s) in as much detail as you are comfortable sharing? For how long did it last?
4. Was the perpetrator one person, multiple people or unknown? How did the perpetrator contact you? Did you know this person?
5. Which apps/ social media platforms were involved? (e.g., social media, messaging apps, email, dating platforms, video calls, etc.
6. Were there any warning signs or earlier interactions that made you uncomfortable before the incident escalated?
7. If photos or videos were shared or morphed, how do you think the perpetrator got access to your images or personal data?
8. Did you receive any threats, attempts to blackmail, or demands (e.g., for money, sexual favours, silence, etc.)?
9. What was the first thing you did after realising you were being harassed or your content was misused?
10. Did you discuss it with anyone (family, friends, colleague, NGO, lawyer)?

II. Reporting and Registration: Police or other agencies

1. Did you complain to the police or any other similar agency/helpline, etc.?

1A. Any reason for not approaching the police?

2. How soon after the incident did you approach the police or any official body?
3. How did you file the complaint? (Through the Cyber Crime Reporting Portal (cybercrime.gov.in), a helpline number, a visit to a police station, or through someone else)
4. If you used the online portal, did you face any difficulty in understanding or navigating it?
5. Did the police register your complaint immediately? If not, why? How long did it take?
6. Were you given a Complaint Number or FIR Number?
7. What kind of information or evidence did the police ask for? (e.g., screenshots, URLs, chat records, etc.)
8. Did the police take any immediate action, such as contacting the platform, tracing the offender?
9. Did you face any problems during the complaint process? Did the police believe your complaint? Were they sensitive in dealing with your case?
10. Did you have to visit the police station or cyber cell multiple times? If yes, how many times?
11. Did any police officer demand payment or a bribe at any stage?
12. After registration, did you get any updates on your case proactively?
13. Did you face pressures to "settle" the case from anyone?
14. How do you feel the police handled your case overall?
15. Do you think the police have the training and sensitivity to handle cases of cyber sexual harassment?
16. Were there any female officers or cybercrime specialists available during the process?
17. What could the police have done better in your case?

III. Reporting and Coordination: Platforms / Social Media Companies

1. Did you report the incident to the platform or service provider (e.g., Facebook, Instagram, WhatsApp, X/Twitter, etc.)?

2. How easy or difficult was it to locate the reporting option?
3. How did the platform respond? How long did the platform take to respond?
4. Did they take down the post, suspend the account, or ask for more proof? (Or was there no resolution from their side?)
5. Did the platform share any updates or reasons for their action/inaction?
6. Did the police coordinate with the platform to remove the content or trace the perpetrator/ harasser?
7. Were you satisfied with the platform's response? Why or why not?
8. Do you think social media companies should be doing more to protect users from sexual harassment and non-consensual content?

IV. Reporting/Resolution: Legal and Court Process

1. Did your case reach the court or involve any legal proceedings?

a. Any reason for not approaching the court (lack of follow-up, cost, emotional exhaustion, fear, stigma, etc.)?

2. Did you engage a lawyer? Was it a private lawyer or a government legal aid lawyer?
3. How was your experience with the legal process — documentation, hearings, interactions with lawyers or judges?
4. Is the case still ongoing? If yes, since when has the matter been pending in court? If not, how long did the case take?
5. Was any person fined, arrested, summoned, or convicted in your case?
6. Were any steps taken to remove or block harmful online content during the case?
7. Roughly how much did you have to spend on the legal process?
8. Do you think courts are adequately equipped and sensitive to handle gender-based online crimes?

V. Other Experiences and Impacts

1. Did you have to reach out to anyone (NGO, lawyer, media, local politician, social worker), influential or in authority, for support or intervention? Did their involvement help?
2. Did you experience any backlash, threats, or online trolling after reporting? Were you blamed by any person or authority for the incident or for filing the complaint?
3. Do you believe any of your personal information (phone number, house address) was leaked by any agency, platform, or individual, leading to the incident or after?
4. How did the incident and its aftermath affect you mentally, emotionally, socially, professionally, or financially? (Probe separately for the crime and the complaint process)

4A. (Probe if they say something related) Did you experience any long-term mental health issues?

4B. Did you seek counselling? If yes, how easy or difficult was it to access these services? What helped you cope during or after the incident?

5. Do you feel that your caste/ gender/religious identity or social background influenced the nature of the incident or how your case was handled?
6. After the incident, did you feel safe using the internet or social media again?

VI. Systemic Preparedness, Trust, and Satisfaction

1. What was your experience of the overall resolution of your case? Did the agencies/ authorities involved support you through the process? (Probe separately for police/ courts etc.)
2. What could have made it easier to report and resolve your case?
3. Do you think cybercrime units and specialised police cells for women are sensitive and effective?
4. Is there anything else you'd like to share about your experience that we haven't discussed? Any other thoughts or suggestions.

INTERVIEW GUIDE 3: FOR DIGITAL ARREST VICTIMS

I. Crime Details

1. When did the incident occur? For how long were you under a "digital arrest"?
2. Can you describe the incident?
    a. How did the fraudster initially contact you?
    b. Did they ask you to do something or give any information?
    c. Who was the fraudster impersonating?
    d. How many people were on the call?
3. Were you accused of any crime? (If yes) What were they?
4. At that time, what were some signs that made you believe that the fraudster was a legitimate authority?

a. Were you shown any evidence, documents, videos or anything of that nature that made you believe that the person contacting you was indeed from a legitimate authority?

5. What did the fraudster threaten you with? (E.g., legal action, jail, enormous fine, violence towards family members, kidnapping, etc.)
6. Were you asked to not contact anybody about this, such as a lawyer, family member, police, etc. while the scam was taking place?
    a. Did you comply?
7. Were you asked to keep your video on at all times or be available at all times?
8. What were the actions or demands that were made by the fraudster? How much money did they ask for, and was it all demanded at once or in different stages?
    a. What did they say the money was for?
    b. How did you respond to each demand?
9. How do you think that the fraudster was able to collect your personal details?
10. When did you realise that you were being defrauded? What did you do right after?
11. Would you like to share anything else about the incident, before we move onto your experience with the police/banks, etc.?

II. Reporting and Registration: Police

1. How soon after finding out about the fraud did you approach the police?
2. Did you know which authority to contact when you found out about the fraud?
3. How did you first complain to the police- helpline, online portal, physical visit or any other way?
4. Did you face any difficulty in using the online reporting portal (if used) or understanding its language?
5. Registration:

a. Did the police register a complaint immediately? If no, why not? How long did it take?

b. Did you face any other problems in the complaints registration process?

c. Were you given a complaint or FIR number?

d. What information/details did the police ask for?

6. Did the police or the cyber cell take any immediate action, such as tracing the transaction?
7. Did you have to pay a bribe or make any other payment?
8. How many times did you have to visit the police?
9. After the complaint was registered, did you get any updates from the police on your case proactively?
10. How do you feel the police handled your case? What do you think the police could've done better here?
11. Do you think cybercrime units or specialized police cells are effective?
12. Do you think the police have the capacity to deal with cases of cybercrimes?

III. Reporting: Banks

1. Did you approach the bank? If so, when? How easy or difficult was it to approach the bank? How did you contact the bank?
2. What was the response that you got from the bank?
3. Did they explain the grievance redressal process or timelines?
4. What did they do with your transaction (e.g., freeze it, inform the recipient's bank, cancel it, etc.)
5. To your knowledge, did the banks coordinate with the police to investigate and/or resolve your case?
6. How long did it take to receive a response or closure from the bank? (How frequently did you have to check in with your bank? Did you get regular updates on your case)
7. Do you think the bank staff was helpful in dealing with your case?
8. Do you think the banks have the capacity to deal with cases of cybercrimes?
9. Did you need to reach out to the banking ombudsman? If yes, how did you do so? what was the response that you received from the ombudsman?

IV. Reporting/resolution: Court

1. Did your case reach the court or did you have to approach any court officer at any point during the case?

a. If your case did not reach court, could you tell us why (e.g., lack of follow-up, high cost, small amount, etc.)?

2. Which court was your case taken to? was the case handled by a special cyber court or regular court?
3. What was the process in the court?
4. What documents/evidence did you have to submit to the court? (optional)
5. How long was your case in the court? How many times did you have to visit?
6. Did you have to engage a lawyer? Was it a private lawyer or a government lawyer?
7. Did the case reach any resolution in the court? If yes, please give details-
   d. Did you get any of the money back? How much?
   e. Was any person arrested or convicted?
   f. Any other resolution?
8. If the case is still ongoing, what stage is it at now?
9. Roughly how much did you have to spend in the legal process?
10. Do you think the courts have the capacity to deal with cases of cybercrimes?

V. Other experiences

1. In your opinion, what could have made it easier to report your case?
2. Did you have to approach someone to put pressure on the agencies to look into your case? You don't have to tell us their name, just their profession, such as if it was a local politician, a police officer, some other government official, media, NGO, or any other? Do you think their intervention helped?
3. Do you think your personal details were leaked by any person or agency because of which you were targeted for this crime? If yes, then who do you think leaked it?
4. Do you think the crime and the subsequent complaints process impacted you professionally, emotionally or socially? If so, can you please describe how?
5. Did you suffer from any further financial loss because of this crime and the case?
6. Did you seek any legal or financial help due to the case?

VI. Systemic preparedness, trust and satisfaction

1. Overall, were you satisfied with your experience with the:
   a. Police
   b. Banks
   c. Courts

2. How do you think the systems can be improved to:

a. Prevent such cases of cybercrimes

b. Ensure better response to complaints of cybercrimes

3. What kind of training or resources do you think police and banks need to handle such crimes better?

4. What changes would you recommend in government policy or law to make cybercrime redressal more effective?

5. Do you think telecom companies, fintech apps like PayTM, or social media platforms should play a bigger role in prevention or resolution? (optional)

6. What kind of awareness campaigns or public education could have helped you avoid the fraud?

7. ls there anything else you'd like to share about your experience that we haven't discussed?

INTERVIEW GUIDE 4: FOR VICTIMS OF HACKING/PHISHING

I. Crime Details

1. Can you describe the incident?

a. Were you contacted by anybody?

b. How do you think the fraudster got access to your account/data?

2. When did you find out that your account was hacked/ How soon after the crime did you find it?

3. Did you lose any money because of the hack?

4. Was your account used to send messages to your contacts? What kind of message was it?

5. Were you able to identify any specific group, individual or location involved in the crime?

II. Response

1. What steps did you take once you realised what had happened?

2. Did you know who to contact after finding out about the hack?

a. Did you face any difficulty in finding who to contact?

3. Did you contact the support team or a helpline of the platform your account was on?

a. What response did you get from them?

b. How helpful were they in resolving the issue or recovering your account?

4. Did you report the case to the police/ national cybercrime portal/helpline?

III. Emotional and Psychological Impact

1. How did you feel when you realised you have been scammed or hacked?

2. Did the experience cause any type of harm – financial, reputational, social, mental.

3. Has it changed how you use online platforms [such as the service that was hacked]?

4. Did the incident affect your day-to-day life outside the internet?

IV. Other Experiences

1. What could have made it easier to report the hack?

2. Do you think there is any specific reason you were targeted for the hack?

3. Did you seek any legal help due to the hack?

V. Systemic Preparedness, Trust, and Satisfaction

1. What do you think the platform/police/ banks or the government could have done better?

2. How satisfied for you with the platform's response to your case? Can you rate them on a scale of 1 to 5. 5 being fully satisfied and 1 being the least satisfied.

3. Is there anything else about your experience you would like to share?

INTERVIEW GUIDE 5: FOR EXPERTS OF CYBER BULLYING & ABUSE

I. Background Information & Scope of Work

1. Could you please tell us a bit about yourself?
2. When and how was [expert's organisation] founded?
3. Can you describe the main interventions your organisation undertakes to promote cyber safety and responsible online behaviour? (Probe: awareness campaigns, workshops, counselling, partnerships, digital literacy modules, etc.)

3.1. Who are your primary target groups? (for example, children, women, schools, law enforcement, or other stakeholders)

4. How does your organisation engage with victims of cyberbullying, cyberstalking, or online harassment?
5. Do you provide direct support or referrals to law enforcement, legal, or psychological services?
6. Have you observed any patterns or trends in the types of cybercrimes or online harms being reported to you? (for example, by age group, gender, or platform)
7. Based on your experience, what are the most common forms of cybercrime or online abuse that your team encounters today?
8. What new threats or challenges have emerged recently (e.g., AI-generated deepfakes, doxxing, sextortion, misinformation)?

II. Police and Redressal Mechanisms

1. Have you collaborated with police, government authorities, or any other agencies (e.g., through training or awareness programs)? If yes, could you describe that collaboration?
2. In your opinion, what gaps exist in how police or other agencies respond to cybercrime complaints?
3. What kinds of training or institutional support do you think police personnel need to respond effectively and sensitively to victims, especially minors and women?
4. How well are mechanisms like the National Cyber Crime Reporting Portal functioning in practice?
5. Are there differences in responses between urban and rural areas or between states?

III. Victim Experience and Psychological Support

1. What challenges do victims commonly face when reporting online abuse or cybercrime? (Probe: awareness, stigma, fear, police insensitivity, technical barriers, delays, etc.)
2. How does [expert's organisation] support victims emotionally or practically through these processes?
3. Are there enough accessible psychosocial support structures (e.g., counsellors, online safety educators) available in India?
4. What role do schools, parents, and social media platforms play in prevention and redressal?

IV. Social Media Platforms

1. How responsive do you find social media companies and platforms in addressing user complaints related to harassment or bullying?
2. Are reporting mechanisms on these platforms accessible, transparent, and effective?
3. What improvements or accountability measures would you recommend for tech companies to ensure safer online spaces?

V. Policy, Legal Framework, and Systemic Reforms

1. Do you think there are legal or procedural gaps that make redressal difficult for victims?
2. What kinds of policing reforms would you recommend to improve cybercrime investigation, victim protection, and awareness?
3. How can people be empowered to handle online risks more effectively?
4. If you could recommend any priority actions for policymakers to strengthen India's cyber safety framework, what would they be?
5. Is there anything else you would like to add that we haven't covered?

INTERVIEW GUIDE 6: FOR BANKERS DEALING WITH FINANCIAL CYBERCRIME

I. Scope and Signs to look out for

1. What is the overall scope of grievances that you usually receive?
2. What suspicious behaviour or warning signs should one look out for to prevent falling for such online scams?
3. If a customer is defrauded of money and/or access to their bank account, what steps would you recommend they take?
4. How do online scammers gain access to the personal information of their victims?
5. What tools do you and concerned authorities use to tend to the grievances of victims?

II. Security and Common Mistakes

1. What steps does the Bank usually take to ensure the security of the funds of its account holders?
2. What common mistakes of account holders do you come across that make them more susceptible to Financial Cybercrimes?
3. What steps do you and your department take when a complaint is registered and verified?
4. Do you often stay in contact with Law enforcement? If you could describe your experience of working with them.
5. In your experience, is law enforcement proactive enough when it comes to tackling cybercrimes?
6. Do you feel law enforcement and banks are more preoccupied with large-scale operations to the point that individual grievances are moved to the back burner?
7. Do you feel that current cybercrime units, both of the Police and Banks, are efficient and equipped enough to deal with the diversifying forms of Cybercrimes?

III. Legal Compliance and Courts

1. Do you work with other internal teams of the bank, such as legal, fraud detection, etc?
2. Do you also coordinate/have coordinated with Courts of any level in the past? If you could elaborate on your experience of working with said Courts.
3. During your experience, what documents or processes did the Courts require to reach a suitable decision?
4. During your experience, how much time did the Courts require to provide a remedy to the aggrieved party?
5. In your experience, how difficult is it for an account holder with no significant connections to deal with and get suitable responses from law enforcement and the Courts?
6. Do you feel that the current legal framework and IT laws are equipped enough to deal with growing cybercrime?

IV. Technical Specifics and Awareness

1. There has been a growing concern around Mule accounts - or people who rent their bank accounts for quick cash. Have you ever dealt with such cases? If yes, please elaborate regarding your experience.
2. How would you describe the growing danger of P2P and crypto trading being used for illegal transactions? How better can relevant authorities equip themselves to deal with this problem?
3. Regarding the number of fake digital arrests, what steps can an account holder take as preventive measures and if they are under surveillance of such scammers?
4. How important do you feel fraud detection is when it comes to tackling Financial Cybercrimes?
5. What steps can Banks and other relevant authorities take to raise awareness regarding financial cybercrimes and how to steer clear of online scammers?

V. Suggestions and Remarks

1. What suggestions would you want to give to central authorities like the RBI or the Ministry of Finance to deal with Cybercrimes?

2. What systematic changes need to be made to safeguard vulnerable sections, such as Senior Citizens, Handicapped people, etc., who often have disproportionate access to law enforcement and other remedial means?
3. What structural changes need to be made in Banks and other relevant authorities to ensure quicker, more fruitful investigations concerning cybercrime that remedy the aggrieved party?
4. Any suggestions and problems that you have noticed with the increased use of third-party UPI apps?
5. Any suggestions on how the relevant authorities can increase outreach and create better awareness when it comes to financial cybercrimes?
6. Any concluding remarks or further suggestions that haven't been discussed in the interview that you would like to share with us?

INTERVIEW GUIDE 7: FOR POLICING EXPERTS

1. What are the most prevalent forms of cybercrimes, apart from financial frauds and scams?
    a. (Probe on other mentioned cybercrimes)
    b. What is the biggest concern regarding cybercrimes these days?
2. Can physical visits to banks for transactions work as a precaution against financial cybercrimes?
3. As an insider in the police service, do you think a large proportion of cybercrime cases are converted to FIRs?
    a. Would the police then have the capacity to investigate them?
    b. As per IT Act only an inspector can investigate these cases, but in Delhi head constables onwards they are all IOs in cybercrime cases, how does this work in practice?
4. How can there be better coordination between different state police forces on the issues of cybercrime?
5. Do you think the onus should be on the state and the government to prevent these cases of cybercrimes?
6. Since England has laws of compensating victims of financial fraud by the banks, can it be done in India too?
    a. What are the alternatives that can be adopted other than the one England has?
7. What can be done for the prevention and redressal of cybercrimes?
8. How do you think India can tackle this by taking the onus away from the victims themselves?
9. What is your opinion on digital signatures?
10. Why do you think property documents are kept out of the documents where digital signatures are applicable?
11. India grants protections under the IT Act, how does this affect the content that the companies publish on their websites?
12. How do government directions to companies interfere with their freedom of speech and expression?
    a. Do you think whatever goes on their website is reflective of their policies?
    b. How do you think the companies should balance between government directives and their responsibility to protect freedom of expression?
    c. What is the right way to go about protection of freedom, speech and expression?

INTERVIEW GUIDE 8: FOR CYBERCRIME EXPERTS (GENERAL)

1. How did you start working with this area of cybercrime?
    a. What is your current role?
    b. What compelled you to work on this issue?
2. What are the types of crimes which are the most pervasive right now?
    a. How is it done and how do the victims get affected by it?
3. Same SIM cards can be used in different states to commit cybercrime, however, if you have the phone number or the transaction number, it is supposed to be blocked immediately. So how do the criminals manage to use the same number for further crimes?
4. How does the data leak happen?
    a. How do you think that the accounts are being hacked even when the people claim that they have not given away any information through phone calls, texts or OTPs?
5. Are the cybercrimes always so organised such as the delivery scams?
    a. Do they access all the information from the dark web?
    b. What is the extent of these organised cybercrimes?
    c. How much money is India losing due to these cybercrimes?
6. In financial cybercrimes, people have complained that they are not able to recover their money or only able to recover half of it, so is it a systemic failure to react promptly or just because the criminals are so active and quick?
    a. Do you think the banks are complicit in these crimes?

b. Is this true for both private as well as public banks or is it more in public banks because we have heard more cases from them?

    c. Could it be because there are more accounts in public banks?
    d. According to you, is the security of systems at par at both private and public banks?
7. How pervasive are non-financial cybercrimes?
    a. Which kinds of such crimes are most common?
    b. Why don't the victims come out more for such crimes?
    c. Is it because they are not very common?
    d. What is the actual ground situation?
8. Are there any alternate support structures that are available for victims of these crimes?
    a. Are there any support systems which are available to help the victims after the official complaint has been filed?
9. What do you think about AI being used to carry out cybercrimes?
10. Do you think the police force is equipped with all the training and the resources that they need?
    a. Do you think they have the capacity to be able to deal with this explosion of cybercrime that we are facing?
    b. What is the quality of police training in handling these cases?
    c. How can an entire structure be constructed even at the lowest ranks, so they have the capacity to deal with it properly?
    d. Do you think that there is a need for some kind of involvement of private agencies or individuals like yourself to be able to strengthen this?
    e. Do you think that some state police departments are less cooperative than others?
    f. What can be done to improve that?

11. How vulnerable are the non-banking Financial Companies?
    a. How do the police deal with this?
    b. How does the investigation take place in such cases?
12. How complicated is the nexus of arresting low level team members for crimes who turn out to be victims of cyber fraud? [context: trafficked persons being coerced to carry out cyber fraud]
    a. How far does this nexus go?
    b. How difficult does it become to see who is the victim, who is the accused and why they are doing what they are doing?
13. Do you think there is a better way of communication between the banks and the police?
    a. Can there be a systemic process through which this can be done instead of the police reaching out to the banks over and over again and the banks responding or not responding at their own convenience?
    b. Do victims go through this process themselves?
14. For non-English speaking victims, especially from rural areas, accessing the complaint platform is a great barrier, how do you think they navigate registering?
15. There have been complaints of banks denying the victims' liability, so how do you think the victims can prove themselves and how can the banks do better to help them?
    a. Do you think it's better to approach the bank first or to register a complaint first?

Common Cause is a registered society dedicated to championing public causes, campaign for probity in public life and integrity of institutions. It seeks to promote democracy, good governance and public policy reforms through advocacy, interventions by formal and informal policy engagements. Common Cause is especially known for the difference it has made through a large number of Public Interest Litigations filed in the Courts, such as the recent ones on the setting aside of the Electoral Bonds Scheme; cancellation of the entire telecom spectrum; cancellation of arbitrarily allocated coal blocks; Apex Court's recognition of individuals right to die with dignity and legal validity of living will.

Centre for the Study of Developing Societies (CSDS) is one of India's leading institutes for research in the social sciences and humanities. Since its inception in 1963, the Centre has been known for its critical outlook on received models of development and progress. It is animated by a vision of equality and democratic transformation. Lokniti is a research programme of the CSDS established in 1997. It houses a cluster of research initiatives that seek to engage with national and global debates on democratic politics by initiating empirically grounded yet theoretically oriented studies. The large volume of data collected by Lokniti on party politics and voting behaviour has gone a long way in helping social science scholars make sense of Indian elections and democracy.

Common Cause
Common Cause House,
5, Institutional Area, Nelson Mandela Road,
Vasant Kunj, New Delhi 110 070
Phone: +91-11-45152796
E-mail: commoncauseindia@gmail.com
Website: www.commoncause.in

Lokniti - Centre for the Study of Developing Societies (CSDS)
29, Rajpur Road, Civil Lines, Delhi 110054
Phone: +91-11-45789412; +91-11-40727733
Email: csdsmain@csds.in; lokniti@csds.in
Website: www.csds.in; www.lokniti.org

COMMON CAUSE
A ROMANCE WITH PUBLIC CAUSES SINCE 1980

लोकनीति
Programme for Comparative Democracy

LAL FAMILY FOUNDATION

CSDS
centre for the study of developing societies