

Status of Policing in India Report 2026
Cybercrimes—Victim Perspectives and Systemic Responses

EXECUTIVE SUMMARY

Over the past decade, cybercrime has become part of everyday life in India -touching people's money, their data, and their sense of safety online. It doesn't stay confined to one place or one kind of victim: anyone with a phone, a bank account, or a social media profile is at risk. Traversing jurisdictions, affecting multiple institutions and communities, and evolving into a highly organised ecosystem, cybercrime networks have proliferated across India.

In this context, the *Status of Policing in India Report (SPIR) 2026: Cybercrime—Victim Perspectives and Systemic Responses* turns its focus to cybercrime - how it is perpetrated, who it targets, and how citizens, the police and the banking system respond to it. Continuing the SPIR series' focus on public trust in and experience of the police, this edition examines the modus operandi of cybercriminals, the lived experience of victims, the digital habits and vulnerabilities of ordinary citizens, and the preparedness of the police and banks to handle complaints.

The latest edition of SPIR is jointly conducted by Common Cause and Lokniti-CSDS. This study draws on a survey across 16 Indian states with over 8,306 respondents, aiming to examine the rapidly changing nature of cybercrimes in India and the systems meant to respond to them. The qualitative component of the study is based on detailed one-on-one interviews and a focus group discussion, presenting findings from open-ended conversations with 37 respondents--domain experts, cybercrime victims and those who closely assisted them, and kin of individuals charged with cybercrime.

Key findings of the SPIR 2026 are presented below.

FINDINGS FROM QUALITATIVE INTERVIEWS

The Anatomy of Cybercrime: Perpetration, Under-reporting and Impact

- 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.
- Organised networks run both financial and non-financial cybercrime, trading leaked data, mule accounts and fake SIM cards as ready-made “kits”.
- Cybercrime is heavily under-reported due to stigma, distrust of authorities, and a sense that complaints won't be taken seriously. Most cases of online gender-based violence and non-consensual image abuse go unreported.
- Victims described stress, trauma and depression due to the cybercrime and the complaints procedure that followed -- including a miscarriage, a victim who left her profession and moved to a different country, and another who fell into severe depression after losing his life savings post-retirement.

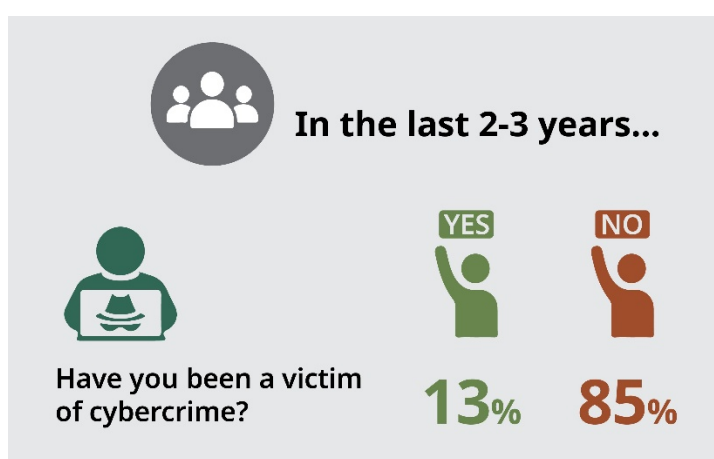
Institutional Responses: A Difficult and Unequal Road

- 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.
- 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.

SURVEY FINDINGS: CYBERSECURITY, VICTIMISATION AND REDRESSAL MECHANISM FOR CYBERCRIMES

Threats to Digital Safety and Cybercrime Victimization

- 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 that are linked to illegal activities, and unknown numbers claiming to be a friend. Data shows that greater usage of online payment is associated with higher exposure to fraudulent calls.
- **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.



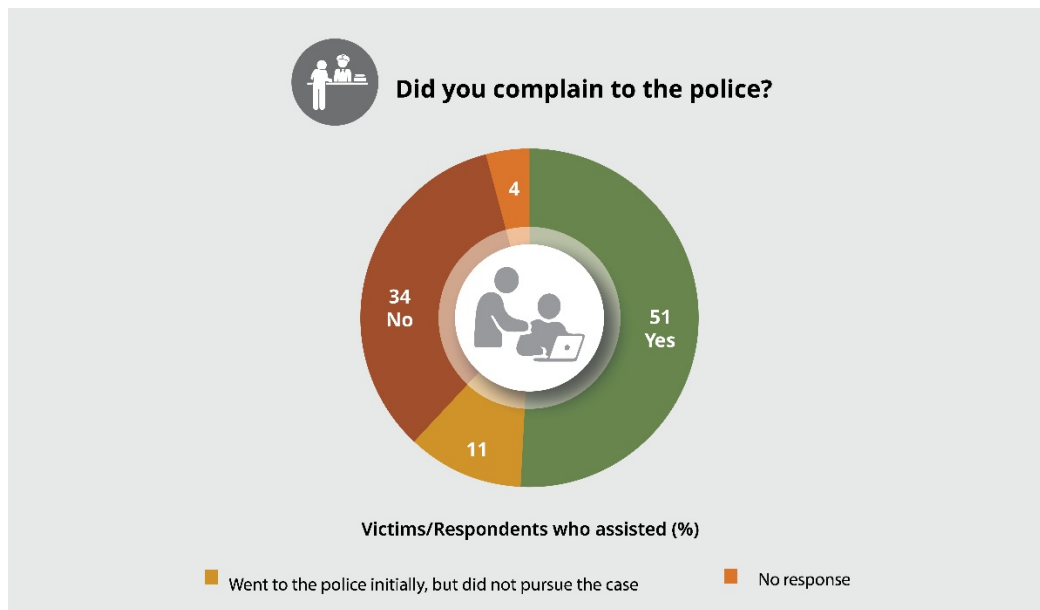
- **More than half of all cybercrimes reported involve digital financial frauds.** Eleven percent of the victims faced personal data theft, seven percent faced cyberbullying and four percent faced online sexual abuse. Respondents from upper

class backgrounds and those who are more educated are more likely to face digital financial frauds.

- **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.

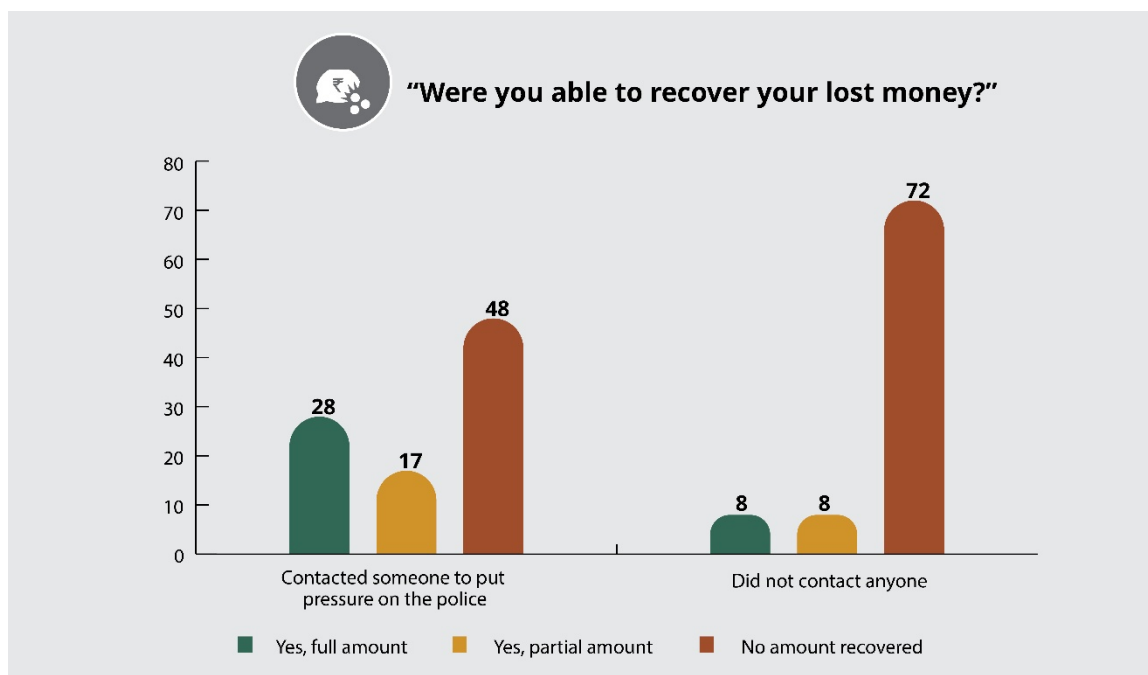
Experience with the Police

- **About half of the victims (51%) complained to the police** after the cybercrime, while another 11 percent went to the police initially but did not pursue the case.



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

- 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.
- **Over two in five (42%) 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 more 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.**



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.

Experience with the Banks

- 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.**



Note: The rest did not respond. For more information on the index, refer to Appendix 2. 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?

- **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.

Digital Habits and Cyber-security

- **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.
- **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 more prone to cybercrime than those who are not regular users.**

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 cybercrimes 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.

- 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.
- 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.

Trust in Institutions and Path Ahead

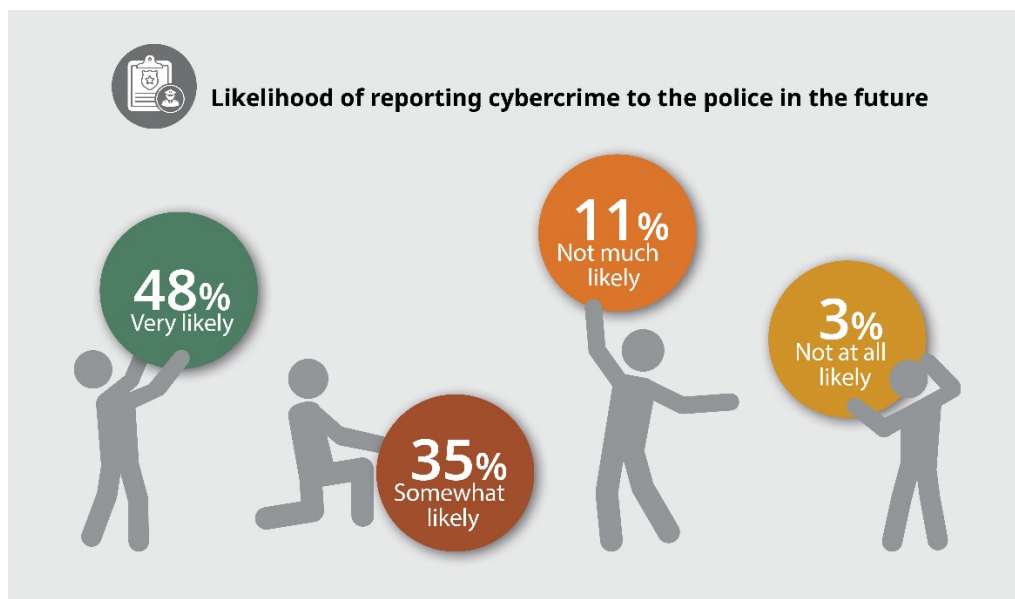
- Nearly three out of four people feel that the police are equipped to deal with financial cybercrimes. Twenty-nine percent feel they are “well equipped”, while 44 percent feel they are “somewhat equipped”.
- **Victims of cybercrimes are less likely to believe that police are well-equipped to deal with cases of 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 cybercrimes.

	To deal with 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?

- 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 say that, in case they face such a crime in the future, they will report it to the police.**



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?



Please scan the QR code or click on the link given below to download the copy of the Report

https://commoncause.in/pdf/SPIR_2026.pdf