CANONSPHERE LAW REVIEW

ISSN: 3107-460X (Online)

CANONSPHERE LAW REVIEW

Volume 1 Issue 3

July to September, 2025

TABLE OF CONTENTS

THE ILLUSION OF AUTHORITY: UNDERSTANDING DIGITAL ARREST IN INDIA

This short article is written by N. Likhitha Prasad, an LLM Student of Jain (Deemed-to-be-University) School of Law, Bengaluru.

ABSTRACT

The rapid growth of digital technologies and internet penetration in India has opened up once-in-a-lifetime opportunities for communication, commerce, and governance. However, in tandem with these benefits, cybercrime has reared its head as a serious threat. One of the most noted forms of this phenomenon is called "Digital Arrest" - a sophisticated scam that relies on fear, authority and psychological manipulation to extort funds from unsuspecting individuals. In incidents of Digital Arrest, criminals impersonate law enforcement officers, customs officials, or other government authorities, and individuals are falsely implicated of committing crimes, such as narcotics trafficking, money laundering, or other cyber offenses, and subsequently intimidate them in real time via video calls, surveil them at home, all the while threatening to arrest them or seize their property unless they produce financial payment as falls to clean their name.

This study addresses the meaning, modus operandi and legal implications of digital arrest scams in an Indian context, as well the various cyber techniques deployed by criminals, ranging from caller ID spoofing, phishing, counterfeit documents to the impersonation of a judicial or law enforcement authority. The paper carefully examines the social, psychological and economic implications for victims of digital arrest, beyond just loss of financial funds, but also severe mental trauma, social dislocation and extreme cases of victim suicides. The legal analysis relies on the Information Technology Act, 2000, and Bharatiya Nyaya Sanhita, 2023, exploring just how existing laws deal with crimes of cheating, impersonation, forgery, and extortion in digital spaces. The courts and others have reinforced in multiple ways that there is no legal basis for arrest via online means; hence, “digital arrest” can only be viewed as fraudulent. Despite the fact that the government has established a number of channels for victims to report such illegal behavior, notably through the Indian Cyber Crime Coordination Center (I4C) and the

National Cyber Crime Reporting Portal and the 1930 telephone helpline. Despite recent specific warnings to the public, the issue continues to worsen, as seen in reference to the thousands of crores of rupees in financial loss.

This research promotes deeper discussion about the potential to strengthen law enforcement capacity, increase cyber literacy, forge effective international cooperation and establish victim support initiatives through analysis of case studies and statistical information. In conclusion, the study concludes that the challenge of preventing or defending against digital arrest scams will require societal shifts to alertness or resilience that should include legal and technological means as well as literacy in the digital ecosystem, through societal awareness and action.

Keywords: Digital Arrest, Cybercrime, Impersonation, Online Fraud, Cybercriminals

INTRODUCTION

The digital revolution has transformed every aspect of contemporary society, from financial transactions and work to socialising and governance. India emerging as a digital economy in the globe, reliance on digital systems has surged. However, alongside these developments, cybercrime has developed into a corresponding threat that uses the same technological networks that empower our lives. Among the variety of cybercrimes, the emergence of Digital Arrest scams has surfaced as one of the major threats in recent years. Although the term Digital Arrest sounds legal in nature, this crime is more accurately described as a type of cyber-enabled fraud.

In Digital Arrest criminals use fear, authority, and technology to extort financial payments from unsuspecting persons. Digital Arrest scams differ from traditional fraud in that fraud is often more subtle, employing techniques of social engineering, impersonation and real-time intimidation. Victims are often induced to believe they are being investigated and as such, pressured to make financial payments. This paper will analyse the mechanisms of these scams, the legality of the scammer's actions, the psychological and financial impact of being scammed, and the role of law enforcement and judiciary in addressing this problem.

What particularly makes this scam insidious is the foreground of psychological manipulation; victims were monitored for hours using video surveillance, coerced into embarrassing themselves, and threatened with transferring large sums of money as "security deposits" or "penalties." Fraudsters typically have elaborate processes to make the deception plausible; for example, they supply documents that appear fake, pretend to be speaking to the police, and even fake a police station, often having staged a studio type of environment to make it convincing.

This research aims to elucidate the ascendance of digital arrest by exploring its mechanisms, triggers, and potential counter-functionality within law. It employs statutory frameworks under the Information Technology Act, 2000, and Bharatiya Nyaya Sanhita, 2023 which will be elaborated on, where relevant, along with some case law and governmental advisories.

RESEARCH METHODOLOGY

This research utilizes descriptive exploratory methodology. It employs both primary and secondary data obtained from credible sources, including news portals, government reports, statutory laws, research journals and papers, and case studies of cybercrime. It applies a doctrinal method of research to understand legal regulations related to cybercrime as well as case studies involving digital arrest frauds, which is a method of studying law.

RESEARCH OBJECTIVE/PURPOSE

The major aims of the study are:

1. To understand the meaning and nature of digital arrest scams;
2. To evaluate the legal framework in India relating to them; and
3. To analyze government initiatives, judicial responses and law enforcement practices.

MEANING OF DIGITAL ARREST

Digital arrest is a scam which utilizes intimidation, coercion, deceit, and fear to extract money from victims. Fraudsters impersonate law enforcement officers and threaten victims with arrest, bank account freezing, and passport cancellation in order to get them to pay a sum of amount in order to abstain from being brought into legal action.[1]

When fraudsters call a potential victim and say they have sent or are the intended recipient of a package, including illegal items, drugs, fake passports, or any other sort of contraband, this is known as a "digital arrest." They sometimes inform their loved ones when one of the victims is in custody after being taken into custody for an offense or accident. The con artists demand cash in exchange for making compromises. Some gullible victims are compelled to go through a "Digital Arrest" and publicly reveal themselves to con artists through Skype or another video conferencing service until their demands are satisfied. To make themselves seem real, the criminals are known to dress in attire and utilize studios that look like police

[1] https://www.niti.gov.in/sites/default/files/2025-04/Digital_Arrest_The_Modern_Day_Cyber_Scam.pdf, accessed on 09 August, 2025.

stations and government buildings. They contact individuals via messaging apps, emails, or video calls, accusing them of alleged illegal activities, such as money laundering or cybercrimes. The scammers present fabricated evidence and intimidate victims into making payments or sharing sensitive information to avoid fictitious legal repercussions.

CRIMES LEADING TO DIGITAL ARREST

If the fraudster commits certain actions, they are tempting the crime of digital arrest against the victim, which is stratified below:

- Hacking: This refers to the illegal access of individuals' computer systems or networks, where offenders exploit accounts in breach of law or legal responsibilities, subsequently threatening victims by impersonating law enforcement and swindling them out of money by subjecting them to fictitious trials and imposed penalties.
- Cyber-stalking and Online Harassment: These cybercriminals closely monitor individuals and can access their social media accounts; they may use digital platforms to intimidate, harass, stalk, or threaten victims, sometimes even impersonating them.
- Phishing: Phishing involves deceitfully obtaining sensitive information such as passwords and financial information from individuals, portraying the fraudsters as reliable entities, and subsequently using that information to scam money through digital threats of arrest.
- Pornography: The creation or distribution of pornographic material, regardless of whether it involves minors, constitutes an offense. Individuals frequently answer calls that inadvertently display pornographic content, and once the call is terminated, these offenders promptly call back, accusing the individual of engaging in pornography.
- Financial Fraud: Offenses such as credit card fraud, identity theft, and similar crimes are perpetrated against victims to instill fear. False accusations of unlawful payments from their account have been directed at them, attempting to entangle them in this crime.
- Misinformation and Hostile Speech: The spread of inaccurate information or provocative material via the victim's account places them at the core of this offense. These criminals

typically monitor the online behaviors of their victims or their family members for weeks prior to placing these deceptive calls.[2]

LEGALITY OF DIGITAL ARREST IN INDIA

"Digital arrest" has no statutory recognition under Indian law. It is not a lawful act of apprehension but rather a **fraudulent cybercrime** where offenders impersonate government officials or law enforcement agencies to extort money from victims. The newly introduced criminal law restricts police officers or law enforcement agencies from carrying out digital arrests.

COMMON MODUS OPERANDI OF SCAMMERS

The digital arrest operates as follows:

- Initial Contact and impersonation: Fraudsters use phone calls, emails, WhatsApp messages, or fake official correspondence and pose as law enforcement or government officials (CBI, ED, Customs, Interpol, etc.).
- Instilling Fear: The target is wrongfully blamed for offences such as money laundering or cybercrime and warned of imminent arrest if they don't respond swiftly.
- Threats of Legal Action: Cybercriminals typically warn victims that they are under investigation or facing legal action due to unpaid taxes, illegal downloads, or other fabricated offences. These threats are designed to cause panic and compel victims to act quickly without verifying the claims.
- Urgency and Pressure: The scammer often creates a sense of urgency by stating that immediate action is required to avoid arrest, legal consequences, or other severe penalties. Victims are deterred from using reason/rationale or seeking advice from others by this pressure.

[2] Jyoti Chauhan, Digital Arrest: An Emerging CyberCrime In India, available at https://ijlmh.com/wp-content/uploads/Digital-Arrest-An-Emerging-Cybercrime-in-India.pdf, accessed on 11 August 2025.

- Phishing and Fake Websites: Scammers frequently use phishing emails or fake websites that mimic legitimate government portals. Victims are tricked into entering personal or financial information, which is then used for fraudulent purposes.
- Social Engineering: Cybercriminals may also use social engineering tactics, such as gathering information about the victim through social media, past data breaches, or public records, to make the scam appear more credible
- Digital Verification: To enhance reliability, fraudsters provide counterfeit documents, phony videos, or altered arrest warrants, making the assertion seem genuine.
- Coercion/Intimidation: The victims face risk of being arrested, having their accounts frozen, or having their passports revoked. They are advised not to consult with relatives or lawyers and are asked to pay a "security deposit" or "penalty."[3]
- Payment Methods: Digital transactions like UPI, bitcoin, or prepaid gift cards are used for payments, and sometimes fraudsters use remote banking information monitoring.[4]
- Vanishing Act: After the victim sends the money, the fraudsters disappear, and the victim only understands they've been tricked after attempting to confirm the matter with real authorities.
- Money Laundering: The illegally obtained money is frequently split into smaller sums, routed through various accounts, and ultimately moved to offshore accounts for unlawful purposes.[5]

CYBERCRIMINAL TACTICS AND TECHNIQUES

Although the methods employed in digital arrest scams are always changing, they often involve technology, psychological manipulation, and trust exploitation. Some of the most effective tactics include:

- Faking authenticity
- Counterfeit Documents and Emails

[3] https://www.researchgate.net/publication/387820138_The_evolution_of_digital_arrest_cyber-crimes_in_India_Trends_and_patterns_preventive_measures, accessed on 12 August 2025.
[4] Digital Arrest: Modern Day Scam available at https://www.niti.gov.in/sites/default/files/2025-04/Digital_Arrest_The_Modern_Day_Cyber_Scam.pdf, accessed on 13 August 2025.
[5] file:///C:/Users/user/Downloads/In_Re_In_the_matter_of_tackling_the_issue_of_DigitRH20252401251818411 2COM617944.pdf, accessed on 16 August 2025.

- Leveraging Fear and Power
- Non-Traceable Payment Solutions

GROWING THREAT OF CYBERCRIME

Cybercrime has evolved into a global issue, with individuals, businesses, and governments all being targeted by criminals exploiting digital systems. The rise in cybercrime can be attributed to several factors:

- Heightened Internet Engagement
- Complexity of Cyber Attacks
- Absence of Awareness

LAWS REGULATING THE DIGITAL ARREST

The rise of digital arrest scams underscores the need for robust legal frameworks. The Role of Legislations/Laws in Tackling Digital Arrest Scams are stratified below:

Bharatiya Nyaya Sanhita, 2023 (BNS 2023)

Section 3 (5) – (common intention)
Section 61 (2) – (criminal conspiracy)
Section 111 – (organized crimes)
Section 204 - (impersonating a government official)
Section 318 - (cheating),
Section 319 - (cheating by impersonation),
Section 335 - (making a false document)
Section 336 (3) - (forgery for purpose of cheating)
Section 338 – (forgery of valuable security, will, etc.)
Section 340 (2) – (forged document or electronic record and using it as genuine)
Section 351 – (criminal intimidation)

Information Technology Act, 2000

In India, the Information Technology Act, 2000 serves as the cornerstone for cyber law enforcement. Key provisions include:

1. Section 66D: Penalizes cheating by personation through computer resources, with imprisonment of up to three years and fines up to ₹1,00,000.
2. Section 66C: Addresses identity theft, punishing fraudulent use of another's identity with similar penalties.
3. Section 66E: Focuses on privacy violations, particularly the unauthorized capture or transmission of private images.
4. Section 67: Penalizes the transmission of obscene content, which may be used during scams. These provisions, while comprehensive, require enhanced enforcement and public awareness to effectively deter such crimes.[6]

CAUSES OF DIGITAL ARREST

The causes of digital arrest are listed below:

- Technological Failures
- Policy and Regulation
- Digital Inequality
- Ethical and Social Concerns

INDIA'S FIGHT AGAINST CYBER CRIME AND DIGITAL ARREST

To tackle the rising threat of cybercrime, the Indian government has intensified its initiatives against digital arrest. Main initiatives consist of [7]:

- Indian Cyber Crime Coordination Centre (I4C): This centre, which was established by the Ministry of Home Affairs, provides resources for preventing cybercrime and coordinates national efforts to combat it.
- National Cyber Crime Reporting Portal: A specialized platform enables the public to report cybercrimes, particularly those affecting women and children, facilitating prompt response from law enforcement.
- Financial Cyber Fraud Reporting System: Initiated in 2021, this system has effectively preserved more than ₹3431 Crore through 9.94 lakh complaints by enabling prompt reporting of financial frauds.

[6] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5076535, accessed on 17 August 2025.
[7] https://www.niti.gov.in/sites/default/files/2025-04/Digital_Arrest_The_Modern_Day_Cyber_Scam.pdf, accessed on 19 August 2025.

- Cyber Forensic Labs: The ability of law enforcement to handle and analyse digital evidence has been significantly improved by the establishment of the Evidence Laboratory in Hyderabad and the National Cyber Forensic Laboratory in Delhi.

- Training via CyTrain: I4C's digital platform educates law enforcement and judicial personnel on cybercrime investigation and prosecution, having trained more than 98,000 police officers to date.
- Awareness Initiatives: In order to promote cyber safety and security, the government has started awareness campaigns using SMS, social media, Cyber Dost, the SancharSathi portal and app, and digital screens in public places like metro stations and airports.
- Grievance Redressal Helpline: The government has introduced a toll-free number 1930 to help individuals file online cyber complaints. By 2024, over 9.94 lakh grievances were filed, involving amounts exceeding Rs. Savings amounted to 3431 crores.[8]

INSTANCES/RECENT SCENARIO'S OF DIGITAL ARREST

- The Criminal Investigation Department (CID) has caught a cybercriminal who tricked an Army officer out of almost Rs. 2.98 crore by getting him to invest on a false platform that pretended to be the Chicago Board of Options Exchange.[9]
- In another example of "digital arrest," cyber criminals pretending to be police officials allegedly kept two lady's captive on a video chat for almost nine hours and made them strip naked for an "online medical examination reported on 23 July 2025.[10]
- A cybercriminal was caught in Ahmedabad, Gujarat, for defrauding an elderly person out of Rs 49.88 lakh by pretending to verify his account, after placing him under digital arrest for 'being involved in a Rs 300cr scam'. [11]

[8] https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=2082761, accessed on 20 August 2025.
[9] https://timesofindia.indiatimes.com/city/ranchi/cyber-fraud-nabbed-in-2-98-crore scam/articleshow/123080522.cms, accessed on 20 August 2025.
[10] https://timesofindia.indiatimes.com/business/cybersecurity/digital-arrest-scam-two-women-held-on-hostage-for-nearly-nine-hours-by-fraudsters-posing-as-police/articleshow/122862160.cms, & https://timesofindia.indiatimes.com/business/cybersecurity/digital-arrest-scam-two-women-held-on-hostage-for-nearly-nine-hours-by-fraudsters-posing-as-police/articleshow/122862160.cms, accessed on 20 August 2025.
[11] https://timesofindia.indiatimes.com/city/ranchi/cyber-fraud-held-from-abad-for-scamming-elderly-of-50l/articleshow/122819893.cms, accessed on 20 August 2025.

- Bengaluru: A 48-year-old contract staffer with Bescom, who fell prey to the digital arrest fraud and lost nearly Rs 13 lakh to cybercriminals, was found hanging from a tree in his village in Ramanagar district reported on 16 July 2025.[12]
- Cyber thieves tricked an elderly pair in Madhya Pradesh into breaking a fixed deposit, causing them to lose ₹50 lakh during a 13-day digital arrest. The robbers impersonated DSP. [13]
- Three people are arrested for cheating an elderly woman out of Rs 20 crore through a "digital arrest" scam. One of the fraudsters pretends to be a "CBI officer" in order to steal money from the victim.[14]
- The Tambaram City Cyber Crime Wing police detained two men who allegedly participated/involved in a "digital arrest" scam and stole ₹1.24 crore from a woman.[15]
- Cybercriminals who claimed to be members of the Mumbai police and threatened with drug trafficking digitally detained three people, including two elderly people. On August 22, 2025, they laundered funds and then stole a sum of Rs.1.8 crores from them.[16]
- Scammers deceive an industrialist out of ₹7 crores by faking a Supreme Court hearing and impersonating the Chief Justice of India (CJI).[17]

---

12 https://timesofindia.indiatimes.com/city/bengaluru/bengaluru-man-hangs-himself-after-losing-rs-13l-to-digital-arrest-fraud/articleshow/122586844.cms, accessed on 20 August 2025.

13 https://www.freepressjournal.in/indore/madhya-pradeshs-elderly-couple-loses-50-lakh-in-13-day-digital-arrest-cyber-crooks-posed-as-dsp-forced-them-to-break-fd, accessed on 22 August 2025.

14 https://www.thehindu.com/news/cities/mumbai/elderly-woman-loses-20-crore-to-digital-arrest-fraud-3-held/article69353437.ece , & https://www.thehindu.com/news/cities/mumbai/elderly-woman-loses-20-crore-to-digital-arrest-fraud-3-held/article69353437.ece#google_vignette, accessed on 02 October 2025.

15 https://www.thehindu.com/news/cities/chennai/two-persons-held-for-digital-arrest-scam/article69968531.ece, accessed on 24 August 2025.

16 https://www.countryandpolitics.in/2025/08/22/three-including-two-senior-citizens-kept-under-digital-arrest-by-cyber-frauds-posing-as-mumbai-officials-threatening-to-foist-false-drugs-money-laundering-case-robbed-rs-1-8-crore-in-seperate-cases/ , & https://www.countryandpolitics.in/2025/08/22/three-including-two-senior-citizens-kept-under-digital-arrest-by-cyber-frauds-posing-as-mumbai-officials-threatening-to-foist-false-drugs-money-laundering-case-robbed-rs-1-8-crore-in-seperate-cases/, accessed on 02 October 2025.

17 **https://www.livelaw.in/top-stories/scammers-fake-supreme-court-hearing-impersonate-cji-dupe-industrialist-of-7-crore-271253**, accessed on 24 August 2025.

CASES/PRECEDENTS

- **Suo Motu – In the Matter of Tackling the Issue of Digital Arrest Scams v. Union of India[18],**

  The expression "Digital Arrest" was described by the Hon'ble Rajasthan High Court. Digital arrest is the practice of first creating fear and panic in people before demanding money. They ultimately become victims of cybercrime as a result of being deceived by them. The Court warned that "'digital arrest' is a crucial point to remember." In India, digital arrest has no legal basis. Digital arrest is a very complex scam that can ensnare even well-educated people. There is no legislation allowing law enforcement to make arrests via video calls.[19]

- **Akshya & Anr vs Union of India[20],**

  This petition addresses the so-called "new age cyber crimes"—notably "digital arrest" scams. The petition seeks:

  - A **public awareness campaign** on emerging cyber scams.
  - **Simplified procedures** for filing cyber-crime complaints.
  - **Guidelines** to ensure quicker investigations and improved coordination among government agencies to prevent and stop the transfer of illicit proceeds.
  - Highlighted the serious threat posed by **"digital arrest" scams**, where criminals forge arrest warrants, court orders, and impersonate authorities to extort money—undermining the criminal justice system's integrity.[21]

- **West Bengal – Kalyani District Court Judgment[22],**

[18] 2025(1)RLW493(Raj.) :MANU/RH/0056/2025, https://www.casemine.com/judgement/in/6791d8bcf67f9c2a314ec348, accessed on 02 October 2025.
[19] file:///C:/Users/user/Downloads/In_Re_In_the_matter_of_tackling_the_issue_of_DigitRH202524012518184112COM617944.pdf & **https://www.livelaw.in/high-court/rajasthan-high-court/rajasthan-high-court-suo-motu-cognizance-digital-arrest-scams-281745**, accessed on 24 August 2025.
[20] W.P. (C) 528/2024
[21] https://indiankanoon.org/doc/93233007/, accessed on 24 August 2025.
[22] https://timesofindia.indiatimes.com/india/in-a-first-9-sentenced-to-life-by-court-in-bengal-for-digital-arrest-fraud/articleshow/122773681.cms & https://www.indiatoday.in/india/law-news/story/indias-first-digital-arrest-conviction-nine-people-sentenced-to-life-by-bengal-court-2758042-2025-07-19, accessed on 24 August 2025.

Nine fraudsters were given a life sentence by a Kalyani court for stealing Rs. 1 Crore from a Ranaghat local using the "digital arrest" technique. This was a historic decision. The criminals, who were apprehended in several states, were members of a group that is accused of stealing Rs. 100 crore from 108 victims throughout the country. The Information Technology Act, 2000, and the BNS, 2023, are the laws used to bring charges against the defendants. The prosecution's assertion that such cybercrimes are "economic terrorism" was accepted by the court. The first conviction for digital arrest fraud in the nation is handed down by the court.[23]

- **Nishant Roy v. State of U.P[24],**

  The accused in this case was involved in a "digital arrest" scam—a sophisticated fraud where victims are duped via video calls impersonating law enforcement and coerced into transferring funds. The victim by name Kakoli Das, targeted between April 23–25, 2024; ₹1.48 crore. Sections 384 (extortion), 406 (criminal breach of trust), 419 (cheating), 420 (cheating), 506 (criminal intimidation), 507 (criminal intimidation—repeat offender), and 34 IPC; Sections 66-C (identity theft) & 66-D (fraudulent impersonation) of the IT Act.[25] Allahabad High Court rejected bail to the digital arrest accused.[26]

- **Leela Parthasarathy v. State of Maharashtra & Ors[27],**

  The petition of a septuagenarian woman who was tricked of Rs 32 lakhs and held in 'digital arrest' was heard by the Hon'ble Bombay High Court through a division bench. The Mumbai Police officers, who had previously declined to file the FIR, were summoned by the court and subsequently carried out a "shabby probe." The way the cops claim it to be not "Bigger Scams" has drawn ire from a division bench comprised of

---

[23] https://www.uniindia.net/first-ever-conviction-in-digital-arrest-scam-kalyani-court-sentences-nine-to-life-imprisonment/east/news/3519982.html, accessed on 24 August 2025.

[24] 2025:AHC:7570

[25] https://indiankanoon.org/doc/78404091/, accessed on 24 August 2025.

[26] **https://www.livelaw.in/high-court/allahabad-high-court/allahabad-high-court-cyber-crime-silent-virus-innocent-victims-denies-bail-digital-arrest-accused-281716**, accessed on 24 August 2025.

[27] https://www.livelaw.in/high-court/bombay-high-court/police-must-register-fir-when-approached-cannot-say-it-has-bigger-scams-to-unearth-bombay-hc-o-285890 & https://indianexpress.com/article/cities/mumbai/bombay-hc-pulls-up-mumbai-police-for-delay-in-action-on-71-yr-old-womans-digital-arrest-complaint-9895348/, accessed on 24 August 2025.

Justices Revati Mohite-Dere and Dr Neela Gokhale. The bench also voiced its displeasure at the national helpline number '1930' for 'cyber fraud' not functioning 'effectively'.[28]

IMPLICATIONS OF DIGITAL ARREST

Digital Arrest has significant consequences in the economic, social, and cultural sectors. Disruptions to digital services can result in financial losses economically, while they can worsen inequalities and alienation socially. A person's psychological or mental health is negatively impacted by digital arrest, which also causes stress.

PREVALENCE OF DIGITAL ARREST SCAMS IN INDIA

Digital arrest scams have risen at a serious rate. Just between January and April 2024, people suffered losses approximately to ₹120 crore (₹1.2 billion) across 4,599 reported cases. The above timeline also reported 7.4 lakh (740,000) cybercrime complaints, indicating a wider spectrum of cyber threats.

Over 92,000 Indians fell victim to this scam in 2024, losing large sums of money.[29] In just the first two months of 2025, 17,718 cases involving ₹210.21 crore were reported, as of February 28.[30]

RECOMMENDATIONS

- Awareness Campaigns
- Strengthening NCRP & Helpline 1930

---

[28] **https://www.livelaw.in/high-court/bombay-high-court/apologize-to-public-if-national-cybercrime-helpline-doesnt-work-bombay-high-court-summons-officials-in-case-over-digital-arrest-of-senior-citizen-285777**, accessed on 24 August 2025.

[29] https://www.bbc.com/news/articles/cdrdyxk4k4ro, accessed on 23 August 2025.

[30] https://indiatomorrow.net/2025/07/08/cybercrimes-india-witnesses-big-surge-in-digital-arrest-scams/ & https://www.business-standard.com/india-news/digital-arrests-cyber-crimes-tripled-during-2022-24-govt-tells-parliament-125031200978_1.html, & https://www.juscorpus.com/the-increasing-trend-of-digital-arrests-in-india-legal-challenges-and-measures/, accessed on 02 October 2025.

- Collaboration with Telecom & Tech Companies
- Training Law Enforcement
- International Cooperation
- Stricter Punishments and Victim Support System
- Cyber Literacy in Curriculum and Behavior change in citizens to raise queries

CONCLUSION

Digital arrest scams represent a dangerous evolution of cyber fraud that manipulates fear and authority to exploit individuals. With cases multiplying across India, it is clear that cybercriminals are continuously innovating their techniques. Although legal provisions exist under the BNS, 2023, and IT Act, 2000, gaps in enforcement, public awareness, and technological monitoring persist. Judicial precedents have highlighted the seriousness of this threat, labelling it a form of economic terrorism. India's proactive steps, such as I4C, NCRP, and awareness campaigns, mark significant progress, but stronger preventive measures, international collaboration, and victim support mechanisms are crucial. Ultimately, combating digital arrest requires a combination of legal robustness, public vigilance, and cyber resilience to secure the digital ecosystem.