The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

DIGITAL ARREST SCAMS: WHAT DOES THE LAW SAY?

(Shreyanshi Pathak)

INTRODUCTION

Digital arrest scams are among the fastest-growing cyber frauds in India today. Victims across the country have lost large sums of money after being wrongly convinced that they were under investigation, or even under arrest, by law enforcement authorities. Unlike most cybercrimes, this fraud does not rely on hacking or technical skill. It relies on fear, and on the fact that most people do not know how a real police investigation actually works.

This article explains how a digital arrest scam works, why "digital arrest" is not a real legal term, which Indian laws actually apply to such cases, and what steps the government has taken to fight this crime. The key point this article makes is simple: if digital arrest does not exist in law, why is it becoming one of the most dangerous scams in the country?

HOW A DIGITAL ARREST SCAM WORKS

A digital arrest scam does not happen all at once. It unfolds in clear stages, each one designed to increase the victim's fear and stop them from thinking clearly.

First contact. The scam usually begins with a phone call, a WhatsApp message, or a courier notification. The victim may be told that a parcel booked in their name contains illegal items, or that their phone number is linked to a cybercrime case. This message is alarming enough to make the victim want an immediate explanation.

Impersonation. The caller then hands the conversation over to someone posing as a police officer, a CBI official, a customs officer, or an officer from the Enforcement Directorate. Fraudsters use fake ID cards, fabricated FIRs, forged court documents, and police-style uniforms on video calls to appear convincing.

Fear and isolation. Victims are told they are under "digital arrest" and must not contact their family, friends, or a lawyer, as this could supposedly harm a "sensitive investigation." This isolation is deliberate. It removes every option the victim has to check whether the claim is true.

Fake proof. To make the fraud look real, victims are often kept on a continuous video call for hours, asked to sit in a particular position in front of the camera, and shown fake legal documents.

Demand for money. Once the victim is frightened enough, the scammer asks for money, often described as a "refundable security deposit," to be transferred to a bank account. This account is either controlled directly by the scammer or is falsely presented as a government account.

Each stage targets a different weakness: not knowing legal procedure, respect for authority, fear of consequences, and simple panic when faced with something that looks official.

THE LEGAL TRUTH: "DIGITAL ARREST" DOES NOT EXIST

This is the most important fact in the entire scam: there is no such thing as a "digital arrest" under Indian law.

No law in India, including the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, or the Information Technology Act, 2000, allows a person to be arrested or detained through a video call. A real arrest requires an officer to be physically present, to inform the person of the reason for arrest, and to follow strict legal procedure. None of this can happen over a phone or laptop screen. The police, the CBI, and the Enforcement Directorate simply do not arrest people over Skype or WhatsApp.

This raises an obvious question: if there is no legal basis for it at all, how does this scam keep succeeding? The answer is that "digital arrest" is not a legal term. It is simply a name that fraudsters invented for their method of extortion. The actual crime being committed is a mix of well-known offences: cheating, impersonation, forgery, identity theft, and criminal intimidation, all carried out using digital tools. The scam works mainly because most people do not know that the entire situation is legally impossible. It is this gap in awareness that fraudsters take advantage of.

WHICH INDIAN LAWS APPLY

Even though "digital arrest" itself is not defined anywhere in law, every act that makes up this scam is already a punishable offence under existing statutes.

Under the Bharatiya Nyaya Sanhita, 2023:

- Section 318 – Cheating
- Section 319 – Cheating by personation, which directly applies since the fraudster pretends to be a police or investigating officer
- Section 336 – Forgery of valuable security or electronic records, covering the fake FIRs and warrants shown to victims
- Section 340 – Using forged electronic records
- Section 351 – Criminal intimidation, covering the threats of arrest or prosecution used to pressure victims into paying[1]

Under the Information Technology Act, 2000:

- Section 66C – Identity theft, which applies when scammers misuse fake IDs or official-looking credentials
- Section 66D – Cheating by personation using a computer resource, which fits this scam closely, since the entire fraud takes place over video calls and messaging apps[2]

These provisions show that Indian law is not silent on this issue. A new offence called "digital arrest" is not needed, because the scam can already be prosecuted using existing criminal and cyber laws, as long as it is reported correctly.

THE GOVERNMENT'S RESPONSE

As this scam has grown, several institutions have been strengthened to respond to it more effectively.

[1]Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, §§ 318, 319, 336, 340, 351 (India).
[2]Information Technology Act, 2000, No. 21 of 2000, §§ 66C, 66D (India).

- The Indian Cyber Crime Coordination Centre (I4C), under the Ministry of Home Affairs, works to track and coordinate the response to cybercrime, including digital arrest scams, across states.
- The National Cyber Crime Reporting Portal allows victims to report such incidents online, so complaints reach the right authorities faster.
- The Cyber Crime Helpline (1930) gives victims a direct number to call, which is especially useful in the first few hours after money has been transferred.[3]
- Awareness campaigns by the Ministry of Home Affairs regularly remind the public that no government agency arrests, questions, or verifies anyone through a video call.
- Banks have also become quicker at freezing suspicious transactions once they are reported, which helps stop funds before they are moved further.

None of these steps create a new offence. Instead, they make it faster to detect a scam, report it, and recover stolen funds, which matters greatly in fraud cases where every hour can decide whether the money is recovered.

This coordinated approach is beginning to show results. In April 2026, the CBI arrested three people, including a bank official, in connection with a ₹1.6 crore digital arrest scam targeting a senior citizen; the investigation traced mule accounts and layered transactions across Telangana and Andhra Pradesh, showing how banking-sector complicity and cross-state coordination have become central to both the fraud and its detection.[4]

Even so, the response remains largely reactive. Most of these mechanisms activate only after a victim has already transferred money, and recovery still depends on how quickly a transaction is reported before funds are layered across multiple mule accounts or moved offshore. The institutions in place are necessary, but they treat the symptoms of the scam rather than its root cause, which is the public's unfamiliarity with how a real investigation works. Sustained prevention will depend less on new enforcement powers and more on closing that awareness gap before the first call is even made.

---

[3] Ministry of Home Affairs, Indian Cyber Crime Coordination Centre, https://i4c.mha.gov.in; National Crime Records Bureau, National Cyber Crime Reporting Portal, https://cybercrime.gov.in (last visited July 17, 2026).

[4] See Rs 1.6 Crore Digital Arrest Scam: CBI Held Three, Including Bank Official, Deccan Herald (Apr. 18, 2026), https://www.deccanherald.com/india/cbi-busts-rs-16-crore-digital-arrest-scam-bank-official-among-3-held-3972761.

WHY AWARENESS MATTERS

Since this scam works mainly through fear rather than technical hacking, legal provisions alone are not enough to stop it. Public awareness plays an equally important role.

Government advisories have made one fact clear again and again: no investigating agency in India carries out arrests or questioning over a video call. If this single fact were widely known, the scam would lose its power before it even begins. In this sense, awareness works as the first line of defence, often stopping the fraud before it can even start.

Reporting quickly also matters. The faster a fraudulent transaction is reported, the higher the chance that banks and cyber cells can freeze the funds before they are moved through multiple accounts and become impossible to trace. This is exactly why the 1930 helpline and quick bank action have become such an important part of India's response to this crime.

CONCLUSION

Digital arrest scams show that cybercriminals are relying more on fear than on technology. No law in India allows arrest or questioning through a video call, and this gap is not a weakness in the legal system, it is the very illusion the scam is built on. Indian law, through the Bharatiya Nyaya Sanhita, 2023 and the Information Technology Act, 2000, already provides enough legal ground to prosecute the cheating, impersonation, forgery, and intimidation involved in this crime.

What is truly needed is not a new law, but wider public understanding. Once people know that no agency arrests anyone over a video call, and once they know how to report such incidents quickly through channels like the Cyber Crime Helpline, this scam becomes far easier to stop.