

# Digital Arrest Scams: Govt Moves to Block Devices in Digital Arrest Scam

March 21, 2026 • vajiramandravi.com



## Digital Arrest Scams Latest News

- The Union Home Ministry has asked WhatsApp to implement measures like blocking device IDs, detecting scams, and strengthening AI tools to curb the rising menace of “**digital arrest**” **scams** in India.
- A high-level Inter-Departmental Committee (IDC), set up by the Union Home Ministry in December 2025, met with WhatsApp representatives and asked the platform to implement these measures.

## What is Digital Arrest Scam

- In a digital arrest scam, fraudsters:
  - Impersonate law enforcement officers (CBI, police, ATS, etc.) on video calls.
  - Tell victims they are under investigation for serious crimes.
  - Psychologically trap them and coerce them into transferring large sums of money to avoid “arrest”.
- These scams are entirely fake — no real agency conducts arrests over video calls.

## How Big is the Problem

- 1.23 lakh cases of digital arrest were recorded in 2024 alone — nearly three times the number in 2022.
- **Total estimated losses:** nearly ₹3,000 crore.
- The Supreme Court took suo motu cognizance (acted on its own) of the issue in October 2024, expressing “grave concern”.
- Fraudsters use mule accounts (third-party bank accounts) to move crores across banks and state borders within minutes, making them hard to trace.

## Background: Government’s Response

- The **Inter-Departmental Committee (IDC)** was constituted by the Union Home Ministry in December 2025
- It brings together multiple government departments to tackle digital arrest scams in a coordinated manner
- The third meeting of this committee took place recently, where WhatsApp representatives made detailed submissions about the platform’s existing detection and enforcement mechanisms.

## Key Measures WhatsApp Has Been Asked to Implement

- WhatsApp has been asked to implement various measures to tackle the threat of digital arrest, including the impersonation of law enforcement officers to perpetrate the scam.

### Blocking Device IDs of Repeat Offenders

- WhatsApp has been asked to assess and block the Device IDs (unique identifiers of phones/devices) used in digital arrest scams.
- This would prevent repeat offenders from simply creating new accounts on new or the same devices.
- A detailed proposal is expected within 45 days.

### Skype-like Safety Features

- WhatsApp has been asked to introduce safety features similar to Microsoft’s Skype, including:
  - More information about who is calling
  - Warning signals for suspicious or unverified accounts
  - Better detection of scam networks
- A proposal on these features is expected within 30 days.

### Retaining Deleted Account Data

- WhatsApp must ensure user data from deleted accounts is retained for at least 180 days, as required under **IT Rules, 2021**.
- This is critical for law enforcement agencies investigating fraud cases.

### Blocking Harmful APK Files

- APK files are Android app installation files — scammers often use malicious APKs to gain access to victims' devices.
- WhatsApp has been asked to strengthen its technology to detect and block such harmful files and similar content.
- Technical measures are expected within one month.

## AI & Machine Learning to Detect Impersonation

- WhatsApp is expanding its AI and machine learning systems to detect:
  - Impersonation of law enforcement officers
  - Misuse of official logos (Delhi Police, Mumbai Police, CBI, ATS, etc.)
  - Synthetic or AI-generated/deepfake content used in video call scams
- The platform has already deployed logo detection and media matching systems to identify and remove impersonating accounts.
- Periodic progress updates will be shared with the government.

## SIM Binding Directive — A Separate but Related Order

- In November 2025, the Department of Telecommunications (DoT) directed all app-based communication platforms — WhatsApp, Telegram, Signal, Snapchat — to implement **SIM binding**.
  - SIM binding (SIM linkage) means the app can only be used with one specific, active SIM card, eliminating anonymous or multi-device misuse.
- This strengthens user traceability and national security compliance.
- WhatsApp has committed to implementing this within 4–6 months and submitting an Action Taken Report (ATR) by March-end.

## WhatsApp's Commitments to Law Enforcement

- Timely response to flagged fraud networks and impersonation reports.
- Compliance with updated IT Rules for identification and labelling of AI-generated or deepfake content.
- Enhanced cooperation with investigative agencies on digital extortion cases.

**Source: IE**

---

Source: <https://vajiramandravi.com/current-affairs/digital-arrest-scams/>

© Vajiram & Ravi. For personal use only.