



CYBER CENTRE OF EXCELLENCE
Gujarat Police

DIGITAL ARREST

The Scam That Doesn't Exist in Law

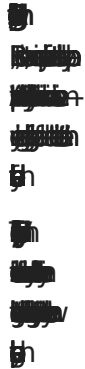


A Public Awareness Guide
Cyber Crime Helpline: **1930** | cybercrime.gov.in





What Is a Digital Arrest?



The single most important fact:

There is **NO** such legal concept as “digital arrest” in Indian law. No police officer, CBI agent, judge, or RBI official will ever arrest you over a video call. No real investigation demands money through UPI, bank transfer, or cryptocurrency. If you hear the words “digital arrest” — the call is a scam. Period.

The Scale of the Problem



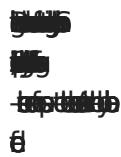
Estimated losses to digital arrest
scams in India over 18 months



Cybercrime cases registered in
India in 2023 (NCRB)



1930 Cyber Helpline operated by
I4C, Ministry of Home Affairs





How the Scam Works



1

The Hook — A Sudden Call

You receive an unexpected call, often from an international number (+92, +1, +44) or a spoofed Indian number. The caller claims to be from FedEx, DHL, customs, the CBI, the Mumbai Police, or TRAI. The script: “A parcel in your name contains drugs, fake passports, or SIM cards used in money laundering.”

2

The Authority Display

The call is transferred to a “senior officer” on Skype or WhatsApp video. You see a man in police uniform, in what looks like a real police station, with the Ashoka emblem behind him. He shows fake ID cards, fake FIR copies, and forged court orders bearing your name and Aadhaar details.

3

The Threat

Heavy charges are recited: Section 420, NDPS Act, PMLA, 10 years in jail. They claim your Aadhaar and PAN are linked to terror funding or to a high-profile case (Naresh Goyal, Jet Airways, etc.). The pressure is relentless and designed to overwhelm rational thought.

4

The Isolation

You are placed under “digital arrest” and ordered to stay on the video call at all times. You cannot tell family. You cannot leave the camera. The matter is “sub-judice.” Some victims are kept on camera for 3 hours; some for 5 days. This isolation is the most dangerous stage.

5

The Drain

You are told to transfer your funds to an “RBI escrow account” or “government verification account” for clearance — with a promise of return in 24 hours after “verification.” The money is moved through mule accounts, converted to crypto, and is gone. The calls stop. The scammers disappear.

Red Flags: How to Spot the Scam



Common Scam Scenarios in 2026

Courier Parcel Scam



Aadhaar / SIM Misuse Scam



Income Tax / Customs Scam



Bank Money-Laundering Scam





What To Do If You Receive Such a Call



✓ DO THIS

-
-
-
-
-
-
-
-
-

X NEVER DO THIS

-
-
-
-
-
-
-
-

Remember: A real Indian police officer or central agency will **always** approach you through a written notice and a physical visit, with a documented FIR number you can verify at the local police station. They will **never** demand money, OTPs, or video-call “custody”.



How to Report — Step by Step

CYBER CRIME HELPLINE

1930

Toll-free | 24x7 | All India

Operated by the Indian Cyber Crime Coordination Centre (I4C), Ministry of Home Affairs, Government of India

The Reporting Process

1

Dial 1930

A trained operator notes down the fraud details — account number, UPI ID, transaction ID, amount, date, and your basic information — and creates a complaint ticket on the National Cyber Crime Reporting Portal (NCRP).

2

Ticket escalation

The complaint is automatically escalated to the relevant banks, wallets, and merchants. You receive an SMS with an acknowledgment number and instructions to complete a detailed online complaint within 24 hours.

3

File the full complaint at cybercrime.gov.in

Log in with the acknowledgment number, complete all fields, and upload evidence: screenshots, call logs, bank statements, and any documents shared by the scammers.

4

Bank action — the golden hour

If reported within roughly 60 minutes, banks can often freeze the receiving account and stop further movement of funds. The Citizen Financial Cyber Fraud Reporting system enables real-time action between police and banks.

5

Visit your local cyber police station

Carry a printed copy of the complaint, all screenshots, bank statements, and a valid ID. Request an FIR if not already filed. Follow up regularly using your complaint number.



Understanding Your Complaint Status

Status	What it means
Provisionally Recommended for Filing	Your complaint has been received and is being assessed for filing.
Forwarded to Law Enforcement Agency	Complaint escalated to police / cybercrime unit for investigation.
Investigation in Progress	Authorities are tracking IPs, transactions, and fraudster details.
Money Successfully Blocked / Recovered	The defrauded amount has been traced and is being refunded.
Closed / No Action	Investigation could not be progressed (insufficient evidence or untraceable).



Family Safety Checklist

☐☐☐☐☐☐☐☐

Real Cases Reported in India

Mumbai — 73-year-old doctor (2025)



Delhi — elderly citizen, ED impersonation



Bangalore — software engineer





Important Contacts & Resources

Service	Contact
National Cyber Crime Helpline	1930 (24x7, toll-free)
National Cyber Crime Reporting Portal	cybercrime.gov.in
Police Emergency	112
Women Helpline	1091
Senior Citizen Helpline	14567
RBI Sachet (suspicious entities)	sachet.rbi.org.in
Report SIM-card / spoofed-call fraud (DoT)	sancharsaathi.gov.in
CERT-In (incident reporting)	incident@cert-in.org.in

Five Things to Remember

1

Digital arrest is not a real legal concept.

Indian law contains no provision authorising arrest by video call.

2

No real officer will ever ask for money.

Police, CBI, ED, RBI, and customs never request payments through UPI, bank transfer, or crypto. Ever.

3

Fear is the scam's only weapon.

Disconnect, breathe, and talk to a family member — the scam dies the moment isolation breaks.

4

The first hour matters most.

Call 1930 immediately. Banks can freeze fraudulent accounts and reverse transactions within the golden hour.

5

Awareness saves money — share it.

Talk about this guide with parents, grandparents, neighbours, and colleagues. One conversation can prevent a life-altering loss.

If you remember only one number from this guide, make it 1930.

If you remember only one website, make it cybercrime.gov.in.

If you remember only one rule, make it: **hang up.**