

Digital Arrest Scam: What It Is and What to Do

"Digital arrest" does not exist in Indian law. How the fake police, CBI and customs calls work, the signs, and the three steps to take - Stop, Think, Take action - including if you have already paid.

8 min read · Content last verified 16 September 2026 · Reviewed by Shravya M

Free awareness guide. Not legal or financial advice. <https://www.shravyadigital.com/guides/digital-arrest-scam>

CONTENTS

1. The short answer
2. What it looks like
3. How the scam works
4. Why it works: three moves
5. The signs: it's a scam if...
6. What to do: Stop, Think, Take action
7. If you already paid
8. Share this with someone older

The short answer

"Digital arrest" does not exist. No police force, CBI, Narcotics Control Bureau, Enforcement Directorate, RBI or any other agency in India arrests, questions or keeps anyone under watch over a phone or video call, and none of them asks you to pay money to "settle" a case.

The Prime Minister said it plainly in *Mann Ki Baat* on 27 October 2024: there is no system like digital arrest in the law; it is fraud, carried out by gangs of criminals.

Warning: If a caller says you are under "digital arrest", hang up. Call **1930** or report it at **cybercrime.gov.in**, and tell your family.

What it looks like

Meera, a retired teacher, gets a call. "This is courier customs. A parcel in your name has been stopped. It contains fake passports and drugs." Before she can answer, the call is "transferred" to a man in police uniform on a video call. Behind him is what looks like a police station. He shows her an "arrest warrant" with her name on it. He tells her not to hang up, not to tell anyone, and not to leave the room: she is under "digital arrest" until the investigation is over. To prove her money is clean, she must move her savings to a "verification account". It will be returned, he says, once she is cleared.

Meera's story is made up. The method is not. The Ministry of Home Affairs has described every part of it in its public alerts.

How the scam works

The Ministry of Home Affairs warned in May 2024 about a large number of complaints of intimidation, blackmail, extortion and "digital arrests" by criminals pretending to be police, CBI, narcotics officers, RBI, the Enforcement Directorate and other agencies. The calls follow a few set stories:

- **The parcel.** You sent, or are about to receive, a parcel with drugs, fake passports or other illegal items.
- **The family member.** Someone close to you has been caught in a crime or an accident and is "in custody".
- **Your account or SIM.** Your bank account, Aadhaar or mobile number has been "used in money laundering" or another crime.

Then a demand for money follows, to "settle the case", "verify your funds" or "avoid arrest".

The show can be convincing. According to the Ministry, fraudsters use studios made to look like police stations and government offices, and wear uniforms. Victims have been kept on video calls for hours or days, until they paid. The Ministry describes these as organised crimes, run by syndicates operating across borders.

Why it works: three moves

In the same *Mann Ki Baat* episode, the Prime Minister described the three moves these gangs use:

1. **They collect your personal details first.** They may know where you travelled, where your children study, or your address, so the call feels official.
2. **They create fear.** Uniforms, an office set-up, legal section numbers. The fear is meant to stop you thinking clearly.
3. **They create time pressure.** "Decide now or you will be arrested." You are not allowed to hang up, to call anyone, or to take time to think.

Every move is designed to keep you **alone, afraid and hurried**. The defence is to break all three.

The signs: it's a scam if...

- Anyone says you are under "**digital arrest**", or tells you to stay on a video call.
- An "officer" contacts you on **WhatsApp, Skype or another video app**.
- You are told **not to tell your family** or anyone else.
- You are asked to **transfer money** to "verify", "secure" or "clear" it, or to pay a fine or a "settlement".
- You are shown an **arrest warrant, court order or ID card** on a screen or in a message.
- The call comes out of nowhere about a **parcel, a SIM card, or an account** you know nothing about.

A number that looks Indian is not proof either. Fraudsters have used international calls made to look like Indian mobile numbers; the government has directed telecom companies to block them, but don't treat the number on your screen as proof of anything.

What to do: Stop, Think, Take action

These three steps come from the Prime Minister's *Mann Ki Baat* address on 27 October 2024.

1. Stop

- Don't panic. Don't do anything in a hurry.
- Don't share any personal or bank details.
- If you can, take screenshots and record the call.

2. Think

- **No government agency threatens you over the phone, questions you on a video call, or asks for money this way.**
- If a call is making you scared, that fear is itself the sign that something is wrong.

3. Take action

- **End the call.** If you're worried a real case might exist, go to or call your local police station yourself, using a number you found on your own, not one the caller gave you.
- **Call 1930**, the national cybercrime helpline, or report at **cybercrime.gov.in**.
- **Tell your family and your local police.**
- **Keep the evidence:** the numbers, video-call IDs, screenshots and any messages.

The rule: Hang up, tell someone, call 1930. A real officer never arrests you on a video call.

If you already paid

Move fast. Money that is still in the fraudster's account can sometimes be put on hold before it is moved on.

1. **Call 1930** straight away, and report at **cybercrime.gov.in**.
2. **Call your bank** using the number on your card, passbook or bank app. Ask them to stop any further payments and register a complaint. Write down the reference number.
3. **Keep everything**: screenshots, phone numbers, account numbers and UPI IDs you paid to, transaction IDs and times.
4. **Tell your family**. You have done nothing wrong: these gangs target people of every age and background.

What RBI's new rules say about calls like this

From **1 January 2027**, RBI's new customer-protection rules for banks count a payment you approved yourself **under coercion or duress** from a third party as a fraudulent transaction. A "digital arrest" call is the kind of pressure this describes. For losses of ₹50,000 or less, an individual may receive compensation of 85% of the net loss, up to ₹25,000, once in their lifetime, but **only if** they reported the fraud to **both** 1930 or cybercrime.gov.in **and** their bank within **5 calendar days**.

Your bank decides each case, and nothing is automatic. Report fast, and to both. Our free guide to [UPI and payment scams](#) explains these rules in more detail.

Warning: Anyone who calls offering to "recover" your money for a fee is running a second scam. Police and banks don't charge to recover money.

Share this with someone older

People who have never heard of this scam are the easiest to frighten with it. Forward this page, or the PDF version, to parents and grandparents, and tell them one thing:

The rule: There is no such thing as a digital arrest. Hang up and call family.

Sources

Checked against these primary sources on 16 September 2026. Rules change: if something here looks out of date, trust the source.

- Ministry of Home Affairs, "Alert against incidents of Blackmail and Digital Arrest by cyber criminals" (PIB, 14 May 2024) (<https://www.pib.gov.in/PressReleasePage.aspx?PRID=2020570>)
- Prime Minister's address, Mann Ki Baat episode 115 (27 Oct 2024) (https://www.pmindia.gov.in/en/news_updates/pms-address-in-the-115th-episode-of-mann-ki-baat/)
- Ministry of Home Affairs, "Steps taken to address the issue of digital arrest scams" (PIB, 12 Mar 2025) (<https://www.pib.gov.in/PressReleasePage.aspx?PRID=2110809>)
- RBI (Commercial Banks - Responsible Business Conduct) Third Amendment Directions, 2026 (24 Jun 2026, effective 1 Jan 2027) (<https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=13543&Mode=0>)
- National Cyber Crime Reporting Portal and helpline 1930 (<https://cybercrime.gov.in/>)