



CSAM 2026

There is no such thing as a digital arrest



Theme — Fear is the fraudster's weapon

Digital arrest is a scam in which fraudsters pose as police, CBI, customs or RBI officials on video calls. They frighten victims into transferring money.

A retired schoolteacher received a video call from a man in uniform. The caller claimed the teacher's Aadhaar had been used in a money laundering case. He kept the teacher on camera for two days and told him not to tell anyone. The teacher was then asked to break his fixed deposit and transfer Rs. 6 lakh to an RBI verification account. At the branch, an alert cashier noticed he was anxious and constantly on the phone. The Branch Manager spoke to him calmly and called his son. The transfer was stopped.

RED FLAGS

- ▲ A government official arrests or questions someone over a video call.
- ▲ The victim is told to keep the matter secret, even from family.
- ▲ Money must be moved to a safe account or a verification account.
- ▲ There is extreme urgency, threats, or fake documents sent on messaging apps.

WHAT YOU SHOULD DO

- ✓ Watch for elderly customers breaking fixed deposits in a hurry or transferring large sums to unknown accounts.
- ✓ Ask gently what the money is for, and involve the Branch Manager.
- ✓ Contact a family member where appropriate.
- ✓ Tell customers plainly that no Indian agency arrests anyone over a call.

IF YOU ARE A VICTIM

- 1 Call 1930 immediately. The first few hours matter most for freezing funds.
- 2 Register a complaint at cybercrime.gov.in.
- 3 Report the fraud call or number on Chakshu at sancharsaathi.gov.in.
- 4 Inform the bank so that the beneficiary account can be flagged.

GUIDELINES TO FOLLOW

- Brief every branch at the start of the month on the impersonation methods currently in use in your area.
- Where a customer aged 60 or above asks for a large transfer or a premature deposit closure, have a second officer speak to them before it is processed.
- Keep a short printed script at the counter for staff to use when a customer appears to be acting under instruction from a caller.
- Record every such case, whether or not money was lost, and circulate the pattern to all branches.

A calm conversation at the counter can save a customer's life savings.



CSAM 2026

AI tools are helpful, but customer data must stay inside the bank

Theme — Smart tools, safe hands



AI chatbots and writing tools save time. However, anything typed into a public AI tool may be stored on servers outside the bank's control.

A clerk at a bank's head office wanted to draft recovery letters quickly. He pasted a list of 300 overdue KCC borrowers into a free online chatbot, including their names, account numbers and Aadhaar numbers. The data left the bank permanently. The same week, the IT cell received a perfectly written email, apparently from the CBS vendor, asking for VPN credentials for an urgent patch. It had been written using AI. The IT officer verified by phone and found it was fake.

RED FLAGS

- ▲ Customer or bank data is pasted into public AI tools.
- ▲ AI browser extensions or apps are installed without IT approval.
- ▲ Flawless, urgent emails or voice messages ask for credentials or payments.
- ▲ AI-generated content is used without checking.

WHAT YOU SHOULD DO

- ✓ Board and senior management: approve an AI usage policy for the bank.
- ✓ IT and CISO: publish a list of approved tools, block unapproved AI sites and extensions, and apply controls that stop sensitive data leaving the network.
- ✓ All staff: never enter customer data, passwords, audit reports or internal notes into public AI tools.
- ✓ All staff: verify any unusual request through a known phone number.

IF YOU ARE A VICTIM

- 1 Inform the CISO or IT-in-charge immediately.
- 2 Assess whether the incident is reportable to CERT-In within 6 hours, and inform NABARD.
- 3 Where there is financial loss, report at 1930 or cybercrime.gov.in.

GUIDELINES TO FOLLOW

- Maintain a list of approved tools, name an owner for it, and review it every quarter.
- Classify the bank's data and state plainly which classes may never be typed into any external tool.
- Verify every payment or credential instruction by calling back on a number already held on record, whatever the instruction looks or sounds like.
- Keep a record of approved-tool use for official work so that it can be reviewed like any other system activity.

Use AI wisely. Keep the bank's data inside the bank.

Report cyber fraud immediately
cybercrime.gov.in · sancharsaathi.gov.in

1930



CSAM 2026

Fingerprints, SIM cards and fake KYC links

Theme — Protect what identifies you



Fraudsters now target the things that prove who we are: fingerprints, mobile numbers and KYC details.

An SHG member found Rs. 18,000 withdrawn through AePS at a micro-ATM she had never visited. Weeks earlier, her fingerprint had been taken on a device for a so-called ration verification. A small trader's phone suddenly lost network, and by morning his account was empty because a fraudster had obtained a duplicate SIM. A farmer received an SMS saying that his KYC expires today, with a link. He clicked it and entered his details.

RED FLAGS

- ▲ Someone collects fingerprints outside official centres.
- ▲ The mobile signal is lost suddenly and for a long time.
- ▲ An SMS or call asks for a KYC update through a link.
- ▲ AePS debits appear without any visit to a Bank Mitra or micro-ATM.

WHAT YOU SHOULD DO

- ✓ Lock Aadhaar biometrics through the official UIDAI website and unlock them only when needed.
- ✓ Update KYC only at the branch. The bank never sends KYC links.
- ✓ If the mobile network is lost unexpectedly, contact the mobile operator and the bank at once.
- ✓ Keep SMS alerts active for all transactions.
- ✓ Display these tips at the branch counter in the local language.

IF YOU ARE A VICTIM

- 1 Call 1930 or report at cybercrime.gov.in.
- 2 Inform the bank at the earliest, ideally within 3 working days, so that the customer's liability stays limited.
- 3 Lock Aadhaar biometrics immediately.
- 4 Check mobile connections issued in your name on sancharsaathi.gov.in.

GUIDELINES TO FOLLOW

- Make biometric locking part of the standard account opening conversation, and help the customer do it at the counter.
- Apply a cooling-off period on high-value and channel transactions after any change in the registered mobile number.
- Reconcile the AePS and micro-ATM activity of every business correspondent weekly, and question volumes that do not match the location.
- Keep transaction alerts live on every account and treat a failure in the alert system as an incident, not a service issue.

Your fingerprint, SIM and KYC are keys to your account. Guard them like cash.

Report cyber fraud immediately
cybercrime.gov.in · sancharsaathi.gov.in

1930