FREE GUIDE · 2026 EDITION

5 Ways Criminals Are Using AI Against Your Family Right Now

Know the tactics. Know what to do. Share this before it happens.

Mayank Jain · mayankjain.io

Two of the five scams in this guide are entirely new — they simply could not have existed before AI. The other three are not new ideas: authority impersonation, romance fraud, and fake customer service all existed long before AI. But AI has transformed them — making them more convincing, more personalised, and scalable to millions of victims at once. Each scam is labelled so you know which is which.

You don't need to become a tech expert. You just need to know what to look for.

SCAM 1 OF 5

■■ AI Voice Cloning — Audio Impersonation

● AI-NATIVE — This scam could not exist without AI

WHAT IS IT?

Using just 10–30 seconds of audio from a social media video or voicemail, criminals clone a voice and call a family member pretending to be someone they love in an emergency — "I've been in an accident," "I'm in hospital," "I need money right now." This is audio-only: a phone call or WhatsApp voice note. The voice sounds identical. The panic feels real. The money is gone before anyone stops to think.

Real Example

A Delhi family received a call that sounded exactly like their son studying in Pune — saying he had been in a road accident and needed Rs. 50,000 immediately for hospital admission. The voice had been cloned from videos on his Instagram. The family transferred the money before it occurred to them to call him directly.

REMEMBER THIS

1. Agree on a family code word right now — one word only your family knows. Ask for it on any suspicious call. No code word means hang up.

2. Always hang up and call back on a number you already have saved. Never trust the number that called you.

WARNING SIGNS

- Extreme urgency — "You must send money right now"
- Request for payment via UPI, wire transfer, or gift cards
- Caller insists you keep it secret from other family members

HOW TO PROTECT YOURSELF

- Hang up and call back on a number you already have saved — never trust the number that called
- Ask for the family code word — if they don't know it, it's not them
- Never send money based on a single call without speaking to one other family member first

---

SCAM 2 OF 5

■ The "Digital Arrest" Scam — AI-Powered Authority Fraud

● **AI-AMPLIFIED — This scam existed before. AI made it faster, smarter, and industrial-scale.**

WHAT IS IT?

You receive a call — or a video call — from someone claiming to be a police officer, CBI agent, customs official, or court representative. They tell you that you are under "digital arrest": you must stay on the call, cannot hang up or speak to anyone, and must pay immediately to resolve the matter. The voice, the uniform on screen, and the official-looking documents they send over WhatsApp are AI-generated. Authority fraud existed before AI — AI added the convincing voice, the fake video, and the scale to run thousands of calls simultaneously.

Real Example

A Mumbai professional was kept on a video call for six hours by someone in a "CBI officer" uniform with a fabricated official backdrop. AI-generated court documents arrived over WhatsApp, and Rs. 8 lakh was paid to "settle" a money laundering case. Prime Minister Modi warned the nation about "digital arrest" by name in his Mann Ki Baat broadcast — this scam is that widespread.

WARNING SIGNS

- A government official contacts you via WhatsApp or a personal call
- You are told you cannot hang up or contact anyone — "digital arrest"
- They demand immediate payment to avoid arrest or case filing

HOW TO PROTECT YOURSELF

- No government agency in India ever arrests anyone over a video call — hang up immediately
- Call a family member, then call the agency on their official number to verify
- Report to 1930 — the National Cybercrime Helpline

SCAM 3 OF 5

■ Deepfake Video Calls — Visual Impersonation

● **AI-NATIVE — This scam could not exist without AI**

WHAT IS IT?

Where voice cloning fakes audio, deepfakes go further — generating realistic live video of a real person saying things they never said, using only publicly available photos. Criminals use this in video calls on WhatsApp, Zoom, or Teams to impersonate family members, bosses, or officials. When you can see the face and hear the voice, almost no one questions it.

Real Example

A Hong Kong company transferred $25 million after criminals used deepfake video in a conference call — every person on screen, including the CFO, was AI-generated. The same tactic is now reaching families: a "video call from your son" asking urgently for money.

WARNING SIGNS

- A financial request arrives only via a video call or WhatsApp video
- The face looks slightly "off," movements are stiff, or audio doesn't quite match
- The person refuses to switch to a voice call or meet in person

HOW TO PROTECT YOURSELF

- Use the family code word — even on video calls
- Ask them to do something spontaneous: wave both hands, touch their ear
- Hang up and call back on a saved number before sending anything

---

SCAM 4 OF 5

■ Romance & Investment Fraud — "Pig Butchering"

● **AI-AMPLIFIED — This scam existed before. AI made it faster, smarter, and industrial-scale.**

WHAT IS IT?

Romance scams and investment fraud both existed before AI — but they have always gone hand in hand, and this combination even has a name: "pig butchering." The romance is not accidental; it is deliberate trust-building to make the investment ask believable later. AI transformed the scale: one criminal can now run hundreds of these relationships simultaneously, 24/7, in any language, without fatigue.

Real Example

A retired engineer in Bangalore lost Rs. 34 lakh to someone he met on LinkedIn who posed as an investment advisor. After six weeks of daily messages and a convincing fake investment platform, the money and the contact vanished. Investigators confirmed the entire persona was AI-managed.

WARNING SIGNS

- Someone you've never met in person is unusually attentive and quick to become close
- Always has an excuse not to video call, or calls are very brief
- Conversation eventually steers toward a "can't miss" investment opportunity

HOW TO PROTECT YOURSELF

- Never send money to someone you have not met in person
- If investment returns sound too good to be true, they are
- Tell a family member before making any financial decision with someone you met online

---

SCAM 5 OF 5

■ Fake AI Customer Service & IT Support

● **AI-AMPLIFIED — This scam existed before. AI made it faster, smarter, and industrial-scale.**

WHAT IS IT?

Fake customer service existed before AI — but it required people to answer phones. Now AI chatbots impersonate banks, telecom providers, electricity boards, and government departments at any hour, with no human involved. It also happens inside companies: a message appearing to be from your IT department or HR can be an AI-generated fake. The conversation feels real until they ask for your OTP or device access.

Real Example

A Pune resident received an SMS saying his electricity connection would be cut in two hours. He called the number in the message — an AI chatbot posing as the electricity board asked for his account number and OTP to "process the payment." His bank account was drained before the two hours were up.

WARNING SIGNS

- You found the number in an SMS, WhatsApp message, or Google search — not on your bill or card
- They ask for your OTP, PIN, or account number to "verify" your identity
- They ask you to install an app to "help resolve" your issue

HOW TO PROTECT YOURSELF

- Always use numbers printed on your bill, card, or the official app — never from a message
- No real bank, utility, or company will ever ask for your OTP — end the call immediately
- Never install any app at the request of someone who called or messaged you

---

You Now Know What Most People Don't.

The single most powerful protection against AI scams is awareness. Share this guide with your parents, your partner, your children. A five-minute conversation about these five scams — and agreeing on a family code word — could save your family from a devastating loss.

For more free guides on protecting your phone, email, and family, visit mayankjain.io

---

Want more guides like this?

Sign up free to receive new guides, checklists,
and plain-language tips straight to your inbox.

mayankjain.io

No spam. Unsubscribe any time.