SECURING HUMAN FOUNDATION

⚠ Beware of AI fraud

Awareness is protection

A familiar voice, a familiar face — yet it could be a fraudster!

With AI, fraudsters can fake a loved one's voice, face and photos in minutes. Verify first, then trust.



How fraudsters use AI

Voice-clone calls

A few seconds of audio from social media is enough to copy a loved one's voice — then comes the call: "I've had an accident, send money now."

Deepfake video calls

They fake the face of someone you know, your boss or a police officer on a video call and ask for money or secrets.

Photo morphing and blackmail

They turn ordinary social media photos into obscene images with AI and demand money, threatening to defame you.

Uploading photos to AI apps

Photos, face data and phone permissions given to free "AI photo editor", "cartoon look" or trending apps can be misused.

Fake celebrity investment ads

Deepfake videos of famous politicians, cricketers or business leaders lure you into "guaranteed profit" trading apps.

AI-written fake messages

Error-free AI-written emails, messages and fake "customer care" chatbots look completely genuine, so people trust them.

Been cheated? Dial immediately 1930 | www.cybercrime.gov.in

SECURING HUMAN FOUNDATION

Stay safe

Create a family "safety password"

AI can fake a voice and a face — but not your family's secret word!

1. **Decide on it today** — a secret word (e.g. "green umbrella") that's nowhere on social media.
2. **Share it only in person** — never on WhatsApp, SMS or a call.
3. **A call asking for money? Ask for the password first.** No password — hang up.
4. **Teach elders and children especially.** If in doubt, change it at once.

How to protect yourself from AI fraud

- ✓ **Hurry and fear = danger.** Hear "send money right now"? Be on alert.
- ✓ **Verify on video calls.** Ask them to turn their head — deepfakes glitch.
- ✓ **Keep profiles private.** Don't post voice videos or children's photos publicly.
- ✓ **Never upload** personal photos or Aadhaar/PAN to unknown AI apps.
- ✓ **Turn on WhatsApp two-step verification** so your account can't be hijacked.
- ✓ **Ignore celebrity investment ads.** Invest only through SEBI-registered firms.
- ✓ **Blackmailed? Don't pay.** It's not your fault — report it right away.
- ✓ **Police never do "digital arrest".** Hang up on such video calls.

Cheated or blackmailed? Do this immediately

National Cyber Crime Helpline

1930

24 × 7 · Free

National Cyber Crime Reporting Portal

www.cybercrime.gov.in

File a complaint online

1. **Call 1930 at once.** Reporting in the first hour can stop the money.
2. **Keep evidence** — numbers, screenshots, recordings, chats.
3. **File a complaint** at cybercrime.gov.in.
4. **Report fake photos/videos** on the app to get them removed.

Report fraud calls / messages: www.sancharsaathi.gov.in (Chakshu) · **Stop private or morphed photos spreading:** www.stopncii.org