AI-Based Scams

Voice cloning, deepfake videos and AI-written messages - and simple checks that still work.

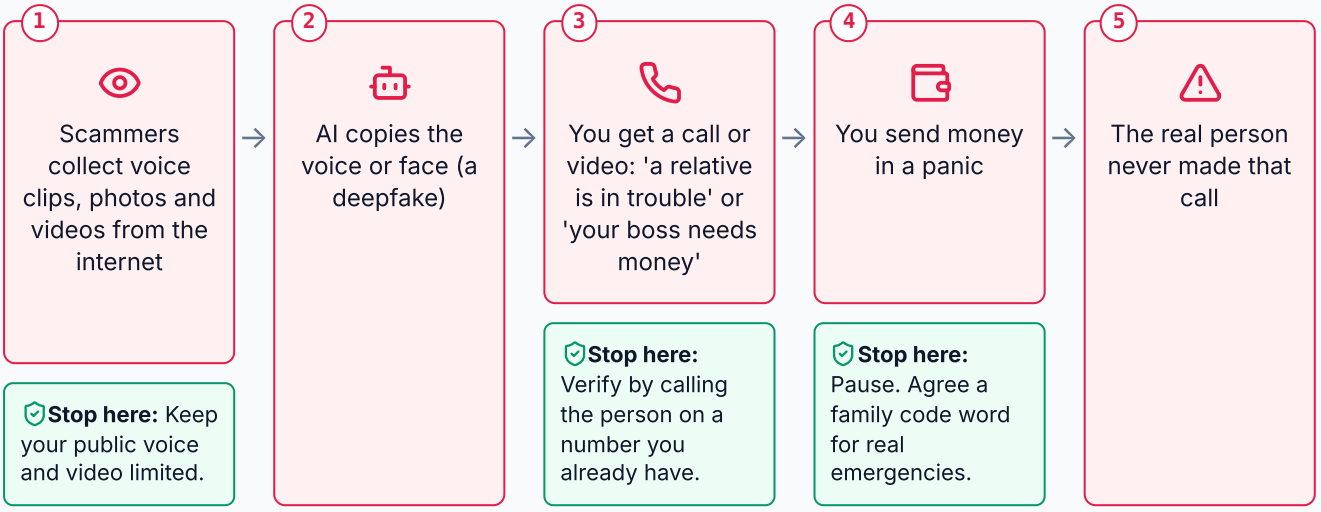
Lost money in an online fraud? Call 1930 right away and report at cybercrime.gov.in.

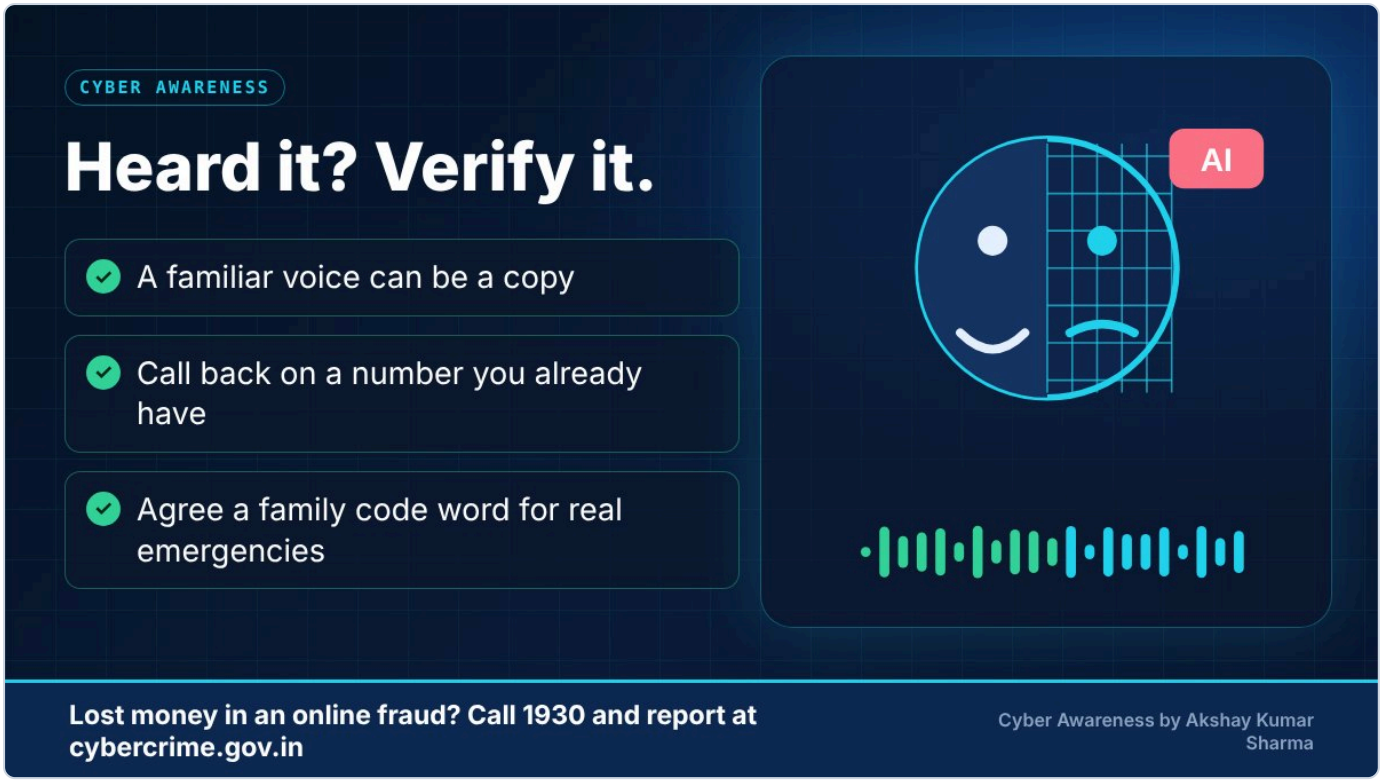
What it is

AI tools make it easier to copy someone's voice, create realistic fake videos, and write convincing messages in any language. A scammer may call in what sounds like a relative asking for urgent money, or share a fake video of a public figure promoting an investment. The technology is new, but the trick is old: trust plus urgency.

How it works - and where you can stop it

Red boxes show what the attacker does. Green boxes show where you can break the chain.





Common warning signs

- ⚠ An urgent call or voice note from a 'relative' or 'friend' asking for money, from a new number.
- ⚠ A video or audio of a famous person endorsing a scheme or giveaway.
- ⚠ Messages that are perfectly written but ask for unusual actions or payments.
- ⚠ Video calls where the person's face or lip movement looks slightly off, or the call quality is conveniently poor.
- ⚠ Pressure not to verify through other means.

Practical prevention tips

- Agree on a family 'safe word' or ask a question only the real person could answer.
- Hang up and call the person back on their known number before sending money.
- Be careful with investment promotions featuring celebrities. Verify through official channels.
- Limit public voice and video samples, and keep social profiles private.
- Treat urgency as a warning sign, regardless of how real the voice or face seems.

Risky habit vs safe habit

RISKY	SAFE
✕ Trust a familiar voice on its own	✓ Verify through a second channel
✕ Send money at once for an 'emergency'	✓ Pause and call the person directly
✕ Believe a celebrity video that promotes an investment	✓ Check the official channels of that person or company
✕ Upload your photos to unknown AI apps	✓ Use trusted apps and read their privacy terms

What to do if it happens

1. Stop all payments and verify using another channel.
2. Report the call, message or fake profile on the platform and to Sanchar Saathi if it came by phone.
3. Call the cyber crime helpline 1930 immediately - reporting quickly gives the best chance of stopping the transfer.
4. Also file a complaint on the National Cyber Crime Reporting Portal (cybercrime.gov.in).
5. Inform your bank or payment app right away and ask them to block the card, account or UPI ID involved.
6. Keep screenshots, transaction IDs, phone numbers, UPI IDs and chat history. Do not delete anything.
7. Change passwords of affected accounts and do not share OTPs or PINs with anyone who calls you afterwards offering to 'recover' your money.

Official reporting resources

- National Cyber Crime Reporting Portal (cybercrime.gov.in) - https://cybercrime.gov.in/
- Cyber crime helpline 1930 (for financial cyber fraud) - 1930
- Sanchar Saathi - report suspected fraud calls/messages (Chakshu) - https://sancharsaathi.gov.in/
- CERT-In (Indian Computer Emergency Response Team) - https://www.cert-in.org.in/

Never share your banking password, OTP, UPI PIN, card CVV or full card number with anyone - not even someone claiming to be from your bank, police or a government office. This website will never ask for them.

This website is an educational resource. It is not an official government reporting portal or an emergency response service. If you are a victim of cyber fraud, report it through the official channels listed on each page.