

Recognize AI Generated Cyber Scams

A SAFETY GUIDE

We live in a world where the digital and real often blur. As technology evolves, unfortunately, so do the ways people misuse it. With time, as cyber fraudsters adapt to evolving digital habits, they now exploit AI tools like voice cloning and deepfakes to craft convincing fake messages, videos, and calls. These scams are designed to manipulate your trust, emotions, and sense of urgency. Understanding what they are, how they operate, and the steps to stay safe is the best way to protect yourself.

FAMILY EMERGENCY SCAM

IMAGINE

Late at night, your phone rings. It's your son's/daughter's voice, frantically calling out:

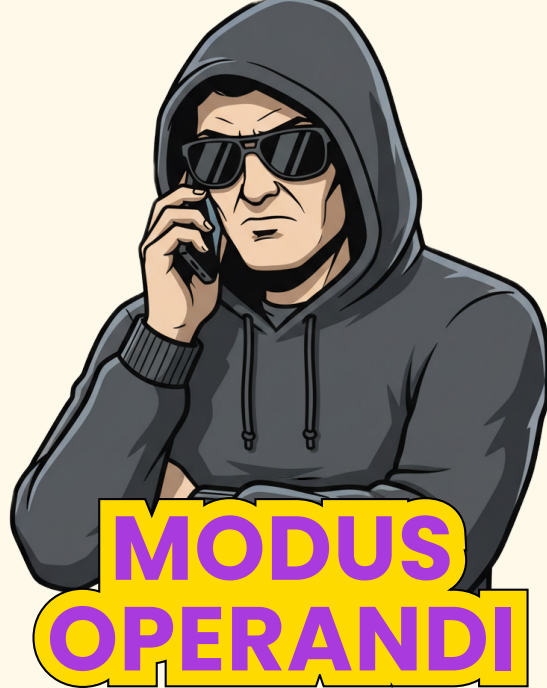


WHAT IS IT?

This is a **Deepfake Family Emergency Scam**, wherein fraudsters use AI-generated voices or videos to imitate friends, family or anyone close to you. Scammers create a sense of panic with the hope that you will act before verifying anything about the authenticity of any specific demand.

HOW DOES THIS SCAM WORK?

- Scammers crop voice/video clips from social media (WhatsApp status, Instagram reels or DMs, YouTube) and use inexpensive AI tools to clone voice or generate a deepfake video that mimics tone, accent, and speech patterns.
- Initiates a late-night/odd-hour call or WhatsApp message with parents, spouse or a family member, often from a spoofed or unknown number, to increase surprise and lower scrutiny.
- Uses an urgent script ("I'm in trouble," "Police/hospital here," "Don't tell anyone") to create panic and pressure for secrecy.
- Adds credibility with personal details taken from profiles (names, places, friends) to make the plea more believable.
- Demands for immediate payments and use irreversible payment methods like UPI transfer or asks for OTPs and banking details.
- Escalates pressure if the victim hesitates by creating fake authority voices, background noise or releases additional distress voice clips.
- Gives a short deadline to comply or threatens with dire consequences.
- Extracts funds quickly and launders them through multiple wallets takes out.



BEWARE OF THESE SIGNS

- The voice sounds right but the tone or phrasing feels slightly off.
- They push hard for instant payments or OTPs.
- They insist, "Don't tell anyone!", that's your biggest warning sign.

- Listen carefully during calls for odd pauses or unnatural phrasing, and treat anything that feels "off" as suspicious.
- First and foremost, ask the caller to make you speak again with the claimed person in custody (which most likely will never happen as there is no real person involved!)
- If the caller hesitates, ask him/her to answer 'secret question' or confirm any 'unique identity marks' on their behalf known only to you and the person in custody.
- Before you react to any money requests, initiate contact with the said person by calling them directly.
- If unable to establish direct contact, then cross-verify details by calling another family member or a friend to confirm the situation.
- Do not entertain any money transfer requests and insist on a verifiable process (call police or request to meet in person).
- Take your time during the interaction, slow it down, pause, and verify before taking any action.



POINTS TO REMEMBER

- Pause, think and then react.
- Use a secret word/emoji with your family to confirm identity.



If you fall victim to a cybercrime, act immediately instead of waiting for the situation to worsen.

Call 1930 right away for cases involving financial fraud or **visit cybercrime.gov.in** to register your complaint online.

Check out other AI Generated Cyber Scams in our CSAM infographic series.

Fake Customer Support AI Chatbots

AI Dating/Romance Scam

AI-Based Investment Scam

SUPPORTED BY

