

# Recognoze 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.

**Here's a compilation of emerging AI-driven scams that you should watch out for.**

## FAMILY EMERGENCY SCAM

### JUST 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 or take out cash to avoid traceability.

### 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.

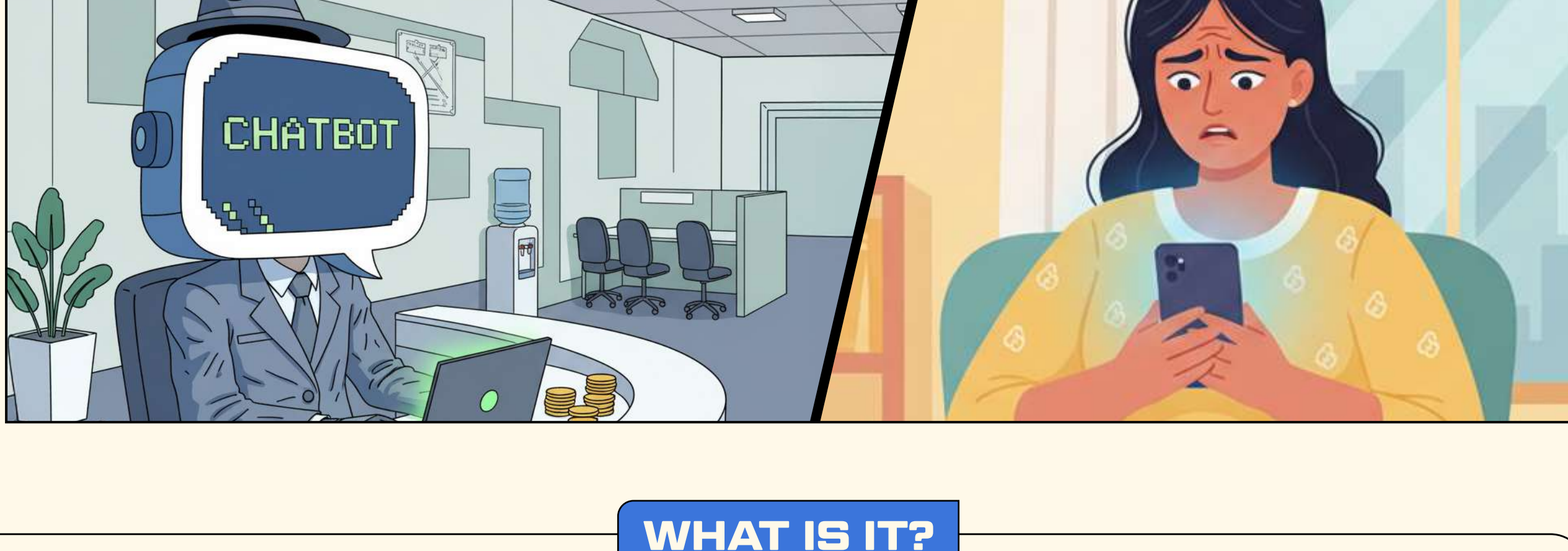
### POINTS TO REMEMBER

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

## FAKE CUSTOMER SUPPORT AI CHATBOTS

### JUST IMAGINE

You tweet about a payment issue with your bank. Minutes later, a "customer care" account replies with a link. The logo looks real, the tone polite.



### WHAT IS IT?

This is a **Fake Customer Support AI Chatbot** where fraudsters use AI-powered bots to instantly track complaints online. They mimic official customer care handles or create fake chatbots on WhatsApp/Telegram to trick users into sharing sensitive details.

### HOW DOES THIS SCAM WORK?

- Scammers set up fake "Customer Care" pages, bot accounts, or look-alike websites with toll-free numbers.
- They copy brand logos, colors and legal text so the fake page looks authentic.
- AI bots scan for keywords like "refund" or "transaction failed" and reply instantly with a fake helpline or link.
- They clone real website and create look alike domain (for example, replacing one letter in the URL), while copy brand colors, logos, and even legal disclaimers so victims don't suspect they're on a fake page.
- When victims call, AI-powered voices or scripted agents greet them politely, give fake ticket IDs, and even play hold music. This builds trust and convinces people they're talking to genuine support staff.
- They ask for account/UPI/card details, OTPs, or ask you to install remote-access apps for "verification."
- They create a feeling of urgency and push victims into quick action by saying things like "Your refund will expire soon," or "Your chat will be blocked if you don't verify immediately."
- Once details are shared or remote access is given, we quietly tap money, redirect UPI transfers, or save credentials for later misuse.
- After stealing funds or data, they disconnect numbers, delete accounts, and vanish to avoid tracing.

### BEWARE OF THESE SIGNS

- Only engage through official verified handles or apps.
- Bookmark your bank's genuine site for direct use.
- Completely ignore chatbots offering outrageous deals and demanding immediate action or sensitive details to claim them.

- Always be cautious of new or unverified "support" handles or phone numbers.
- Don't trust instant responses. Real customer care doesn't usually DM links.
- Fake pages may look convincing, so double-check the URL and account details carefully.
- Never click on links sent in direct messages or social media replies.
- If you call a number found online, hang up and call the official helpline from the company's app or website.
- Never share your OTP, PIN, or full password with anyone claiming to be support.
- Do not download or install remote-access or screen-sharing apps for "technical help."
- If someone pressures you with urgency, pause and verify before taking any action.
- If you accidentally share details, contact your bank or payment app immediately to secure or block your account.

### POINTS TO REMEMBER

- Look out for generic names like "Bank Helpline 24/7."
- Avoid clicking on direct links in DMs asking for verification.
- Stay cautious of overly quick replies (bots work instantly, real humans take time).

### SUPPORTED BY

