CYBER SURAKSHA DRIVE

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

Recognize AI Generated Cyber Scams

A SAFETY GUIDE

Recognize AI Generated Cyber Scams

A SAFETY GUIDE

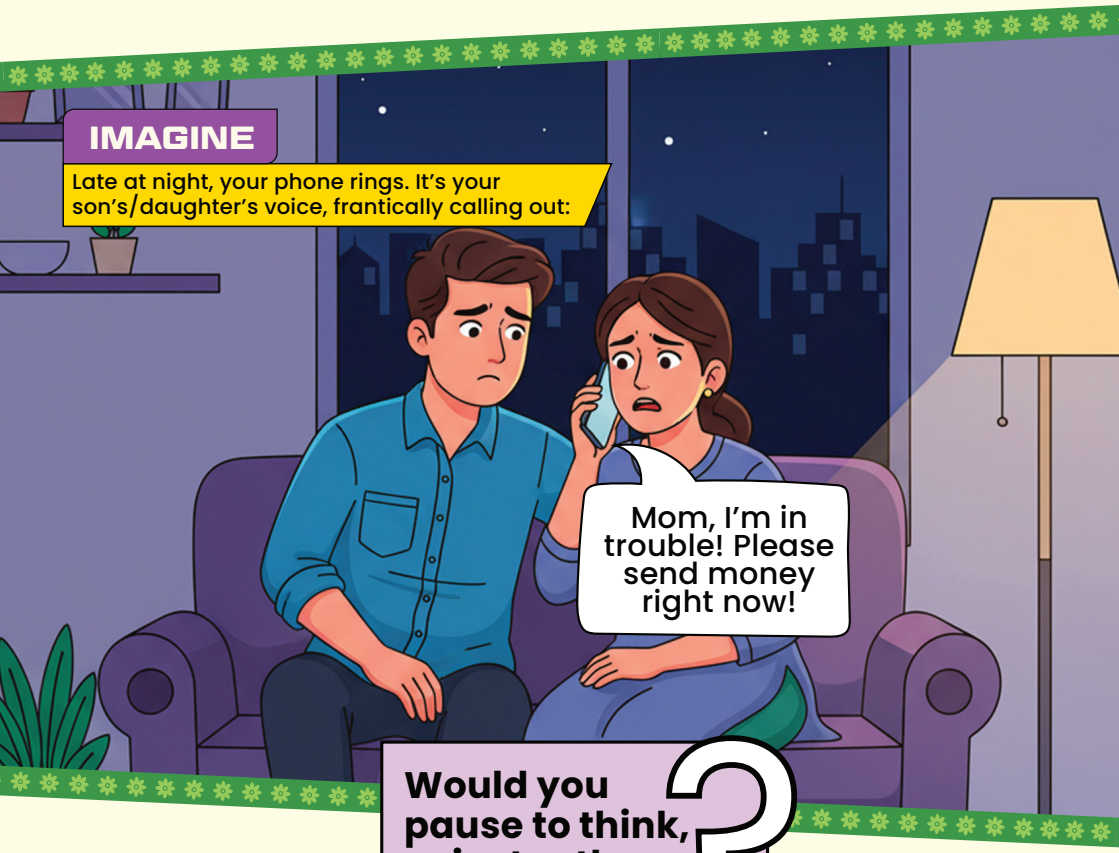
We live in a world where the digital and real often blur. As technology evolves, unfortunately, so do the ways people misuse it. With time, as cyber fraudsters adapt to evolving digital habits, they now exploit AI tools like voice cloning and deepfakes to craft convincing fake messages, videos, and calls. 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.

This guide will help you understand how AI-driven scams work and how to protect yourself from falling victim. Common types of AI-enabled scams covered in this guide include:

1. Family Emergency Scam
2. Fake Customer Support AI Chatbots
3. AI Dating/Romance Scam
4. AI-Based Investment Scam

1.

FAMILY EMERGENCY SCAM

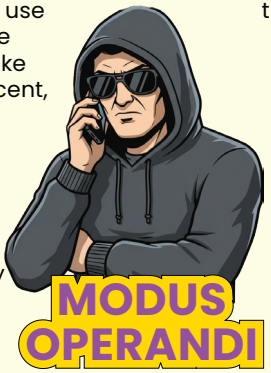


Would you pause to think, or instantly panic?

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?



1. 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.
2. 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.
3. Uses an urgent script ("I'm in trouble," "Police/hospital here," "Don't tell anyone") to create panic and pressure for secrecy.
4. Adds credibility with personal details taken from profiles (names, places, friends) to make the plea more believable.
5. Demands for immediate payments and use irreversible payment methods like UPI transfer or asks for OTPs and banking details.
6. Escalates pressure if the victim hesitates by creating fake authority voices, background noise or releases additional distress voice clips.
7. Gives a short deadline to comply or threatens with dire consequences.
8. 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.

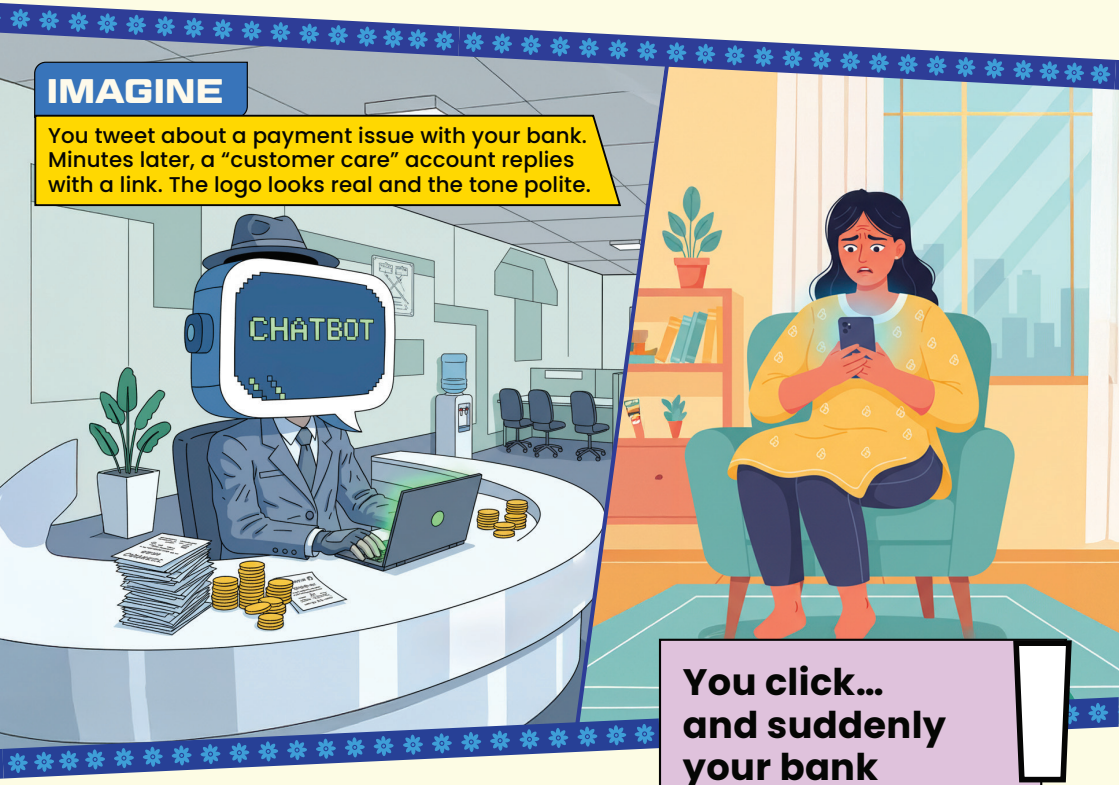
1. Listen carefully during calls for odd pauses or unnatural phrasing, and treat anything that feels “off” as suspicious.
2. First and foremost, ask the caller to make you speak again with the claimed person in custody (which most likely will never happen as there is no real person involved!)
3. If the 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.
4. Before you react to any money requests, initiate contact with the said person by calling them directly.
5. If unable to establish direct contact, then cross-verify details by calling another family member or a friend to confirm the situation.
6. Do not entertain any money transfer requests and insist on a verifiable process (call police or request to meet in person).
7. 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.

2.

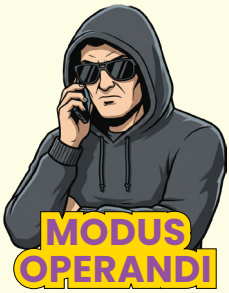
FAKE CUSTOMER SUPPORT AI CHATBOTS



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 platforms like Whatsapp/Telegram to trick users into sharing sensitive details.

HOW DOES THIS SCAM WORK?



1. Scammers set up fake "Customer Care" pages, bot accounts, or look-alike websites with toll-free numbers.
2. They copy brand logos, colors and legal text so the fake page looks authentic.
3. AI bots scan for keywords like "refund" or "transaction failed" and reply instantly with a fake helpline or link.
4. They clone a real website/real websites and create look alike domain (for example, replacing one letter in the URL), while copying brand colors, logos, and even legal disclaimers so victims don't suspect they're on a fake page.
5. 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.
6. They ask for account/UPI/card details, OTPs, or ask you to install remote-access apps for "verification."
7. 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."
8. Once details are shared or remote access is given, scammers quietly tap money, redirect UPI transfers, or save credentials for later misuse.
9. 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.

1. Always be cautious of new or unverified support handles or phone numbers.
2. Don’t trust instant responses. Real customer care doesn't share links via DM.
3. Fake pages may look convincing, so double-check the URL and account details carefully.
4. Never click on links sent in direct messages or social media replies.
5. If you call a number found online, hang up and call the official helpline from the company’s app or website.
6. Never share your OTP, PIN, or full password with anyone to be from customer support.
7. Do not download or install remote-access or screen-sharing apps for “technical help.”
8. If someone pressures you with urgency, pause and verify before taking any action.
9. 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).

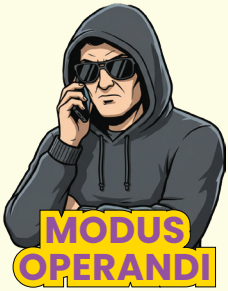
3.

AI DATING/ ROMANCE SCAM

WHAT IS IT?

This is an **AI Dating/Romance Scam** where fraudsters create fake profiles or impersonate users on dating apps and social media. They use AI-generated images, conversations, and even voices to build emotional trust. Once the relationship feels real, they invent emergencies or personal crises to extract money or personal data.

HOW DOES THIS SCAM WORK?



1. Scammers create realistic profiles using AI-generated images, videos, and bios tailored to appeal to the victim.
2. They may use AI-generated audio or video to maintain a consistent and believable presence during interactions.
3. AI chatbots simulate conversations, responding instantly and intelligently to keep victims engaged and allow the scammer to target multiple people at once.
4. Scammers quickly express affection or build emotional trust through compliments, shared interests and empathetic messages.
5. Scammers analyze the victim's profile and interactions to customize messages and scenarios for stronger emotional manipulation.
6. Scammers create emergencies, travel issues, medical expenses, or business problems to pressure victims into sending money or sharing sensitive information.
7. They ask for UPI transfers, bank details, gift cards, or access to accounts under the appearance of trust.
8. Over time, they continue nurturing the relationship to push for more funds or personal information until the victim becomes suspicious or exhausted.
9. Scammers use AI to create networks of fake personas, such as friends or colleagues, to "validate" the scammer's story and make the deception more believable.
10. After committing fraud, scammers delete profiles, block victims, and vanish from all communication channels to avoid any detection.

BEWARE OF THESE SIGNS

- Keep emotions in check when chatting online.
- Trust your instincts and disengage if something feels off.
- If money is requested, end the conversation immediately and don't engage further.

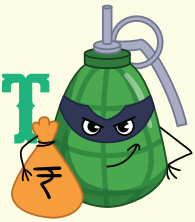
1. Be cautious of profiles that seem "too perfect" or match your interests unusually closely.
2. Take your time to verify the person and avoid rushing into emotional intimacy or sharing personal information, especially financial details.
3. Never send money or share account details, even if the person appears trustworthy.
4. Be skeptical of sudden crises or urgent requests for financial help.
5. Watch for inconsistencies in stories, photos, or conversation patterns.
6. Notice if the person consistently avoids in-person meetings or video calls, often giving logistical excuses.
7. Don't fall for traps like unsolicited declarations of love or deep affection early in the relationship.
8. If you encounter a potential scam, report it to the dating platform app.
9. Preserve screenshots, messages, and other communication if you suspect fraud for evidence.

POINTS TO REMEMBER

- Beware of profiles with AI-generated or stock-like photos that appear unrealistically perfect.
- Avoid sharing money, gifts, or personal financial details with anyone you've just met online.
- Notice if someone forms an emotional connection too quickly or declares love unusually early.
- Question inconsistent stories, repeated excuses for not meeting, or pressure to act immediately.

4.

AI-BASED INVESTMENT SCAM



IMAGINE

You see a video on social media of a respected business leader or a convincing personality endorsing a new AI trading platform.

You click, sign up, deposit a small amount, then start seeing profits in your dashboard.

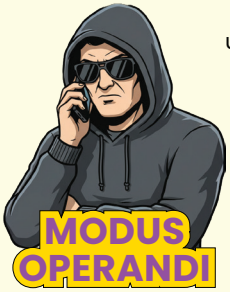
Before you know it, you're asked to invest more or pay processing / clearing/regulatory fees to withdraw.

When you finally ask for your money, the platform disappears and the customer support vanishes.

WHAT IS IT?

This is an **AI-Based Investment Scam** that exploits the growing hype around crypto trading and AI-based algorithmic trading. Fraudsters promote fake AI-driven investment platforms or trading bots that promise extraordinarily high, low-risk returns. In reality, these systems are deceptive, engineered to entice, trap, and drain investors of their money. Often, scammers use deepfake videos, clone celebrity endorsements, and fabricate profit dashboards to appear credible and legitimate.

HOW DOES THIS SCAM WORK?



1. Scammers promote fake AI-based trading platforms through social media ads featuring celebrity faces or endorsements.
2. They promise zero risk and up to 100% monthly returns to attract quick investments.
3. To look legitimate, they post fake media coverage and testimonials copied from real sources.
4. Victims are invited to start with small test amounts in the form of 'free tokens' on fake dashboards to show steady profits to build trust and confidence.
5. Once convinced, victims are urged to invest larger sums with the false urgency of adding tax, regulatory, or processing fees before any withdrawal.
6. Funds are routed through multiple digital wallets to erase trails.
7. When victims try to withdraw, they face sudden account freezes or new compliance demands.
8. The website and customer support vanish or reappear under a new name, leaving victims without any way to recover their money.

BEWARE OF THESE SIGNS

- Claim of guaranteed returns or no risk guarantee.
- Requests to pay extra fees before withdrawal.
- Dashboards showing unusually consistent or extraordinary profits.
- Unverified or unregistered platform with no trace of regulatory oversight.

1. Check if the investment firm is registered with a regulator like SEBI or any recognized securities authority.
2. Look up independent reviews, user complaints, and scam alerts about the platform.
3. Avoid any platform offering guaranteed, risk-free, or extraordinary returns.
4. Deepfake videos and fake endorsements are common; confirm from the celebrity's verified page or news sources.
5. Genuine investments never pressure you to act fast or deposit immediately.

POINTS TO REMEMBER

- If it sounds too good to be true, it probably is.
- Fraudsters use buzzwords like AI or quantum-based trading to sound credible, don't fall for the jargons.
- Safe investments never create urgency; genuine platforms give you time to think, while scams rush you to act.

Cybercrime Redressal Must Follow Steps

Call 1930 within the Golden Hour

If you fall victim to a financial cyber scam, **quickly call 1930** and **report your case within the first hour of the incident** also known as the Golden Hour. Acting fast can significantly increase the chances of recovering your money.

Report the Cybercrime

Always report the incident on the National Cybercrime Reporting Portal (NCRP) at **www.cybercrime.gov.in**. Filing an official complaint helps initiate proper investigation and resolution.

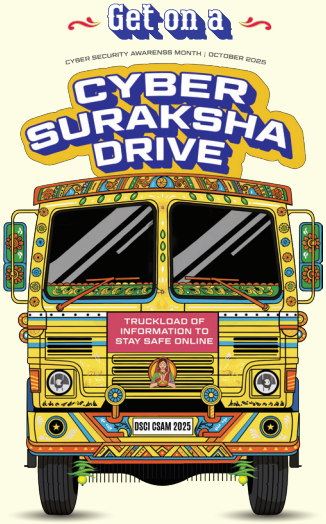
If online reporting is not possible, **visit your nearest cybercrime police station** to lodge the complaint.

Explore Other Awareness Content

English Posters

Hindi Posters

Thematic Screensaver



Awareness Videos

Scan me to explore


CYBER SURAKSHA DRIVE
SUPPORTED BY:
CRED
HDFC BANK
IIFL FINANCE
Kempegowda INTERNATIONAL AIRPORT BENGALURU
Protectt.ai
Providence
pnb
QRC
be assured . be secured
SQ1
nxtgen cybersecurity
target
ZS
SECURITY OK PLEASE
TRUCKLOAD OF INFORMATION TO STAY SAFE ONLINE
DSCI CSAM 2025

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

About DSCI

Data Security Council of India (DSCI) is a not-for-profit, industry body on data protection in India, set up by Nasscom, committed to making cyberspace safe, secure, and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI works together with the Government and their agencies, law enforcement agencies, industry sectors including IT-BPM, BFSI, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

DATA SECURITY COUNCIL OF INDIA
Nasscom Campus, 4th Floor, Plot No. 7-10, Sector 126, Noida, UP-201303

data-security-council-of-india dsci.connect dsci.connect DSCI_Connect dscivideo