

# 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.

## FAKE CUSTOMER SUPPORT AI CHATBOTS

### IMAGINE

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



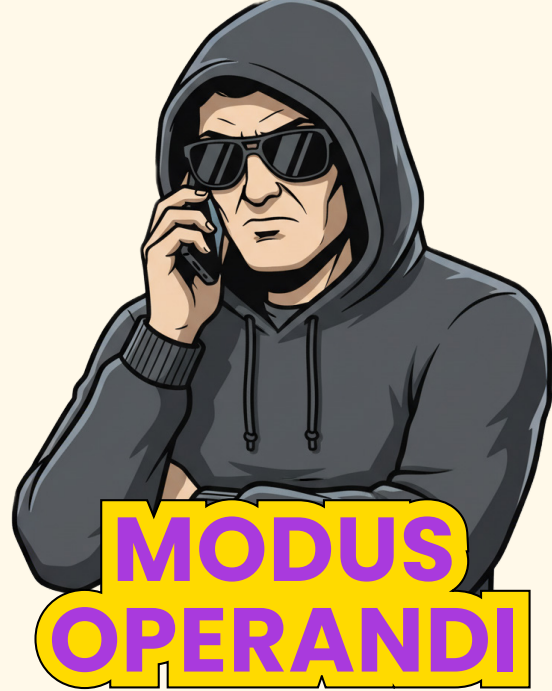
You click... and suddenly your bank details are gone.

### 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).



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](https://cybercrime.gov.in)** to register your complaint online.

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

Family Emergency Scam

AI Dating/Romance Scam

AI-Based Investment Scam

### SUPPORTED BY



CRED



HDFC BANK



IIFL FINANCE



Kempegowda INTERNATIONAL AIRPORT BENGALURU



Protectt.ai



Providence



PNB



QRC Quality • Risk • Compliance  
be assured, be secured



SQ1  
n-tgen cybersecurity



target



ZS