

# 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.

## AI DATING/ROMANCE SCAM

### IMAGINE

You match with someone online. They're attentive, funny, and share all your interests.

Next thing you know that you get attached and soon, they ask you for a financial favor.



### 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?

- Scammers create realistic profiles using AI-generated images, videos, and bios tailored to appeal to the victim.
- They may use AI-generated audio or video to maintain a consistent and believable presence during interactions.
- AI chatbots simulate conversations, responding instantly and intelligently to keep victims engaged and allow the scammer to target multiple people at once.
- Scammers quickly express affection or build emotional trust through compliments, shared interests and empathetic messages.
- Scammers analyze the victim's profile and interactions to customize messages and scenarios for stronger emotional manipulation.
- Scammers create emergencies, travel issues, medical expenses, or business problems to pressure victims into sending money or sharing sensitive information.
- They ask for UPI transfers, bank details, gift cards, or access to accounts under the appearance of trust.
- Over time, they continue nurturing the relationship to push for more funds or personal information until the victim becomes suspicious or exhausted.
- 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.
- 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.

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



Notice if someone forms an emotional connection too quickly or declares love unusually early.



Avoid sharing money, gifts, or personal financial details with anyone you've just met online.



Question inconsistent stories, repeated excuses for not meeting, or pressure to act immediately.



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.

Fake Customer Support AI Chatbots

Family Emergency 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 nextgen cybersecurity



target



ZS