

# 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-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.



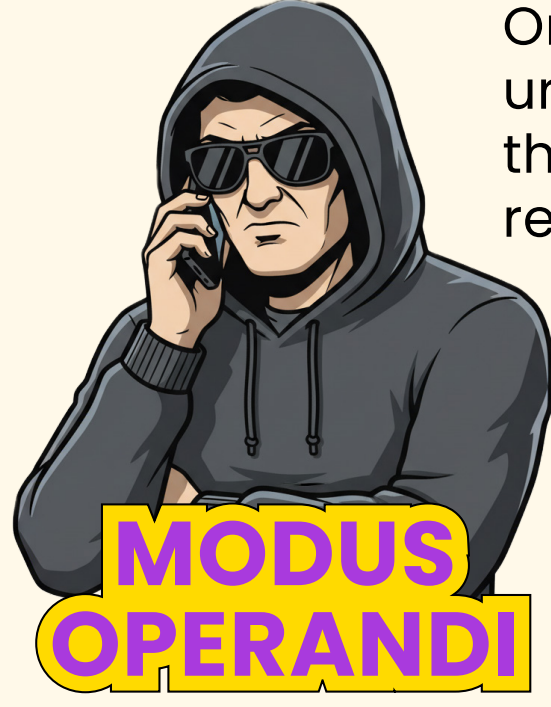
When you finally ask for your money, the platform disappears and the customer support vanishes.

### 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?

- Scammers promote fake AI-based trading platforms through social media ads featuring celebrity faces or endorsements.
- They promise zero risk and up to 100% monthly returns to attract quick investments.
- To look legitimate, they post fake media coverage and testimonials copied from real sources.
- 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.



Once convinced, victims are urged to invest larger sums with the false urgency of adding tax, regulatory, or processing fees before any withdrawal.

Funds are routed through multiple digital wallets to erase trails.

When victims try to withdraw, they face sudden account freezes or new compliance demands.

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.

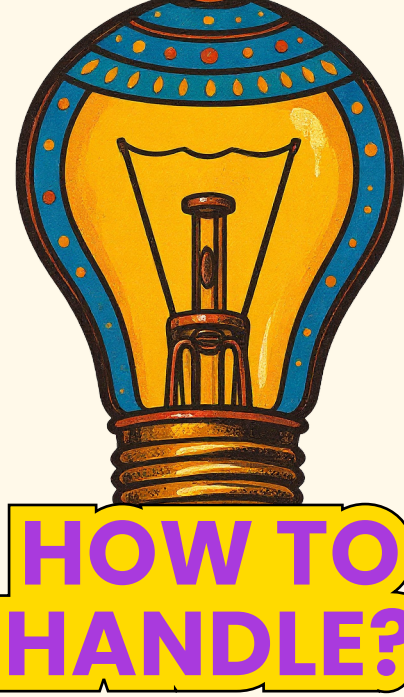


Dashboards showing unusually consistent or extraordinary profits.



Unverified or unregistered platform with no trace of regulatory oversight.

- Check if the investment firm is registered with a regulator like SEBI or any recognized securities authority.
- Look up independent reviews, user complaints, and scam alerts about the platform.
- Avoid any platform offering guaranteed, risk-free, or extraordinary returns.



Deepfake videos and fake endorsements are common; confirm from the celebrity's verified page or news sources.

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.



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

AI Dating/Romance Scam

Family Emergency 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