# Security Advisory: Beware of AI generated Deepfake Scams

AI-generated cyber scams represent a new and sophisticated avenue of threat in the digital landscape. Nowadays, with the power of Artificial Intelligence (AI), cybercriminals may create fake audio, video, or text content that convincingly mimics real person's voice, appearance or communication style, making it challenging to distinguish between genuine and fake.

## Modus Operandi of the Scam

1. Scammers gather information about the target individuals eg: voice recordings, images, videos etc. to create a realistic digital replica.
2. The collected data is then processed by AI algorithms to train AI models and replicate the target's voice, facial expressions, gestures, and communication patterns.
3. Using the trained AI models, fraudster generates the Deepfake contents (such as videos, audios etc.) in which the target person's face or voice is manipulated or replaced with synthetic elements.
4. The Deepfake contents are then delivered through various channels such as voice calls, text messages, video calls, social media etc. to deceive the known persons of the target individual.
5. By exploiting human trust & emotion, scammer then tricks other persons for doing specific action like transferring money, making payments, sharing sensitive information etc.
6. The consequences can range from financial loss to reputational damage, data breaches, and compromised personal or business information.

## Deepfake Scams - Warning Signs & Precautionary Measures

### Warning Signs

- Caller's voice may sound different
- Caller may ask for personal sensitive information
- May request for money transfer, financial help, immediate action etc.
- Inconsistencies in Speech like unnatural pauses, disjointed speech patterns, Distorted Audio or Visuals etc.
- May show some abnormal behaviour or unnatural facial expressions
- May not respond properly while discussing some personal matters / incident

### Precautionary Measures

- ✗ Do not transfer money without cross verifying the request from other trusted communication channel.
- ✗ Never share personal / sensitive information like Card Details, OTP, PIN, CVV, UPI PIN, Password, Financial Credentials with anyone.
- ✓ Look for inconsistencies, visual artifacts or anomalies that may indicate Deepfake signs
- ✗ Avoid oversharing information on social media and keep your profile privacy settings at the most restricted level
- ✓ Always cross-check information / media from official & trusted sources without blindly relying upon forwarded messages , online posts, advertisements etc.

Report Cyber fraud Incident to **https://www.cybercrime.gov.in**
or call **1930** for assistance

यूको बैंक (भारत सरकार का उपक्रम) UCO BANK (A Govt. of India Undertaking) CISO OFFICE

सम्मान आपके विश्वास का Honours Your Trust

*Security Advisory 108 dated 23.08.2023*