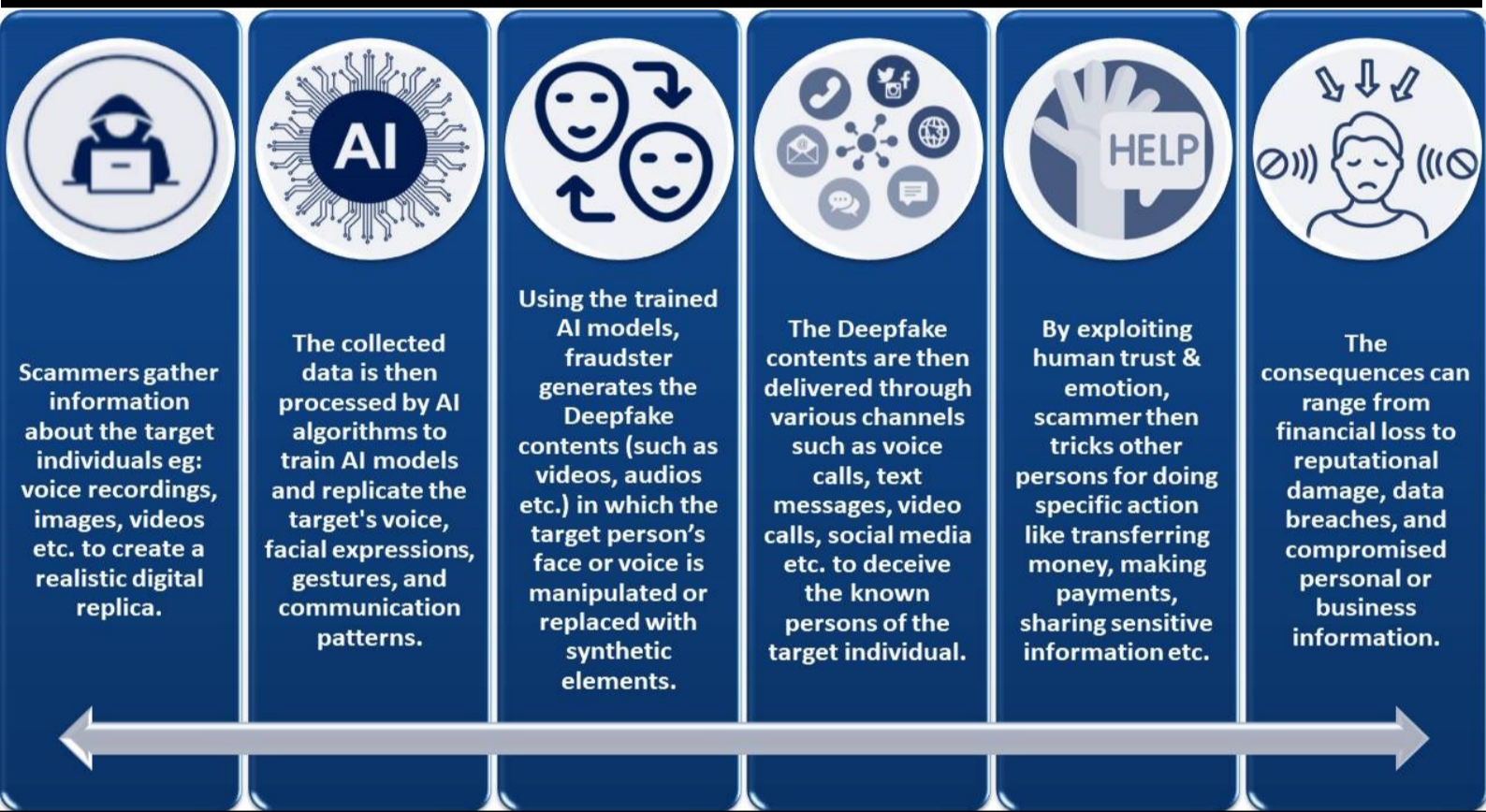




AI-generated cyber scams represent a new and sophisticated avenue of threat in the digital landscape. Nowadays, with the power of Artificial Intelligence (AI), cybercriminals may create fake audio, video, or text content that convincingly mimics real person's voice, appearance or communication style,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

Modus Operandi of the Scam



Deepfake Scams - Warning Signs & Precautionary Measures

Warning Signs

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

- ❌ 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