## Security Advisory

# Beware of **MARK** AI Voice Scams!

Cybercriminals are now using Artificial Intelligence (AI) to replicate the voices of your loved ones, making it seem like they're in trouble and urgently need money. This scam is particularly dangerous as it preys on emotions, inducing fear and urgency, leading victims to act hastily without careful consideration.

#### **Modus Operandi**



Scammers obtain recordings of voices from voicemails or social media platforms for targeted individual's family, friends or relatives.



Use AI software/ tools, they create highly convincing replicas of these voices.



They demand immediate money transfer from individuals by crafting emergency situation for their friends or family members.



The cloned voice, coupled with urgency, results in significant financial losses and emotional distress for victims.

#### **Red Flags**



Distorted voice of known one's in emergency situation

sensitive or financial

information etc.



emergency situation May ask for personal,



Unsolicited calls from unknown numbers, often from foreign countries

Unable to answer questions related to past incidents



Requests for money via various payment methods



Pressurizes to act quickly under fear, emotions etc.

### **Best Practices to avoid such scam**



Use Family Secret code / word / phrase known only to trusted family members.



Never trust unknown callers relying solely upon the voice.



Always contact directly from known & trusted communication channel.



Do not transfer money urgently due to fear or emotional pressure.



Keep profile privacy settings restricted for social media or other online accounts



Avoid oversharing information on social media platforms.

Report cybercrime at https://www.cybercrime.gov.in or call 1930 for assistance.

Security Advisory 120 dated 03.04.2024



सम्मान आपके विश्वास का

Honours Your Trust

