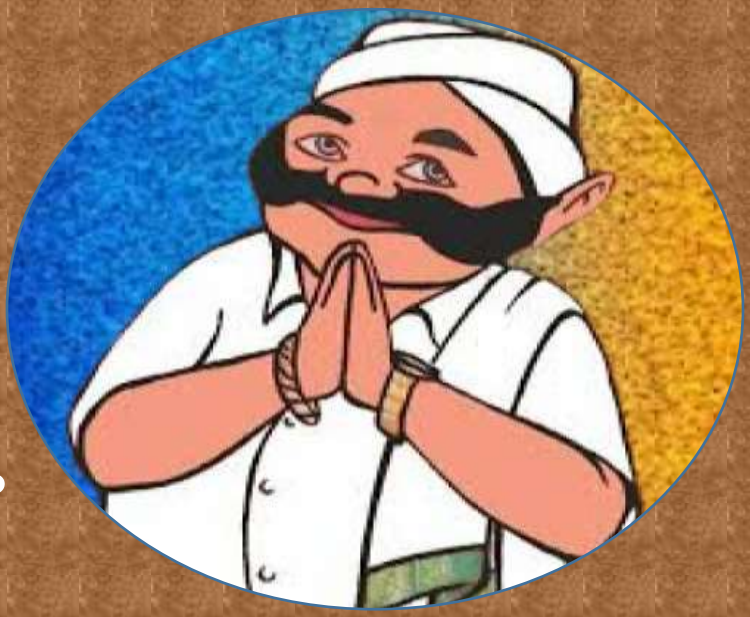
INDIAN OVERSEAS BANK

PRESENTS

AWARENESS INCIDENTS BY

IOB ANNA...



(Chapter 8)

(READ IT.....LEARN IT.....USE IT)

"आईओबी अन्ना, हर दिन चौकन्ना"

Fraud Risk Management Cell (Cyber)

"AI (Artificial Intelligence) Deepfake Scam Part-A" Chapter - 8

AI Deepfake Scam

Deepfakes are a form of artificial intelligence (AI) technology that uses deep learning to create synthetic media by manipulating an image, an audio track, a video, or any combination of those. Deepfake technology analyze and learn patterns from vast amounts of visual and audio data about the target individual which is usually available at social media or publicly available platform. Then deepfake technology enables cybercriminals to superimpose one person's face onto another's body or alter their facial expressions, voice, or gestures. The fabricated content is so realistic that it is very difficult to distinguish between genuine and fake. Most of the time, these cybercriminals impersonate a person very close to the victim like family members, close friends, high-ranking officials, etc. whom the latter will not hesitate to extend any monetary help. The unexpected victim falls prey to such frauds and ends up losing either money or personal information. Cybercriminals are using this technology to carry out to perpetrate scams like social engineering scams, phishing attacks, identity theft, financial fraud, information manipulation, damage to reputations, or political unrest.

Types of Deepfake Scams:

1. **New Account Fraud:** A fraudster can create a deepfake of an applicant to create a fake identity and use it to open an account, bypassing most of the usual checks. The criminal could then use that account to launder money or run up large amounts of debt.
2. **Ghost Fraud:** With ghost fraud, criminals use personal data from a deceased person for access to online services, tap into savings accounts, and gain credit scores, as well as apply for cars, loans, or benefits. Deepfake technology lends credibility to such applications, as the bank officials checking an application see a convincing moving, speaking figure on screen and believe that this is a live human being.
3. **Synthetic Identity Fraud:** Amongst the most sophisticated deepfake tactics, synthetic identity fraud is extremely difficult to detect. Rather than stealing an identity, criminals combine fake, real, and stolen information to 'create' someone who does not exist. These synthetic identities are then used to apply for credit/debit cards or complete other transactions to help build a credit score for the new, non-existent 'customer'. Synthetic identity fraud is the fastest-growing type of financial crime, and deepfake technology adds another layer of validity to these types of attacks.
4. **Social Engineering Scam:** Deepfake technology can analyze vast amounts of data from social media platforms to gather personal information about potential victims. Armed with this information, cybercriminals can exploit human psychology, trust, and vulnerabilities in order to trick individuals into sharing personal, confidential, or sensitive information or to deceive them into performing specific actions.
5. **Fraudulent Claims by Deceased Persons:** Using deepfakes, fraudsters can also make insurance or other claims on behalf of deceased individuals. Claims can successfully continue to be made on pensions, life insurance, and benefits for many years after a person dies and could be done either by a family member or professional fraudster. Here, deepfakes are used to convince the bank that a customer is still alive.
6. **Creating Authentic-Looking Identity Documents:** One-way fraudsters exploit AI and deepfakes is by creating counterfeit identity documents that appear genuine. With AI algorithms capable of generating highly realistic images, fraudsters can produce forged passports, driver's licenses, or other identification papers that pass visual inspections. These counterfeit documents can then be used to establish false identities and deceive identity verification systems.
7. **Business Fraud:** Fraudsters can manipulate audio or video recordings to deceive employees or customers, enabling them to gain unauthorized access to sensitive information or carry out fraudulent transactions.
8. **Evading Fraud Detection Systems:** Traditional fraud detection systems often rely on rule-based algorithms or pattern-recognition techniques. However, AI-powered fraudsters can employ deepfakes to evade these systems. By generating counterfeit data or manipulating patterns fraudsters can trick algorithms into classifying fraudulent activities as legitimate. This poses challenges for fraud detection and increases the risk of undetected identity fraud.

Fraudsters are utilizing more advanced and updated AI technologies in these days, to create deepfake so realistic and seamless that it has become a real challenge for even the most skilled cybersecurity professional to spot the deception. Whether you are an organization or an individual, everyone is responsible for protecting information and preventing fraudulent activity from happening. By staying informed and proactive, we can strive to stay one step ahead of fraudsters and protect ourselves from these emerging risks.

INCIDENT

Karthik is a working as a manager in a company and posted at Chennai. His family is residing at Hyderabad. One day Karthik received a call from his uncle from different number but in distress voice.

Hello, who is there?

Hi Karthik, I am Rajesh, your Uncle. (He is talking in distress voice)

Perpetrator purportedly pretend as Karthik's uncle Mr. Rajesh, who is residing at Hyderabad along with his family and very close to Karthik.

Karthik here the familiar voice and without thinking for a second, he asked his uncle, what happened uncle and where are you.

Perpetrator are waiting for this situation and cut the call. Then they immediately call Karthik on video call to make maximum benefit of this situation. Perpetrator uses the deepfake for video call due to this it is look like Karthik's uncle is on video call. Karthik also picked up the video call because earlier he received the voice call from same number. After seeing the uncle on video call, in distress voice, Karthik also gets tensed.

Hi Uncle, what happened. Why you are in stress?

Hi Karthik! I am in hospital and one of my close friend Shiva, required immediate medical treatment and requires Rs. 1.00 lakh. You also know him. I already arranged Rs. 50.00 thousand but another Rs. 50.00 thousand required immediately.

Karthik already believes on Uncle's voice and video because it is look like identical. Karthik also knows that his Uncle has a friend name Shiva. So, Karthik believes that his uncle genuinely required money for his friend treatment.

Yes, Uncle do not worry, I am sending you money immediately and Karthik transfer the Rs. 50,000/- as details provided by the uncle.

After one hour, Karthik again received a call from same number and Karthik's Uncle (Perpetrator) again requested for Rs. 50,000/-

Hi Karthik, I require another Rs. 50,000/-, can you arrange immediately.

This time Karthik, doubted about the situation and call directly to his Uncle's mobile no. and ask him about the money requirement.

After talking to his uncle, Karthik gets to know that his uncle never called him and never requested for money. Karthik gets shocked and tell the whole story to his uncle. Karthik's uncle also not understand how someone called Karthik with his voice and video call, how it is possible. Then he suggests Karthik that he has to contact IOB Anna, he is a well-known person and he also heared about him. Karthik immediately called the IOB Anna for immediate help.

Karthik called IOB Anna……

Hello IOB Anna, I am Karthik here.

Hello Karthik, tell me what happened.

Anna, I do not know, what happened.

Do not worry Karthik, tell me what happened?

Karthik narrated the whole incident to IOB Anna.

Karthik, I understood your incident. Karthik it is new type of online scam to dupe the people, it is called an AI Deepfake scam. Karthik, you have get scammed by AI Deepfake technology.

Anna, I do not know about this. How it is possible?

Karthik, you are duped by fraudsters through AI (Artificial Intelligence) Deepfake technology. Deepfakes are realistic looking but fake images, voices or videos generated via AI. Deepfake fraud occurs when scammers use this technology to target victims by impersonating close friends or family. Fraudsters collect visual and audio data of targets from their friends & family' social media platforms and use it to target an individual. The scammers use that AI to clone the sound and faces, and when it comes to videos, scammers use AI to map the facial movements of one person onto another. They make then phone calls and video call on which they claim to be the said friends or family and convince their victims to transfer large sums of money.

I am extremely sorry Anna; I did not even know about this. Now what I have to do?

Karthik, now immediately lodge a complaint to cyber police station, National Cyber Crime Reporting portal and bank cyber cell team.

Incident Overview by IOB Anna…….

- Karthik is the victim of online AI Deepfake Scam.
- He reacted on video call from unknown number.
- He heard the distress voice of his uncle on other side, which was not real but due to tension, he believes that he is talking to his uncle on video call and immediately transferred the money.
- He never heard about this type of fraud due to this he believed on fake video call of his uncle which created by fraudsters through the deepfake technology.
- He came in the trap of fraudster by fake video call which was looking realistic but actually it was manipulated.

Awareness Tips by IOB Anna…….

- Deepfakes often exhibit visual or audio artifacts, such as blurred edges, pixelation, or audio distortions. These anomalies can be a telltale sign of tampering.
- Ensure family, friends and employees know about how Deepfake works and the challenges it can pose.
- Have good basic protocols, "Trust but Verify" or “Zero Trust Policy”. A skeptical attitude to voicemail and videos will not guarantee you will never be deceived, but it can help you avoid many traps.
- Be cautious about what you share on social media and other online platforms and set your profiles to “friends and family” only, because scammers can use publicly available information against you convincingly. Uncontrolled sharing on online, may hench you in future.
- Account holders’ identities may need to be reverified at regular interval, even after their account has been set up.
- Solution provider should provide user facial authentication software and make sure it includes certified liveness detection technology.
- Please contact at Cyber Police Help Line No. 1930 in case of any cyber fraud.
- Please contact IOB cyber cell at 044 2858 4890 & IOB customer care at 1800 425 4445 or send mail at cybercell@iob.in in case of cyber payment fraud.

Deepfake!! Ruminate Before You Believe!

इण्डियन ओवरसीज़ बैंक
Indian Overseas Bank
आपकी प्रगति का सच्चा साथी
Good people to grow with

eFRMC

"DEEPFAKE IS A SPOILED BRAT
OF AI TECHNOLOGY,
INITIALLY PEOPLE PLAY WITH
DEEPFAKE,
LATER DEEPFAKE PLAY
WITH THEM".

"FIGHT AGAINST AI DRIVEN PAYMENT
FRAUDS IS EVERYONE'S
RESPONSIBILITY,
&
BY ADOPTION OF CYBER HYGIENE
AND ONLINE BEST PRACTICES,
WE CAN WIN THE FIGHT"

THANKS!