



# INDIAN OVERSEAS BANK PRESENTS AWARENESS INCIDENTS BY



# IOB ANNA...

(Chapter 9)

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



Fraud Risk  
Management  
Cell (Cyber)

“आईओबी अन्ना,  
हर दिन चौकन्ना”

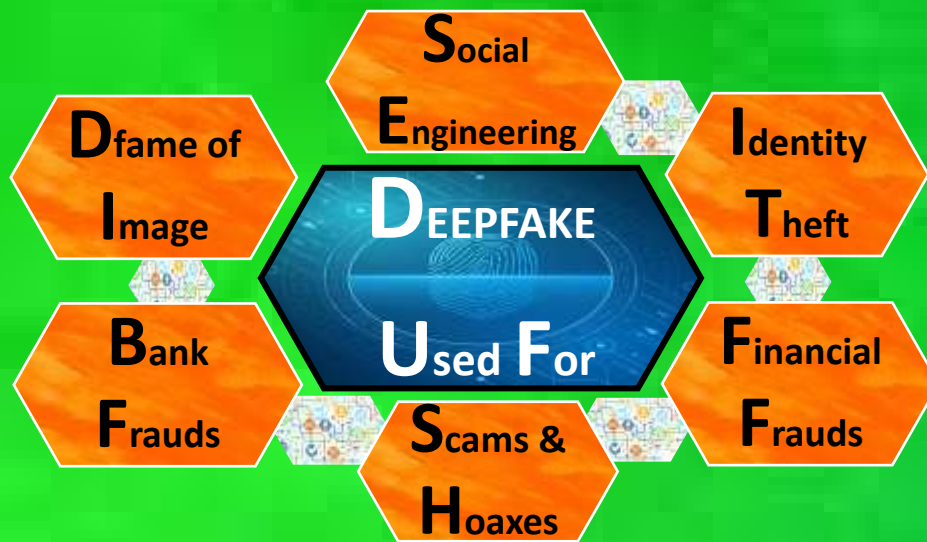
“AI (Artificial  
Intelligence)  
Deepfake Scam  
Part-B”  
Chapter - 9

**AI**  
**DEEPFAKE SCAM**

In last chapter (Chapter 8 - Deepfake Scam Part-A) we have explained about Deepfake technology and their modus operandi. Here we are covering the other areas of deepfake technology scams. These technologies make use of readily accessible images (facial data) and audio clips to craft artificial, yet highly lifelike, videos or images featuring an individual in scenarios they never actually experienced. Most deepfakes are made on high-end computers to process and create replicas of original content. High-quality deepfakes are generated when more data is fed to AI. This is easily available on social media platform. Deepfakes can be used to spread false information, which could spread political or social chaos. Besides, deepfakes also pose a major threat to national security. While there is no concrete way to differentiate deepfakes from real images, synthetic videos could wreak havoc and cause mass hysteria by the time their veracity can be established. Deepfake technology used by Cybercriminals to commit various frauds, to spread false/ manipulated information, to damage reputations, or to political unrest. In recent cases where, Indian cinema actresses got victimize by deepfake technology. It is a fine example of AI deepfake technology scam, where images & videos produced by AI powered tool to demonstrate non-existent human or real individual in unique or non-acceptable set-ups.

## Types of Deepfake Scams:

- 1. WhatsApp Deepfake Scam:** Deepfakes are created using the facial re-enactment technique, which involves using AI to map one person's face onto the face of another person in a video or audio recording. This can be done very convincingly, making it difficult to make out whether the video or audio recording is real or fake. Most of the time, these scamsters impersonate a person very close to the victim whom the latter would not hesitate to extend any monetary help. The unsuspecting victim falls prey to such frauds and ends up losing a lot of money.
- 2. Hiring fraud:** Hiring Fraud, also known as recruitment fraud, is when cybercriminals offer a person a fictitious job via unsolicited emails, online recruitment websites, and text messages. They will try to gain access to personal information, do an illegal job, or solicit payments. Conversely, applicants can also commit fraud by impersonating someone else in video interviews to try to get in. Once the imposter gets hired, they can start stealing valuable company information.
- 3. Manipulating facial recognition systems:** Facial recognition systems are widely used for identity verification, but they can be vulnerable to deepfake attacks. Fraudsters can use AI-generated deepfake images or videos to trick facial recognition algorithms into recognizing them as legitimate individuals. This can allow them to gain unauthorized access to accounts, bypass security measures or even enter secure premises.
- 4. Impersonating Individuals with Deepfake Videos:** Deepfake videos, which involve replacing a person's face with someone else's using AI algorithms, provide fraudsters with a powerful tool for impersonation. By using deepfake technology, fraudsters can create videos in which they appear to be someone else, potentially targeting individuals' personal or professional relationships. In addition to social engineering, this technique can be used for financial fraud or even blackmail.
- 5. Virtual Deception - The Growing Rise of Deepfake Video Call Scams:** Virtual deception is continuously rising with the use of deepfakes in video calls. This scam will be based on deepfake video calls, using what are now well-established employee and business communication channels such as Zoom, Team, etc.
- 6. Misinformation with Deepfake:** Deepfakes can spread misinformation convincingly in which they can morphed the images and videos to humiliate, abuse and extort. These sorts of deepfakes are unsurprisingly used to target females mostly. Cybercriminals may access publicly available and benign images from social media sites or other sources and using deepfake techniques to render explicit videos or pictures, then demanding money even though the material is not real. Many victims, which have included minors, are unaware their images were copied, manipulated, and circulated until it was brought to their attention by someone else. After manipulating illicit content, they may blackmail victims and demand money, personal data, or unwanted favors.
- 7. Friendzone/ Romance Scams:** Cybercriminals utilize deepfake technology to create realistic and compelling online profiles, ensuring they appear genuine and attractive to potential victims. Through deepfake they can generate convincing profile pictures, craft engaging bios, and even simulate human-like conversation patterns. By deepfake, scammers can establish trust and emotional connections with their targets, setting the stage for their deceitful intentions. By employing deepfakes in romance scams, cybercriminals can appear as someone else during video calls, further enhancing the illusion of a genuine connection. Scammers exploit deepfake tools for explicit content by morphing of public photos and videos.



Deepfakes are made all the more catastrophic by a lack of accountability and ambiguity regarding the rights of content producers and suppliers, as well as the people whose resemblance is utilized. Deepfakes propagating harmful untruths have an impact on social image and personal and professional relationships. Cybercriminals use deepfake for financial gain from innocent people. The personal impact of defamatory posts and trolls can take the form of victimization, trauma and toll on mental health and shockingly financial gain & exploitation of females are the main target through deepfake. Recent study says that in coming 5 years, up to 90% of web material will be created synthetically and it will be a threatening scenario for society.

In the view of the above, Government also initiated efforts to identify misinformation and deepfakes that violates the provisions of rules and regulations, and such cases are expeditiously actioned against, well within the timeframes stipulated under the IT Rules 2021. Government also advised that,

"Users are advised not to host such Deep Fake content/ videos/ information. They have to remove any such content within 36 hours after reported by victim to concern authority. Social media intermediaries / Hosts have to ensure expeditious action, well within the timeframes stipulated under the IT Rules 2021, and disable access to the content/ videos/ information."

Along with that government also advised the people that,


"For those who find themselves impacted by deepfakes, strongly advised to file First Information Reports (FIRs) at nearest police station and avail the remedies provided under the Information Technology (IT) rules, 2021".

While the concerns of the deepfake technology cannot be ignored, a proactive approach is necessary to clamp down deepfake technology threat to ensure that people continue to feel safe online. It is a collective responsibility of every person to adopt cyber hygiene for all online activity, which can prevent them and their family & friends from any unwanted situations caused by deepfake technology or otherwise.


## INCIDENT

Murugan is a senior citizen and retired from ITO since 2019. He is living with his wife at village side. He is a pensioner and earning handsome money from agriculture. One day Murugan received a call from anonymous number followed by message on WhatsApp from same mobile

Perpetrator disconnected the call purposely and pretend that call has been disconnected. Then again he called Murugan through voice call, but this time Murugan has no doubt and comfortably attended the call.




Hello, Murugan, I am Bala. Do You remember, we worked together in ITO, Trichy?




Hi Murugan, sorry call disconnected. I have required some urgent money of Rs. 50000/- for medical treatment, sorry for that.

Perpetrator pretend as a Murgan's friend Bala, who work together in ITO, Trichy. Perpetrator get the picture of Mr. Bala from social media and same has been make a profile picture on WhatsApp, so nothing looking suspicious. Murugan also knows that one of his good friend Mr. Bala worked with him in office but after retirement they have not communicated. After looking at the profile picture, Murugan can't doubt that the person is his old friend.


This time Murugan very much comfortable with the call and he knows his friend Bala, he asked straight away for details for transferring the money.



Hi Bala. Why you are sorry. We are friends. Please send me details so I can transfer the money.



Hello, Bala. I recognize you. You have changed a lot. How are you? (And they started chit chat on WhatsApp)



My friend, how are you? It is a long time. (Then Perpetrator asked about his family and business etc.) Then Perpetrator call Murugan on WhatsApp video call, where he looked exactly like shown in profile pic. Face expression, lips, eyes everything is looking similar so nowhere Murugan doubted on him. But call has been disconnected very early.

Perpetrator immediately send the details to Murugan. Murugan received the details and immediately transfer the money. Perpetrators want to take benefit of the situation, so he again called the Murugan for some more money. But this time Murugan got some doubt and cut the call. He searched his friend Bala's mobile no. with other friends and called him and then he got to know that his friend Bala never called him for money.

Murugan blocked that mobile no. and told all the incident to his friend Bala. His friend also got shocked and not understand how it is possible. He told Murugan that you have to contact IOB Anna, he is dealing in cyber frauds, he will surely help you. Murugan immediately called IOB Anna for help.

Murugan called IOB Anna.....



Hello IOB Anna, I am Murugan here.



Hello Murugan, tell me what happened.



Anna, I got cheated through WhatsApp, please help me.



Ok don't Worry, Murugan, tell me what happened?



Murugan told the complete incident to IOB Anna.



Murugan, I understood the matter & scenario. I can understand that you are helpless in that situation because you never seen/heard that earlier. Murugan it is a new way to dupe people, it is an AI driven deepfake technology scam and you have fallen victim that scam.



Murugan, you are fooled by fraudsters through online AI (Artificial Intelligence) deepfake technology. Deepfake technology means deepfake learning with something fake. In this technology, image & voice of known person stitched with machine language to create fake videos and images of known person to commit frauds. Deepfake technology has been used by fraudsters to impersonate as a family or friend and then defraud them easily. Deepfake can create some new hyper-realistic but fraudulent material that cannot be easily captured by human eyes and seems utmost realistic. In deepfake technology, fraudsters have been tricking people for money or sensitive information.



I am shocked Anna; I never heard about this. Now what I have to do?



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

## Incident Overview by IOB Anna.....



- Murugan is the victim of AI deepfake technology scam.
- He reacted on an anonymous number of old friends, to which he did not contacted from several years.
- He chatted with old friend on unknown no. without verification of the no.
- He chatted with old friend on video call after some time and after revealing some family information by the friend which may available online, he never feels suspicious.
- Due to fake video or image looks realistic, no doubt came in Murugan's mind, and he transferred the amount as requested by fraudsters who impersonate as his friend.

## Awareness Tips by IOB Anna.....

- Always verify the identity of the caller from your side whenever unexpected urgent requests came for money or personal information, even if they appear to come from someone you know.
- Stay informed and aware about latest frauds and their modus to prevent falling victim to these scams.
- Stay vigilant and cautious over social activity apps. Always vigilant when video calls come from unknown no. and try to avoid such calls or stay vigilant when you attend them.
- 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.
- If fallen victim of deepfake scam online for obscene content, immediately lodge FIR to remove content from online under IT ACT 2021. (After FIR, content may remove by Social Media Handler from online within 36 hours as per Government Guidelines).
- 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](mailto:cybercell@iob.in) in case of cyber payment fraud.



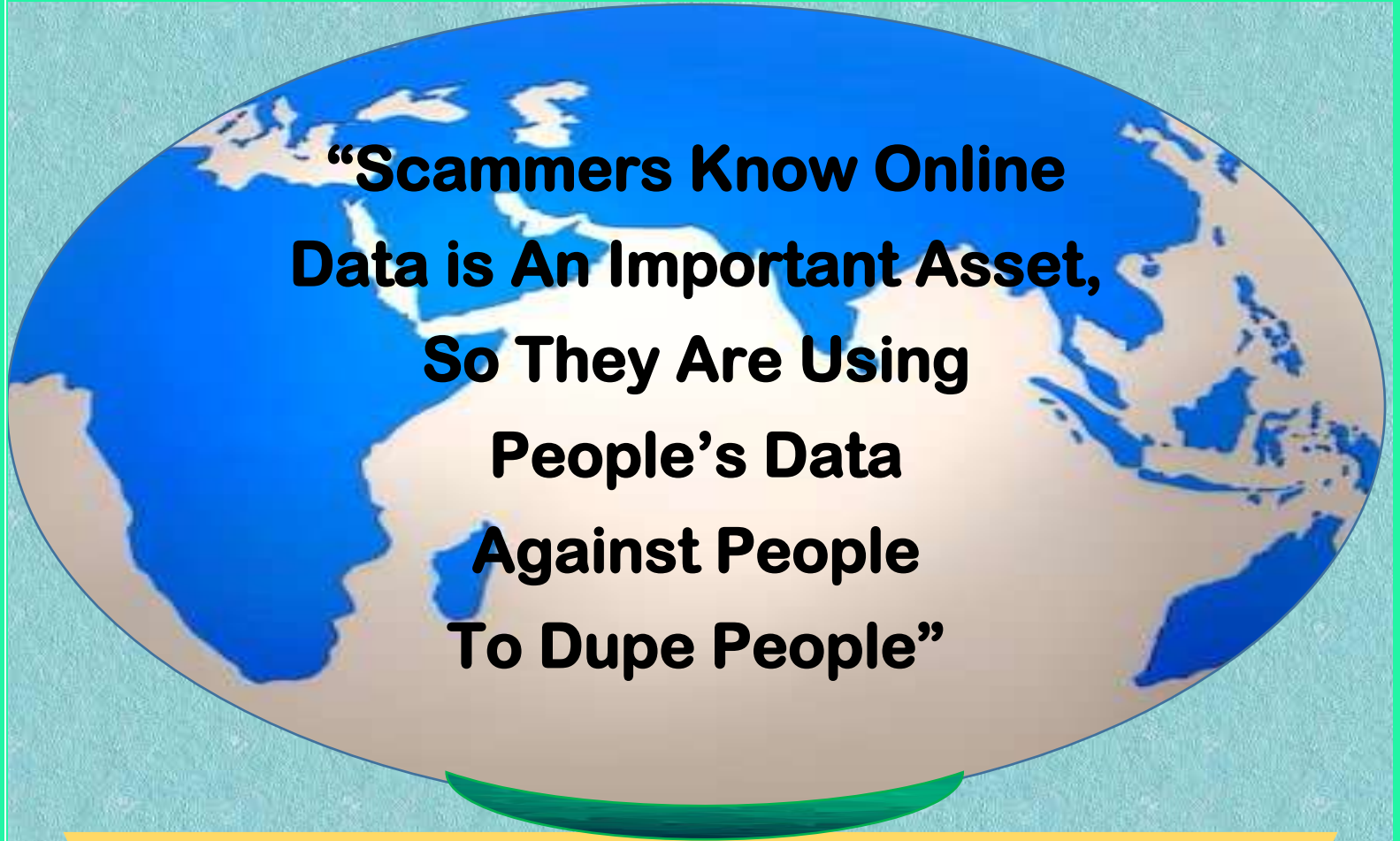
**If UR mind does not beep, Deepfake may hurt U deep!!**



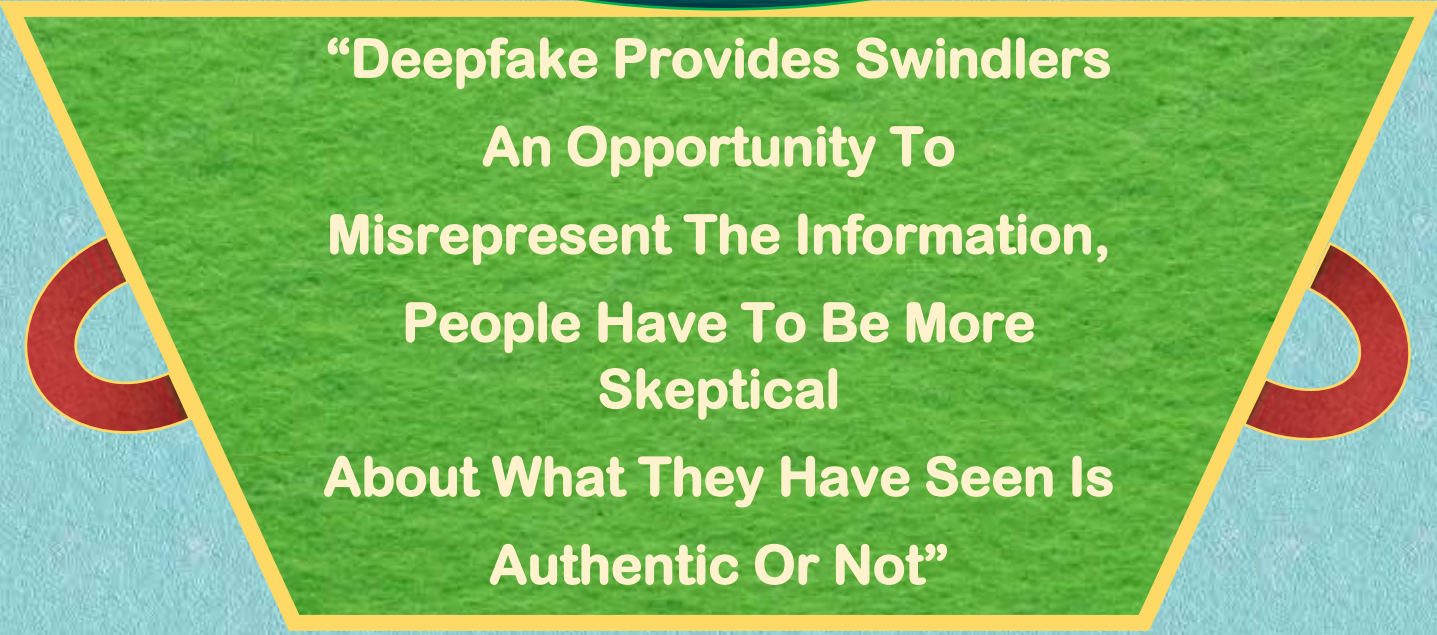
**इण्डियन ओवरसीज़ बैंक**  
**Indian Overseas Bank**

आपकी प्रगति का सच्चा साथी  
Good people to grow with





**“Scammers Know Online  
Data is An Important Asset,  
So They Are Using  
People’s Data  
Against People  
To Dupe People”**



**“Deepfake Provides Swindlers  
An Opportunity To  
Misrepresent The Information,  
People Have To Be More  
Skeptical  
About What They Have Seen Is  
Authentic Or Not”**

**THANKS!**