# INDIAN OVERSEAS BANK

## PRESENTS

## AWARENESS INCIDENTS BY

# IOB ANNA

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

# आईओबी अन्ना हर दिन चौकन्ना

## CYBER HYGIENE SERIES BY IOB ANNA...

# Customer Duped By The Scam Game

## INCIDENT
## घटना

**Gist of the Case:**

**The scammers create a fake WhatsApp account using the profile picture of company heads, often sourced from social media or company websites.**

**They then contact accountants or financial officers and request urgent fund transfers under the guise of critical meetings or high-priority projects. Fake details of beneficiary accounts are provided, along with pressure tactics to rush the transaction, read the statement.**

**Sharing details of the three incidents, police said in the first instance, a company's accounts manager received a WhatsApp message from a scammer impersonating the managing director. Using the company logo as the display picture, the fraudster cited urgency for a Rs 1.25 crore advance payment for a "new project". The manager, misled by the scammer's convincing narrative, transferred the amount.**

**In the second incident, a chief financial officer was duped of Rs 3.50 crore in two separate transactions. The fraudster, impersonating the MD, provided detailed account information and referenced the company's financial position. The urgency of government-related contracts was cited to manipulate the CFO into compliance.**

**In the last incident, impersonating the brother of a company director, the fraudster approached an accountant of a private firm. Using similar tactics, he sought two payments of Rs 50 lakh, claiming it was required for "urgent official work".**

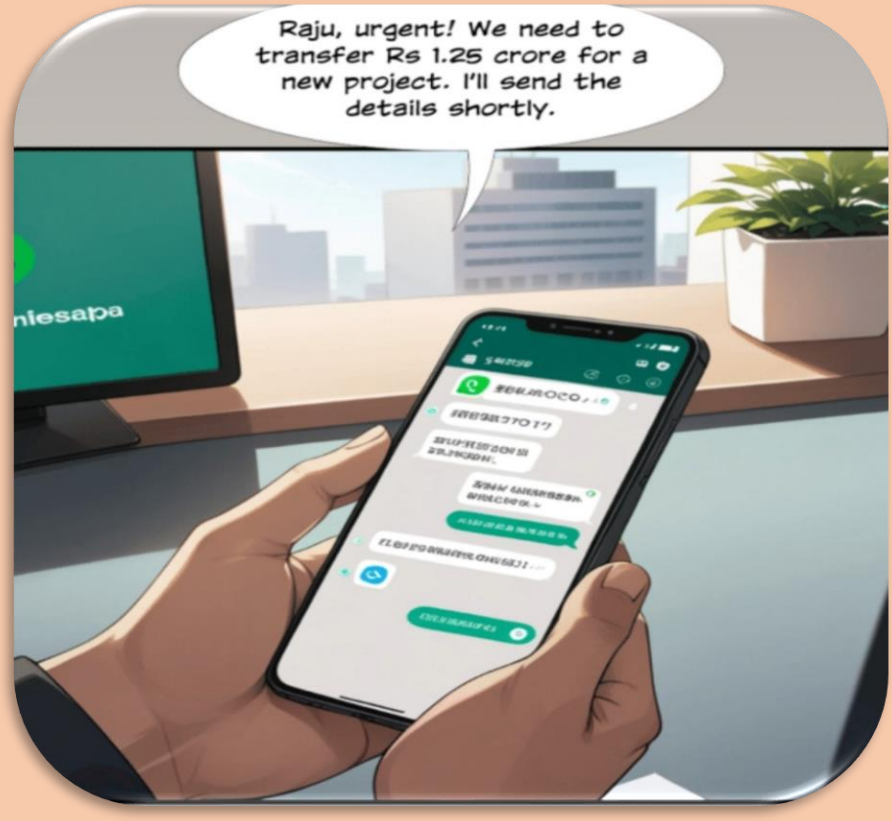
**Meanwhile, authorities have urged companies to adopt stringent protocols to prevent such incidents.**

**Police said that all such requests must be verified physically and the employees receiving such messages should cross-check the details with other senior officials.**

## The Scam Game- Incident-1

- **A well-dressed accounts manager, RAJU, is working on his computer. His phone buzzes on the desk.**


- **Close-up of the phone screen showing a message from "MD - COMPANY X" (scammer). The display picture is the company logo, and the message reads:**




**Raju looks concerned but trusts the message, tapping on the phone.**

# The Scam Game- Incident-2

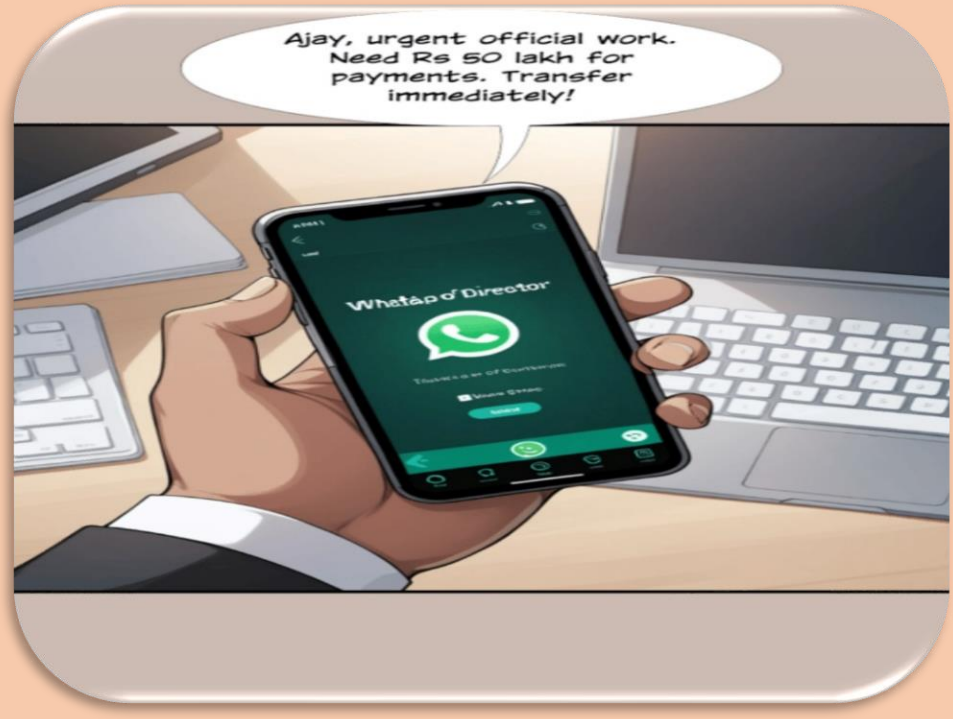
- **A conference room. The CFO, MRS. SINGH, is sitting at a desk, holding her phone. The screen shows a WhatsApp message with the same company logo.**


- **Mrs. Singh, sweating, looks at the detailed message and account info on her phone.**

- **A split panel shows Mrs. Singh transferring the funds to the scammer's account on one side, while on the other side, a timer counts down from 10 seconds.**


## The Scam Game- Incident-3

- **Office of a private firm. The accountant, AJAY, is sitting at his desk, looking at his phone with confusion.**




❖ **Ajay, unsure but pressured, is typing a response.**

❖ **Police station. A detective, INSPECTOR TIWARI, stands at a press conference, addressing the media. A large display screen behind him shows images of the scammers' WhatsApp messages and company logos.**


- **A wide shot of the press conference room, with journalists scribbling notes. Tiwari continues to speak.**


- **A company office. RAJU, MRS. SINGH, and AJAY are sitting in a meeting room, looking worried. An office manager, NINA, stands with a checklist, addressing them.**

- **Raju, Mrs. Singh, and Ajay look relieved as Nina explains the new policy.**


- **Nina, smiling, walks out of the room, leaving the trio to discuss.**


**Stay Alert. Stay Secure.**

- **In Newspaper, Raju read about IOB ANNA, immediately he called to IOB ANNA.**

**HELLO ANNA….. I Need your help. I received a WhatsApp message from scammer. He asked me to transfer Rs,1.15 Crores.**

**OMG! That is a huge sum! Please tell me more about the scam.**

**I am accountant in private firm and one day scrolling through my phone at office. Suddenly I received a WhatsApp message from my boss. In profile photo firm's logo was there. The message reads:**

**"Raju, urgent! We need to transfer Rs 1.15 crore for a new project. I'll send the details shortly."**

**My Colleagues also received same type of messages for different amount.**

**OMG! This type of cyber crime is known as THE SCAM GAME.**

**A scam where a scammer sends a message to an employee to transfer money to another account is called a fund transfer fraud/Scam Game. In this type of scam, a criminal initiates or redirects a money transfer from another user to receive the funds.**

**Raju! How do you realize that they were fake?**

**I got confused. I was ready to transfer the funds to scammer's account. But I called my boss on landline number then I came to know that they were fake.**

**Anna! Please tell me that how to protect from these types of scams.**

**Here are some ways to protect yourself from false promise scams:**

- **Be wary of unsolicited contact**
  Do not respond to unsolicited emails, calls, or texts.

- **Do not share personal information**
  Do not share personal or financial information over the phone, in an email, or on a website you did not initiate.

- **Be cautious of urgent messages**
  Scammers often use urgent messages or get-rich-quick schemes to pressure you into acting.

- **Use multi-factor authentication**
  Use multi-factor authentication to protect your accounts. This requires two or more credentials to log in, such as a passcode, a one-time verification code, or a fingerprint scan.

- **Update your software**
  Keep your phone's operating system and computer's security software up to date to protect against malware and security threats.

**Anna! How to report such types of scams? Now what I must do?**

**Report Suspicious activity: Report the scam attempt to the National Cybercrime Reporting Portal at WWW.CYBERCRIME.GOV.IN or call Cyber Crime Helpline at 1930.**

# Awareness Tips by IOB Anna…….

- Always verify the identity of the caller through another means of communication before taking any action, when it is urgent request.
- Be wary of unexpected urgent requests for money or personal information, even if they appear to come from someone you know.
- Stay informed about different types of online scams and how they work. Awareness is key to preventing falling victim to these scams.
- Stay vigilant and exercise caution in all your interactions over online.
- 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.
- Enable multi factor authentication, if possible, on your financial and important online accounts to add an extra layer of security.
- 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.


# THANK YOU
# धन्यवाद