# INDIAN OVERSEAS BANK

PRESENTS

Awareness Incidents by

# IOB ANNA

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

# ‼आईओबी अन्ना, हर दिन चौकन्ना‼

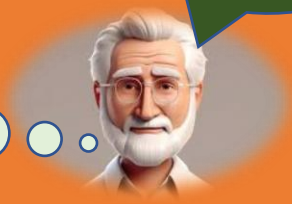
Cyber Hygiene Series by IOB Anna...

## Customer Duped by Digital House Arrest

### INCIDENT

Raj narrates the full incident to his friend Ramesh.

Hello Ramesh! How are you? You won't believe what happened to me, Ramesh. I got scammed by someone pretending to be the CBI chief! I lost Rs.32.00 Lacs.



What? Are you serious? How did that happen?

Two persons posed online as the CBI Chief and CBI Officer and scammed me due to the tune of Rs.32.00 Lacs. They contacted me via a messenger app, claiming they were investigating some serious financial irregularities under PMLA Case.

This is insane! That's a huge sum! Did you give them money?

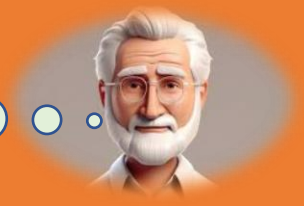
Unfortunately, yes. They sounded so official. They even had a fake badge and everything. I was convinced and I felt that I am helping government official in a big case. They assured that they would help me but asked me to send the money to them promising that the funds would be returned in a day or two days after proving my innocence before the Supreme Court, as per the laws.

Oh my god, Raj! Did you have any idea they were fake?

They have digitally arrested for 15 days. I started to question it when they asked for a "processing fee" for the investigation. But by by that time, I was too deep into it...

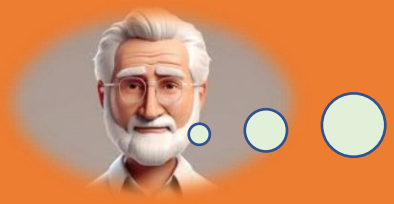
This is so typical! They always use authority to manipulate innocent people. Did you report it to the police, IOB ANNA or anything? I assure you that IOB ANNA will help you in this matter. Please call him immediately.

Thanks, Ramesh. I really appreciate your support. I'll start planning. I will also share this incident with **IOB ANNA**...



Anytime, Raj. Just remember, you aren't alone in this. We'll figure it out together!

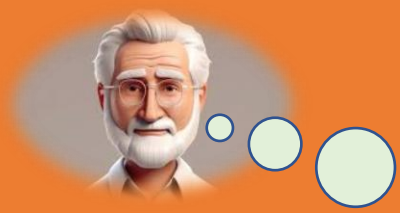
## RAJ CALLED IOB ANNA.....



Hello Anna! I need help from you. I got scammed by someone pretending to be the CBI chief!

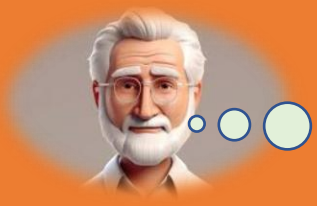
I lost Rs.32.00 Lacs.

Oh my God! That's a huge sum! Please tell me more about the scam.



Two persons posed online as the CBI Chief and CBI Officer and scammed me due to the tune of Rs.32.00 Lacs. They contacted me via a messenger app, claiming they were investigating some serious financial irregularities. Please help me **ANNA.**

Don't worry Raj, can you tell me how you believed them.



Anna! I am Raj, a senior citizen, aged 63 years, living in Chennai. They know my Aadhar number, date of birth and other personal information.

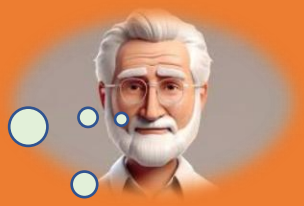
Raj, can you please tell me more about this incident.

Anna! I was convinced and I felt that I am helping government official. They assured that they would help me but asked me to send the money to them promising that the funds would be returned in a day or two days after proving my innocence before the Supreme Court, as per the laws.

Raj, you are defrauded by fraudsters. This type of Cybercrime known as **DIGITAL HOUSE ARREST.**

Digital house arrest is a social engineering scam where cybercriminals impersonate law enforcement officials. They target individuals through phone calls, emails, or even social media messages. The scammers claim the victim's identity proofs such as their bank account, SIM card, Aadhaar card, or other cards linked to their bank account has been used unlawfully.

Oh my god, Raj! How do you realize that they were fake?



I started to question it when they asked for a "processing fee" for the investigation. But by that time, I was too deep into it...

I am extremely sorry Anna; I did not even know about this. Now what I must do? Please tell me How Does the Scam Work?

The scam typically unfolds in these steps:

The Call: The victim receives a call from someone claiming to be from a legitimate organization like the police, social security administration, or bank.

Creating Panic: The caller alleges fraudulent activity on the victim's account or a threat to their identity. They use urgency and fear tactics to pressure the victim into taking immediate action.

Isolating the Victim: Scammers often instruct the victim not to contact anyone, including family or the real authorities, claiming it would jeopardize the investigation. This isolates the victim and makes them more susceptible to manipulation.

Demanding Compliance: The caller demands the victim take specific actions, such as transferring money, providing personal information, or downloading malware.

Anna! Please tell me that How to Protect from these types of Scams?

Be Wary of Unsolicited Calls: Legitimate organizations rarely contact you out of the blue regarding urgent account issues.

Verify Information: Do not trust caller ID – it can be spoofed. If you are unsure, hang up and call the official number of the organization the caller claims to represent.

Never Share Personal Information: Legitimate institutions will not ask for sensitive information like passwords or social security numbers over the phone.

Don't Be Pressured into Action: Take a moment to breathe and don't make hasty decisions due to fear.

Talk to Someone You Trust: Discuss the situation with a friend, family member, or law enforcement officer to gain a clear perspective.

Anna! Now what I must do? How to report such type of Scams?

Report Suspicious Activity: Report the scam attempt to the National Cybercrime Reporting Portal at www.cybercrime.gov.in Or Call Cyber Crime Helpline is 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.