INDIAN OVERSEAS BANK

PRESENTS

AWARENESS INCIDENTS BY

IOB ANNA

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

आईओबी अन्ना हर दिन चौकन्ना

The Fake KYC Trap |फर्जी केवाईसी जाल

INCIDENT घटना

Rahul, a regular bank customer, was at home when he received an SMS on his phone. The message read: *"Your bank account will be blocked. Click here to update KYC immediately."*

Worried about losing access to his account, Rahul clicked the link without thinking twice. A webpage opened that looked exactly like his bank's official website. Trusting it, Rahul entered his **username, password, and OTP**.

At the same time, on the other side of the city, a fraudster sitting at his computer smiled as Rahul's details appeared on his screen. Within minutes, the fraudster initiated a transfer, and ₹25,000 was debited from Rahul's account.

Rahul was shocked when the debit alert popped up on his phone. Panic set in as he realized he had been trapped in a cyber fraud.

Immediately, Rahul contacted his bank and reported the fraud on the **Cybercrime Helpline 1930** and the portal **cybercrime.gov.in**. His account was blocked to prevent further loss.


Your bank account will be blocked. Click here to update KYC immediately.
Oh no! I must update it quickly.


Enter username, password, and OTP to continue.
Better to finish it fast...


Haha! Got his login and OTP. Time to empty his account.


₹25,000 debited from your account.


What?! I never did this transaction!


Never share your OTP, PIN, or password with anyone.
Banks never ask for information through SMS or links. Call 1930 as soon as you encounter fraud.
I was duped, but now I'll caution everyone.

Hindi Version:

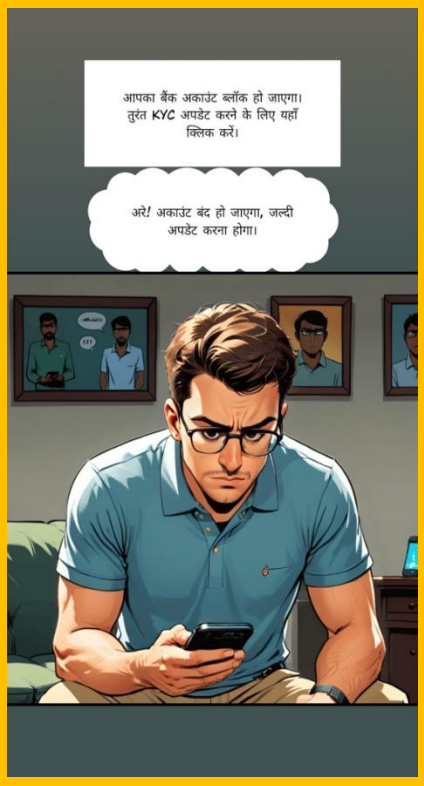
राहुल, एक सामान्य बैंक ग्राहक, घर पर बैठा था जब उसके मोबाइल पर एक एसएमएस आया। मैसेज में लिखा था: ***"आपका बैंक अकाउंट ब्लॉक हो जाएगा। तुरंत KYC अपडेट करने के लिए यहाँ क्लिक करें।"***

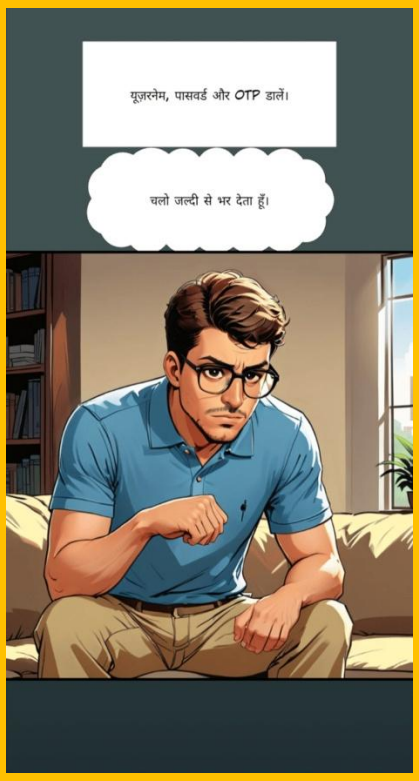
अकाउंट बंद होने की चिंता में राहुल ने तुरंत लिंक पर क्लिक किया। एक वेबसाइट खुली, जो बिल्कुल उसके बैंक की असली वेबसाइट जैसी लग रही थी। उस पर भरोसा करते हुए राहुल ने अपना यूज़रनेम, पासवर्ड और **OTP** भर दिया।

उसी समय, शहर के किसी कोने में बैठा एक ठग अपने कंप्यूटर पर मुस्कुरा रहा था। राहुल की सारी जानकारी उसकी स्क्रीन पर पहुँच चुकी थी। कुछ ही मिनटों में उसने ट्रांज़ैक्शन कर दिया और राहुल के खाते से **₹25,000** निकल गए।

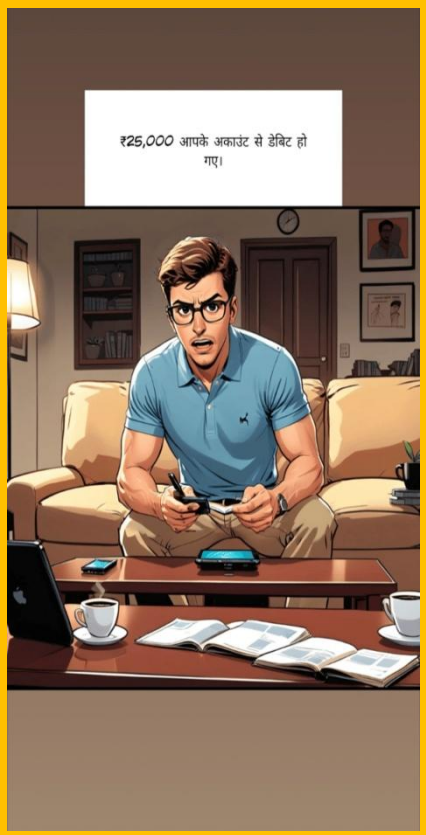
जैसे ही राहुल के मोबाइल पर डेबिट अलर्ट आया, वह सदमे में आ गया। उसे समझ आ गया कि वह साइबर ठगी का शिकार हो चुका है।

राहुल ने तुरंत अपने बैंक से संपर्क किया और साइबरक्राइम हेल्पलाइन **1930 तथा cybercrime.gov.in** पर शिकायत दर्ज कराई। खाते को ब्लॉक करा दिया गया ताकि और नुकसान न हो।


आपका बैंक अकाउंट ब्लॉक हो जाएगा। तुरंत KYC अपडेट करने के लिए यहाँ क्लिक करें।
अरे! अकाउंट बंद हो जाएगा, जल्दी अपडेट करना होगा।


यूज़रनेम, पासवर्ड और OTP डालें।
चलो जल्दी से भर देता हूँ।


हा हा! पासवर्ड और OTP दोनों मिल गए... अब अकाउंट खाली कर दूँगा।


₹25,000 आपके अकाउंट से डेबिट हो गए।


हे भगवान! ये ट्रांज़ैक्शन तो मैंने किया ही नहीं।


OTP, PIN या पासवर्ड कभी किसी से शेयर न करें।
बैंक कभी SMS या लिंक के ज़रिए जानकारी नहीं मांगते।
फ्रॉड होते ही 1930 पर कॉल करें या
मुझे तो ठग लिया, पर अब मैं सबको सावधान करूँगा।

Here are some ways to protect yourself from these types of scams:

- **Verify Messages/Calls**
  If you get any SMS/WhatsApp/Email about KYC, blocking account, lottery or cashback, ignore the link.

- **Type Website Manually**
  Always type your bank's official website in the browser. Never click on links sent via SMS/unknown emails.

- **Check URL Carefully**
  Fake websites often look similar but have spelling mistakes.

- **Keep details secret**
  Never share OTP, PIN, CVV, or Password with anyone. Remember: Bank Employees will never ask for these.

- **Extra Safety Tips**
  Enable **SMS/Email alerts** for all transactions.
  Use **Strong passwords** and update them regularly.
  Keep your phone and banking apps updated.
  Register for your **bank's fraud awareness alerts.**

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.

This incident became a learning point:

- *Banks never ask for KYC updates via SMS or unknown links.*
- *OTP, PIN, and passwords should never be shared.*
- *Any such suspicious messages should be reported immediately.*

इस घटना से यह सबक मिला:

- *बैंक कभी KYC अपडेट के लिए एसएमएस/लिंक नहीं भेजते।*
- *OTP, PIN और पासवर्ड किसी से साझा नहीं करना चाहिए।*
- *ऐसे संदिग्ध संदेश तुरंत रिपोर्ट करने चाहिए।*

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