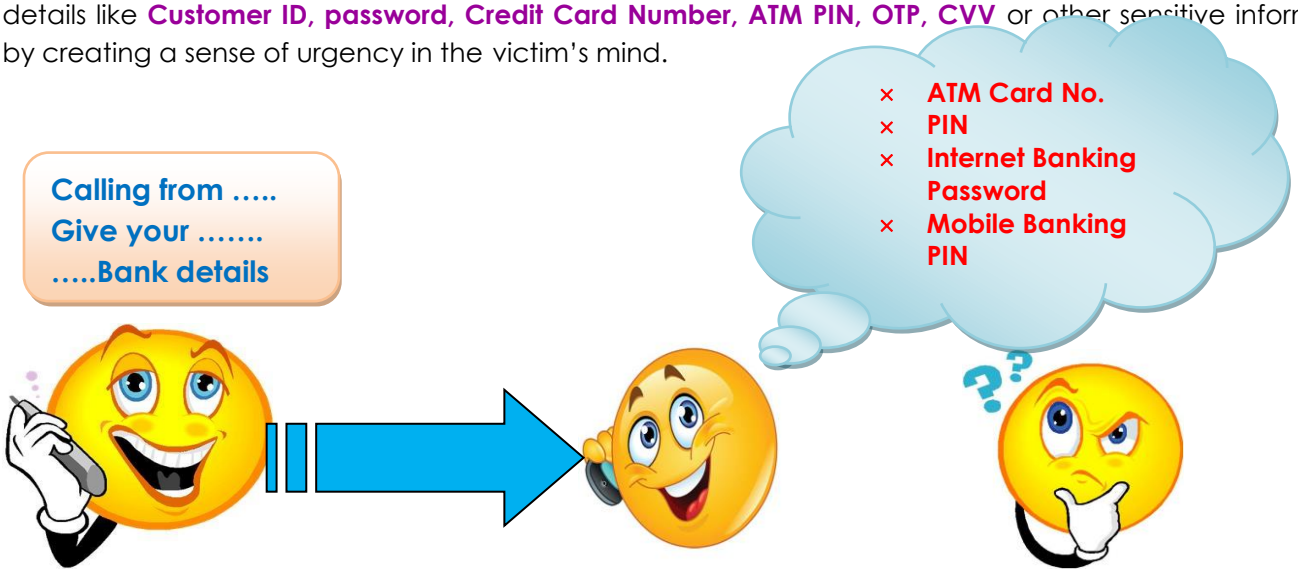
इण्डियन ओवरसीज़ बैंक **INDIAN OVERSEAS BANK**

VISHING – BEWARE OF FRAUDULENT PHONE CALLS

Dear Customer,

Greetings from IOB !

Vishing (also known as **Voice phishing**) is a form of phishing attack in which the attacker (Visher) calls a bank customer (Victim), claims to represent the bank and lures the victim to provide personal banking details like **Customer ID, password, Credit Card Number, ATM PIN, OTP, CVV** or other sensitive information by creating a sense of urgency in the victim's mind.



Steps to be taken if suspected vishing attack:

1. Immediately **change the password, ATM PIN, Mobile Banking PIN, secret questions/answers** that you have shared over the fraudulent call.
2. Verify if any unauthorized transaction has been carried out recently.
3. If yes, then immediately contact your **branch/bank** and report .
4. Recall and record the call details like the phone number, information shared with the Visher etc. It will help bank or the police in further investigation.
5. It is advisable to contact your local/cyber police and lodge a complaint.

Do not share confidential information like Internet banking login ID /Password /OTP /PIN /ATM-Debit /Credit Card Number / CVV/ Expiry Date to anyone. If you receive a mail or phone call asking for the same, be alert, as it is likely to be from a fraudster.

Bank or its employees will never ask for such confidential information through e-mail or over phone.

GOOD PEOPLE TO GROW WITH

With warm regards,
Chief Information Security Officer
Indian Overseas Bank, Central Office, Chennai