इण्डियन ओवरसीज़ बैंक **INDIAN OVERSEAS BANK**

Beware of PHISHING Attacks

Dear Account Holder,

Phishing is a way of attempting to acquire information such as usernames, passwords, and debit/ credit card details by masquerading as a trustworthy entity in an electronic communication.

How I can recognize a message of phishing?

Step1: Carefully verify the URL in the browser.

Step2: Always check for the misspelled URL. So always key in the URL in the address bar yourself don't copy and paste.

Step3: Always check for the trusted website which has ***https*** and ***padlock***.

Step4: Always view any email request for financial or other personal information with suspicion, particularly any "urgent" requests.

Step5: Never respond to the emails that ask for your personal information like credit card /debit card/bank information.

Do's	Don'ts
Be cautious about opening any attachments or downloading files you receive regardless of who sent them.	Don't reply to an e-mail or pop-up message that asks for personal or financial information.
Look for the sender email ID before you enter/give away any personal information.	Don't click on any email or social media messages you don't expect or need
Use antivirus, antispyware and firewall software (update them regularly too)	Don't open suspicious videos, images, spam e-mails and other attachments that you were not expecting, especially ZIP files and NEVER run **.exe** files.
Always update your web browser and enable phishing filter.	Don't respond if you receive any message (sms) asking you to confirm account information.
If you receive any suspicious e-mail do call the company to confirm if it is legitimate or not.	Don't use your company e-mail address for personal things
Do use a separate email accounts for things like shopping online, personal etc.	Do not reveal personal information in order to receive a prize, it's most likely a form of phishing.

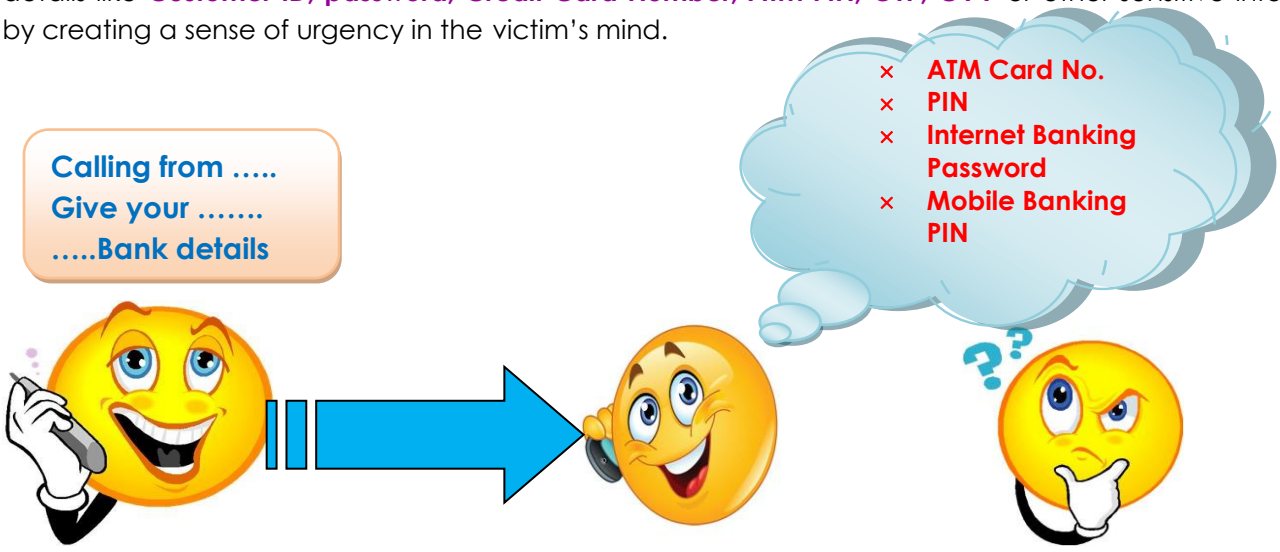
इण्डियन ओवरसीज़ बैंक **INDIAN OVERSEAS BANK**

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