इण्डियन ओवरसीज़ बैंक **Indian Overseas Bank**

AWARENESS AGAINST PHISHING

WHAT IS PHISHING ? :

"Phishing is the **criminally fraudulent process** of attempting to **acquire sensitive information** such as usernames, passwords and Card details by masquerading as a **trustworthy entity** in an electronic communication. "

In such incidents, the e-mail and the web pages appeared genuine. But actually it was not so. Throughout the world, for the past few years, such attacks are commonly reported in the media. Not only reputed Banks, but also e-Commerce Sites, Auction Sites, Social Networking Sites like eBay, paypal, Face Book etc., were affected. Even other orgnaisations like Income Tax Dept, Indian Banks Association (IBA)) were under this type of attack.

The motive here is ***identity theft***. What the fraudsters need is sensitive personal information, especially account/card number, password, PIN etc., to defraud the Banks without raising suspicion. They start gathering information (fishing) from gullible customers (fish), with the genuinely looking e-mail messages (bait). *The idea being that bait is thrown out with the hope that while most will ignore the bait, some will be tempted into biting.*

Our staff members, our customers and other general public may come under this type of attack. Only by awareness, one can avoid falling prey to such attack.

1. Banks or any other genuine organisation will **never** call from the customers on their own any confidential/sensitive information like PIN, password etc., through e-mail or telephone etc., Such information are already available with the Bank/Organisation.

2. Phishers typically include **upsetting or exciting (but false) statements** in their emails to get people to react immediately.

3. If the e-mail is received from the Bank to its customer, generally the **Bank will address with their name** or other personal details available with the Bank.(Eg., Dear Mr, M ,,,)

4. Mostly, the Designation of the person who has signed in the fake e-mail may be not relevant to the Bank.

5. In case of online transactions, it is the customer who initiates the action, where the minimum sensitive details are asked for identification and authentication purpose to permit the transaction. In such cases, the communication takes place through secured channel between the website and the browser (of the user).

6. One should be in a position to understand the difference between the genuine requirement ***where the user initiates action*** and in the earlier incident where the personal ***information is*** **solicited by e-mail**.

HOW TO COUNTER THE PHISHING ATTACK:

1. One should be suspicious of any email **with urgent requests** for personal / financial sensitive information.

2. Even if no suspicion is raised and the mail appears genuine, **the link in an e-mail should never be clicked**. Instead, one may physically type the correct web address (URL), directly in the browser's address bar. *(The link may show the genuine URL.*

However, on clicking, the link may take the user to another fake URL in the back ground. An experienced user only can notice this.)

3. It is always better to contact the Bank either by phone or through their website to confirm the genuineness of the mail/ message. (The contact details provided in the suspected e-mail should not be used without verifying)

4. Even if the mail appears genuine and the link is clicked in good faith and look and feel of the fake website/web page are almost identical to the legitimate one, ***it is reiterated again that Banks will never ask for the sensitive personal information(pasword,PIN)***. Hence, one should avoid filling out personal financial information as directed by the email messages.

5. One should make it a habit to enter the URL address of any banking, shopping, auction, or financial transaction website directly in the web browser and not to depend on displayed links.

6. Once it is suspected that the mail is a phishing mail the customer should forward the mail to the Bank or CERT-In (www.cert-in.org.in) a Central Government organization handling Computer related incidents in India. (incident@cert-in.org.in)

7. Some time it happens that the person receiving such mail is not a customer of the Bank mentioned in the mail. Generally, he/she ignores and deletes the mail. Instead, this fake mail should be forwarded to the concerned Bank or CERT-In (www.cert-in.org.in).

8. Forwarding the phishing mail will help the Bank to warn and protect other customers. When forwarding phishing messages, one should always include the entire original email with its original header information intact.

9. Everyone should regularly log into his/her online accounts and check the profile, transactions, balance, credit and debit card statements to ensure that all operations are legitimate. If anything needs clarification, the bank or the card issuer should be contacted immediately.

GENERAL PRECAUTIONS:

1. Even though the e-mail message is given as an example, since that is predominantly used to lure the public, one should not use the links given in an instant message, chat to get to any web page if it is suspected that the message might not be authentic or if the sender is not known.

2. Similarly, sensitive personal information solicited over phone (voice) or through SMS should also be handled cautiously as above.

3. It is better to avoid to access online banking through a publicly used computer (e.g., cyber café).

4. Similarly the PC /laptop used for online banking should be updated with the latest patches of the Operating Systems and the latest antivirus version.

5. Above all, last but not the least ,every customer should register for SMS alert facility for his/her accounts. In case of any transaction in the account, the customer will get an SMS alert.