ICICI BANK CUSTOMER EDUCATION SERIES

A TIMES BUSINESS ASSOCIATE COMMUNICATION

What is Phishing?

'Phishing' is an act of sending a fraudulent e-mail or creating a forged screen pop-up, in an attempt to capture customer's sensitive personal details like user ID, password, PIN, date of birth, CVV number, etc.

How is Phishing carried out?

Through e-mails

1. Unsuspecting customers are sent e-mails, which look similar to the authentic mails sent by their bank.
2. In these e-mails, the customer is asked to click on a link that redirects them to a fake website resembling the authentic site of the bank.
3. On this fake site, customers are asked to share their personal details.

Through pop-ups

1. A pop-up window appears on the screen while the customer is logged into his/her bank's website.
2. These pop-ups request the customer to re-enter his/her personal online identity details. Since this pop-up appears during the customer's online banking session, it can be easily mistaken to be an authentic request from the bank.
3. This is called 'In-session Phishing' and has surfaced recently.

Once the personal online information is submitted, the phisher then uses it to make online transactions, posing to be the genuine customer.

Your bank will never ask you for personal confidential details through e-mails or pop-ups.

Learn more on how to safeguard yourself from phishing, in next week's article.

ICICI Bank
www.icicibank.com

Upgrade your home computer to a legitimate (non-pirated) operating system with a firewall, latest version of browser and anti-virus / anti-spyware software.

Protect your Internet Password

Never use unprotected computers at cyber cafés for Internet Banking.

SAFE BANKING

We welcome your questions, suggestions and feedback on this column. Please use the 'Email Us' link at www.icicibank.com or send us an SMS to 53030. Please include your full name, address and phone number. Your comments may be edited for clarity and space.

BE AN INFORMED CONSUMER. Watch this space every Monday.