

ICICI BANK CUSTOMER EDUCATION SERIES

A TIMES BUSINESS ASSOCIATE COMMUNICATION



Beware of Vishing!

Mr. Sharma received a call from a person claiming to be an employee of his bank, asking him for his confidential banking details. Mr. Sharma obliged and later discovered unauthorised transactions in his account that left him poorer.

This is 'vishing', a form of phishing where a fraudster uses the phone instead of e-mail to lure people into revealing their confidential banking details.

If you get a call from a stranger asking you for your confidential banking details such as account number, debit/credit-card details, PINs, passwords, etc. report it to your bank with the following information:

- The calling number, if you have a caller ID facility.
- Any pertinent details of the conversation or recorded message.
- The call-back number, if indicated during the call.

When you add a payee through Internet banking, your bank will give you a secret code (in the case of ICICI Bank, a Unique Reference Number – URN) that you will need to use to authorise transfer of money online from your account to the new payee's account. Do not reveal this code to any stranger, even if the person claims to be an employee of your bank. If you receive an SMS with such a code from your bank without your having added a new payee, report it to your bank immediately.

Remember, your bank will never call, e-mail, or text you asking for your account number or related information that is already present in its records.



Never give your PIN, URN or other bank account details on an unsolicited phone call.

BE AN INFORMED CONSUMER. Watch this space every Monday.