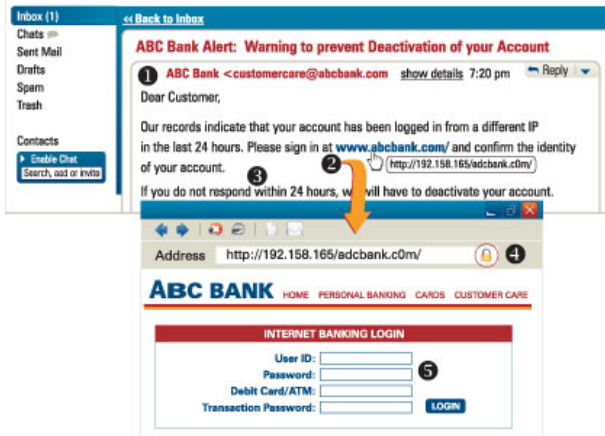



ICICI BANK CUSTOMER EDUCATION SERIES

A TIMES BUSINESS ASSOCIATE COMMUNICATION

How To Identify A Phishing E-Mail



- 1 The e-mail might appear to have come from your bank or financial institution, a company you do business with regularly, from someone you know or from your social networking site.
- 2 If you roll your cursor over the sender's address, it may reveal an incorrect address/URL. Some of the characters of the URL will be missing or made to closely resemble those of the genuine URL. In this case, the character 'b' of 'abcbank' is replaced with 'd'. The URL of the spoofed site will not match the URL of the legitimate site.
- 3 The e-mail may show urgency for action, and threaten to shut down your account unless you do as directed by it.
- 4 The padlock icon  may be missing.
- 5 Any e-mail asking for your personal and confidential data like passwords, CVV number, debit-card-grid codes, user ID, pass-codes, etc. is almost certainly a phishing attempt.

 **Do not respond to such phishing e-mails. Remember, your bank will never ask you for your confidential banking details.**



IMPORTANT: Reserve Bank of India issued Circular no. 54 on May 26, 2010 advising that remittance in any form towards participation in lottery schemes or any other money-circulation schemes can be fraudulent and is prohibited under Foreign Exchange Management Act, 1999.

BE AN INFORMED CONSUMER. Watch this space every Monday.