Beware of ‘phishing’

The growing menace of online theft of data of late is a matter of serious concern for many consumers and business organizations . The privacy and integrity of their personal data have indeed become a question mark. This article is intended to alert consumers about fraudulent Internet correspondence, also known as ‘phishing’, in which e-mail messages, instant messages and websites are used to deceive individuals into providing confidential, personal information. The term relates to the idea that people will ‘take the bait’ and disclose personal information, which can be used for credit card fraud and other serious violations of privacy.

Phishing e-mails generally appear to be sent from legitimate organisations, asking users to either reply or link to a web page to update their personal information. They sometimes contain an organisational logo and even a physical address, but the web address, or URL, does not match that of the legitimate organisation.

Among the data typically requested by phishers are the user’s name and address; Social Security number; account numbers and passwords; bank account and credit card information — sometimes even the account holder’s mother’s maiden name or other private information used for security purposes.

Here are some measures you can take to avoid getting ‘hooked’ by a phishing scheme:
Be alert to any unexpected e-mail, instant message, voicemail or fax that claims to be from a bank, credit card company, online service or charitable organisation with which you have an account or membership

If you do receive such a message, call the appropriate customer or donor service number (but not any number provided in the message) and verify whether it is legitimate
Do not respond to any e-mail, phone or fax instructions that prompt you to divulge your personal information

- Do not click on any links in a suspicious e-mail; clicking on such a link may cause the download of key-logging or ‘spyware’ programmes onto your computer
- Regularly log on to your online banking, credit card or other accounts and reconcile your statement balances to ensure that all transactions are legitimate
- Use up-to-date anti-virus software – including spam filters and even ‘anti-phishing’ programmes, which are available to help screen out potential phishers on websites and e-mails.

BANKS TOO WERE HIT: India's largest bank, the State Bank of India (SBI), had some months ago reported about an attempt at phishing to the Indian Computer Emergency Response Team (CERT-In). This organisation is associated with the ministry of communication and information technology and acts as a referral agency to the Indian e-community for incidents related to computer security. Banking sources indicate that besides SBI, three other international banks have informed CERT-In about attempts at phishing.
