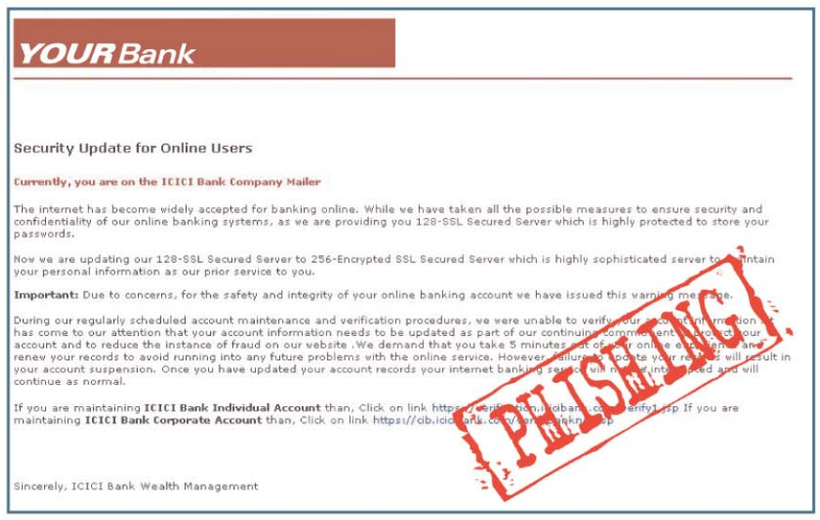
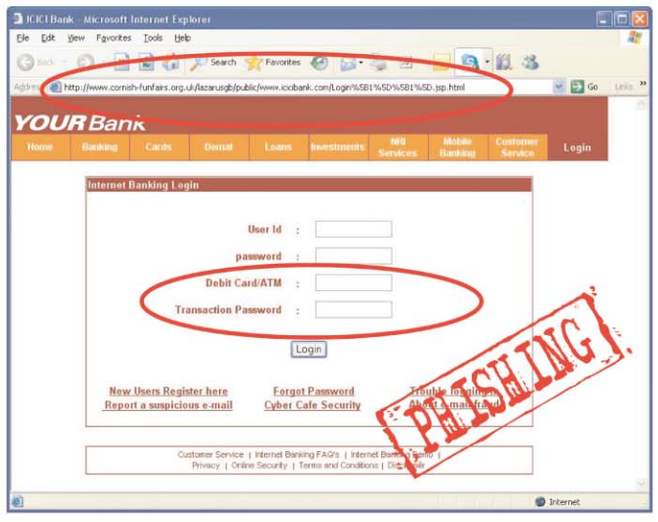
ICICI BANK CUSTOMER FIRST SERIES

TIMES BUSINESS ASSOCIATE COMMUNICATION

A consumer education initiative





URGENT: PLEASE CONFIRM YOUR BANK ACCOUNT RECORDS

FRAUDSTERS ARE ON THE PROWL, TRYING TO EXTRACT YOUR BANK ACCOUNT INFORMATION FROM YOU, FOR MISUSE. ARE YOU EQUIPPED TO IDENTIFY AND IGNORE THEM?

A popular actor-director recently lost Rs.60,258, when his account was used by a fraudster to purchase two air tickets through the Internet. He discovered this when he received his bank statement, where his account was debited for transactions he never made. This kind of theft is the act of modern thieves who misuse your accounts. The simplest thing they do is to send you an e-mail soliciting details required to siphon your money away. What can you do to protect yourself?

WHO IS A PHISHER?

Phishers are fraudsters trying to find information they can misuse. Always beware of e-mails from unknown senders. Treat such e-mails with caution, just as you would ignore a stranger on the street who tries to get friendly. Remember that getting your e-mail details is quite easy. Just because someone sent a mail to your correct ID, it is not reason enough for you to trust.

WHAT IS THE PHISHER LOOKING FOR?

Understand the key security components of your internet banking account. Your user ID, password, your mother's maiden name (or any such question to help you remember the password), your account number and your date of birth are all key details. Obviously, no one other than you and your bank, know ALL these pieces of information. The objective of the fraudster's e-mail is to get these details from you. Just as you would not hand over the keys to your house to a stranger, don't give out key information to anyone on e-mail.

DOs AND DON'Ts

- **Ignore e-mails that ask for your bank account details.**
- **Always TYPE the address of your bank (for example: www.xyzbank.com) in your browser window. Don't access it through links in e-mails.**
- **Do not provide your Internet Banking account user IDs or passwords to anyone.**
- **Do not fall prey to threats of dire action if you do not comply with requests for passwords.**

HOW CAN YOU BE TRICKED?

The thieves know that you will be careful. So they wear a mask. The mail is crafted to look like it is from your bank. The logo and name of the bank is copied to make you believe that the e-mail is 'authentic'. Some mails have a link and you are asked to enter your details there, as if you are logging into your account. Never access your account through a link in an e-mail. It may be disguised and lead you to fraudulent 'phishing' site. The only thing to remember is that the bank already has all the details about your account and will NEVER ask for them. E-mails asking you to approve, verify or update such information are usually fraudulent.

HOW DESPERATE CAN THEY GET?

Phishing is usually done as a mass mailer and may not be personalized. Some of them will have obvious spelling and grammatical errors. Fraudsters know that you may ignore their mail. They will scare you. They will point to something terrible that can happen – suspension of the account, for example – if you don't give the details. These are 'cyber daggers' they point at you. Treat these threats with contempt and ignore them. Your bank will not suspend your account without contacting you and such actions do not usually happen over e-mail. Forward such e-mails to your bank and expose the fraudsters, instead of obliging them.

Keep your Internet account safe and secure and never hand out your keys to cyber thieves.

Kindly send us your suggestions and comments by visiting the "Email Us" link at www.icicibank.com

DID YOU KNOW?

It is not very difficult for 'phishers' to get e-mail IDs. For example, social networking is so common today. Many of us leave personal details and e-mail IDs on such sites, to connect with our friends and other professionals. This information can be gathered and misused by phishers.