About Phishing (Potential Security Threats)

'Phishing' is a common form of Internet piracy. It is deployed to steal users' personal and confidential information like bank account numbers, net banking passwords, credit card numbers, personal identity details etc. Later the perpetrators may use the information for siphoning money from the victim's account or run up bills on victim's credit cards. In the worst case one could also become the victim of identity theft. A few customers of some other Indian banks have been affected by the attempt of phishing during the early 2006.

We would like you to be aware of methodologies in a 'Phishing' attack, do's and don'ts in sharing of personal information and the action to be taken in case you fall prey to a phishing attempt.

Methodologies:

- Phishing attacks use both social engineering and technical subterfuge to steal customers' personal identity data and financial account credentials.
- Customer receives a fraudulent e-mail seemingly from a legitimate internet address.
- The email invites the customer to click on a hyperlink provided in the mail.
- Click on the hyperlink directs the customer to a fake web site that looks similar to the genuine site.
- Usually the email will either promise a reward on compliance or warn of an impending penalty on a non compliance.
- Customer is asked to update his personal information, such as passwords and credit card and bank account numbers etc.
- Customer provides personal details in good faith. Clicks on 'submit' button.
- He gets an error page.
- Customer falls prey to the phishing attempt.

Don'ts:

1. Do not click on any link which has come through e-mail from an unexpected source. It may contain malicious code or could be an attempt to 'Phish'.
2. Do not provide any information on a page which might have come up as a pop-up window.
3. Never provide your password over the phone or in response to an unsolicited request over e-mail.
4. Always remember that information like password, PIN, TIN, etc are strictly confidential and are not known even to employees/service personnel of the Bank. You should therefore, never divulge such information even if asked for.

Do's:

1. Always logon to a site by typing the proper URL in the address bar.
2. Give your User Name and password only at the authenticated login page.
3. Before providing your User Name and password please ensure that the page displayed is an **https://** page and not an **http://** page. Please also look for the lock sign () at the right bottom of the browser and the verisign certificate.
4. Provide your personal details over phone/Internet only if you have initiated a call or session and the counterparty has been duly authenticated by you.
5. Please remember that bank would never ask you to verify your account information through an e-mail.

What to do if you have accidentally revealed password/PIN/TIN etc:

1. If you feel that you have been phished or you have provided your personal information at a place you should not have, please carry out following immediately as a damage mitigation measure.
    - Change your password immediately.
    - Report to the bank by clicking on the link Report Phishing on login page.
    - Check your account statement and ensure that it is correct in every respect.
    - Report any erroneous entries to Bank.
    - Use the other compensatory controls provided by the bank like setting the limits for demand draft and trusted third parties to zero, enabling high security, etc to minimize the risk.