Beware of Fake Websites, Phishing Email

Important Safety related Communique for Internet Banking Users

We wish to inform our esteemed customers that the URL address of our official website is www.sbimauritius.com

Our esteemed customers are also hereby cautioned against acting upon any unsolicited phishing emails and should avoid giving personal and confidential information such as 'User name' and 'Passwords'. Members are particularly advised not to open email from unknown sources or not to reply to or click on any link on the email.

Here are more security tips:

Important Security Tips For Safe Online Banking

1) Access your bank website only by typing the URL in the address bar of your browser.
2) Access you online banking by typing the URL www.sbimauritius.com and then clicking the Internet banking Box available there on your right hand side of the page
3) You can access the official website by typing the URL www.onlinesbiglobal.com in the address bar of your browser and then select the country Mauritius among the drop down menu available over there.
4) Do not click on any links in any e-mail message to access the site.
5) State Bank never sends e-mail and embedded links asking you to update or verify personal, confidential and security details. NEVER RESPOND to such e-mails/phone calls/SMS if you receive.
6) Do not be lured if you receive an e-mail/SMS/phone call promising reward for providing your personal information or for updating your account details in the bank site.
7) Having the following will improve your internet security:

8) Newer version of Operating System with latest security patches.
9) Latest version of Browsers (IE 11 and above, Mozilla Firefox 3.1 and above, Opera 9.5 and above, Safari 3.5 and above, Google chrome,etc.)
10) Firewall is enabled.
11) Antivirus signatures applied
12) Scan your computer regularly with Antivirus to ensure that the system is Virus/Trojan free.
13) Change your Internet Banking password at periodical intervals.
14) Always check the last log-in date and time in the post login page.
15) Avoid accessing Internet banking accounts from cyber cafes or shared PCs.

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 in 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.

Dont's:

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 id and password only at the authenticated login page.
3. Before providing your user id and password please ensure that the URL of the login page starts with the text ‘https://’ and is not ‘http:// ‘.The 's' stands for 'secured' and indicates that the Web page uses encryption.
4. Please also look for the lock sign ( ) at the right bottom of the browser and the verisign certificate.
5. Provide your personal details over phone/Internet only if you have initiated a call or session and the counterpart has been duly authenticated by you.
6. Please remember that the 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:

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 the following immediately as a damage mitigation measure.

- Please lock your user access immediately using 'Lock User Access' option given on the home page of www.onlinesbi.com
- Report to the bank by clicking on the link Report Phishing
- Check your account statement and ensure that it is correct in every respect.
- Report any erroneous entries to the 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.