# Don’t fall prey to phishing emails, fake websites. Important Safety related Communique for Internet Banking Users

**15.03.2016.**

Our esteemed customers are 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. We understand some fake websites like ‘www.sbimauritus.com’ have been wrongly created. While we are making our efforts to kill such fake websites, we request members to be careful while dealing with such emails.

**Important Security Tips For Safe Online Banking**

· Access your online banking by typing the URL www.sbimauritius.com orwww.onlinesbiglobal.com in the address bar of your browser.

· Do not click on any links in any e-mail message to access the site.

· SBI (Mauritius) Ltd 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.

· 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.

· Scan your computer regularly with Antivirus to ensure that the system is Virus/Trojan free.

· Change your Internet Banking password at periodical intervals.

· Always check the last log-in date and time in the post login page.

· 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. 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:**

· 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'.

· Do not provide any information on a page which might have come up as a pop-up window.

· Do not navigate to other websites while performing Internet Banking transactions.

· Do not leave your PC unattended when performing Internet Banking transactions.

· Never provide your password over the phone or in response to an unsolicited request over e-mail.

· Always remember that information like password, PIN 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.

· Avoid accessing Internet banking accounts from cyber cafes or shared PCs.

**Do's:**

· Always logon to a site by typing the proper URL in the address bar.

· Give your user id and password only at the authenticated login page.

· 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.

· Please also look for the lock sign ( ) at the right bottom of the browser and the VeriSign certificate.·

· Always log-off from SBIML Internet Banking window and close your browser when you have finished your transaction.

· 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.

· Please remember that the bank would never ask you to verify your account information through an e-mail.

· Check your Account Statements and balances regularly. Contact us on 213 8009 or 800 2009, if you find any unauthorised transactions immediately.

· Change your Internet Banking password at periodical intervals.

**What to do if you have accidentally revealed password/PIN 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.

Check your account statement and ensure that it is

correct in every respect.

Report any erroneous entries to the bank.

Contact us on Tolfree No. 8002009 or at email id: it@sbimauritius.com for any assistance required in that respect.