SBMNET
Security Tips

23 September 2010

Dear Valued Customer

SBM Internet Banking – Security Tips

At the State Bank of Mauritius, we are committed to make your online banking experience as secure as possible. We have adopted several measures and security standards to enhance the security of your funds and protection of your account. SBM's Internet Banking security tips set out simple steps you can take to ensure that your money and your personal details are safe and secure.

The following security tips help you make the right decisions and hence avoid costly surprises.

1. Accessing SBM Internet Banking the correct way

Always access SBM Internet Banking from SBM official website by typing the URL (http://www.sbmgroup.mu) into your browser and by clicking on the Internet Banking link provided on the website. To ensure the highest level of security, we suggest that you always make sure that you are using browser versions that we recommend. Microsoft Internet Explorer (versions 6.0 and above) or Netscape Navigator (version 6.2.x) browsers on the Microsoft Windows operating system will provide you with the best online experience.

2. Look for the following security indications

- Ensure that you are on the secure SBM Internet Banking website by checking that the URL begins with "**https**" rather than "http".
- Check whether the following icon  (in the form of a closed padlock) appears in the bottom right of the webpage
- Move your cursor on the icon above to check that "SSL secure (128 bit)" is displayed
- Verify the website certificate by double clicking on the icon displayed above and en sure that the following details are present:

    - Issued to sbmmur.sbmonline.com
    - Issued by www.verisign.com
    - Validity date on the certificate has not expired (valid from and to)

3. Safeguarding your Passwords

- NEVER disclose your Internet Banking Id and Password to ANYONE
- Choose a password that you can easily remember but hard-to-guess. For e.g. Partym@1 (Party time at one)

3. Safeguarding your Passwords (Cont'd)

- Use a combination of letters (upper and lower case), numbers and special characters (@, !, ~, etc) when choosing a password
- Do not use dictionary words or family related information when choosing password as these can be easily cracked and guessed
- Your Internet Banking password should be a unique one and not used for accessing other websites
- Change your password regularly to minimize the risk of having your password being compromised
- Do not use options such as "Auto Complete" or "Remember My Password"
- Change your password IMMEDIATELY if you feel that your password might not be secure
- Once you are logged in, SBM Internet Banking will NOT prompt you to re-enter your password details. In case you are asked to re-enter your password details through apop up window, kindly ignore and close the window
- Destroy any SBM correspondences containing your Internet Banking Id and Password details

4. Using Internet Banking in Public Places (Internet Cafés or free wireless access points)

- Avoid using SBM Internet Banking on shared PCs or on public PCs
- Never change sensitive details such as PIN or Password in public places
- Be wary of persons standing close to you when you are entering your password or PIN

5. Ending Your Internet Banking Transactions

- Sign out from the Internet Banking webpage to close an active session instead of just closing the window.
- Delete temporary files and cookies regularly after browsing the Internet

6. Protecting Your PC

- Ensure that no one has access to your PC
- Use a reliable antivirus product and ensure that it is updated regularly
- Configure your PC to obtain latest security patches for your operating system
- Keep your operating system, browser, e-mail up to date with the latest versions and patches
- Use a personal firewall and intrusion detection system to block/detect attacks or malicious programs on your systems
- Do not install free software from the Internet or from unreliable sources

7. Precautions for Emails

- Be wary of emails asking for PIN or Password. SBM never sends emails to collect password or PIN
- Do not click on hyperlinks embedded in emails or third party websites to access SBM's Internet Banking
- Use spam filters on your PC to protect yourself from receiving spam emails

8. Other Safety Measures

- Do not navigate to other websites while performing Internet Banking transactions.
- Do not leave your PC unattended when performing Internet Banking transactions.

9. Monitor your account regularly

- Check the last logon time which is displayed every time you log on to perform Internet Banking transactions
- Check your account statements regularly to protect yourself against frauds
- Contact SBM immediately in case of irregularities.

For more information please call us on 207 0111 or visit your nearest SBM branch or email us at sbm@sbmgroup.mu