Internet Banking
Security Tips

We are aware that security is the most important thing when completing financial transactions online. The security and privacy of your personal information is our priority. We're committed to help you stay safe when you bank online with us.

SBM's Internet Banking security tips set out simple steps you can take to ensure that your transactions and your personal details are safe and secure when transacting online.

1. Accessing SBM Internet Banking

Always access SBM Internet Banking from SBM official website by typing https://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 use of the *latest version of browsers.*

2. Look for Security Indications

- Ensure that you are on the **secure SBM Internet Banking website** by checking that the URL begins with "**https**" rather than "http".
- Look for a **closed padlock icon: ""** in the address bar; it indicates encryption is being used on the web page. This icon is located on the left of the URL on most recent browsers, but may vary in location on older ones.

- Verify the website certificate by double clicking on the icon displayed above and ensure that the following details are present:
  - Valid Security Certificate
  - Issued by DigiCert Inc
-

- SBM Internet Banking has been enhanced with **picture recognition** to protect customers against phishing (fake) website. Genuine SBM Internet Banking will **ALWAYS** display the image that you selected at registration for the service. **NEVER** trust a message asking you to confirm an image *different* from what was selected at the registration process.

3. Protect your Password

- **NEVER** disclose your Internet Banking UserID and Password to ANYONE
- **ALWAYS** choose an easily remembered but hard-to-guess password
- **Do NOT** use dictionary words or family information when choosing a password as these can be easily guessed or cracked
- To choose a **STRONG** password, use a combination of letters (upper and lower case), numbers and special characters (@, !, ~, etc)
- Your Internet Banking password should be **UNIQUE** and **NOT** be used for accessing other websites or social media platforms, such as Facebook, LinkedIn, etc.

- Never write down your Internet Banking password on your desk, paper or anywhere else
- Never save your password in clear text files on your PC

- **IMMEDIATELY** change your password if you feel your password has been compromised
- **CHANGE** your password regularly to minimize the risk of having your password compromised
- **DO NOT** use options such as "Auto Complete" or "Remember My Password"
- You will **NEVER** be prompted to re-enter your IB login details once you are logon your IB account. Remember, you will be prompted to enter **ONLY** your transaction password each and every time you perform an online transaction

4. **Using Internet Banking in Public Places (Cybercafés or free wireless access points)**
   - **DO NOT** use unsecure public Wi-Fi. Using an unsecured public Wi-Fi would allow unauthorized people to intercept any information while you are online.
   - **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/or intrusion detection system to block/detect attacks or malicious programs on your systems
   - Do not install free software from unreliable Internet sources

7. **Email Security**
   - Be wary of unknown emails asking for PIN or Password.
   - 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 Security Measures**
   - **DO NOT** navigate to other websites while performing Internet Banking transactions.
   - **DO NOT** leave your PC unattended when performing Internet Banking transactions.
   - **ALWAYS** logout from SBM Internet Banking when not in use.
   - **ALWAYS** keep your registered mobile number updated with the bank as Internet Banking send OTP (One Time Password) only to the registered mobile number.

9. **Monitor your account regularly**
   - Check the last logon time every time you log on your Internet Banking.
   - Check your account statements regularly to protect yourself against frauds

10. **SBM Contacts**
   - If you notice any suspicious activity relating to your online account, immediately contact our Customer Service on **(230) 2070111** or by email at **sbm@sbmgroup.mu**

All the safeguards in the world won't help you if you give your personal information away. Be smart and protect yourself online.

Disclaimer:
This document is for information purpose and is considered as a good practice.