Security Tips for SBM Bank Online Customers

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.

SBM's online services 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 Online Services

Always access SBM Online Services from SBM official website by typing https://www.sbmbank.co.ke into your browser and by clicking on the SPS link provided on the website. (https://sps.sbmbank.co.ke/account/logon)

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 secured website by checking that the URL begins with **"https:// "** rather than **"http://".**
- Look for a **closed padlock icon**: https:// "in the address bar; it indicates encryption is being used on the web page. The 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 to ensure that it is valid and details of issuer.

3. Protect your Password

- **NEVER** disclose your UserID and Password to ANYONE
- **ALWAYS** choose an easily remembered but hard-to-guess password as per the guidelines set
- **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 password should be **UNIQUE** and **NOT** be used for accessing other websites or social media platforms, such as Facebook, LinkedIn, etc.
    - o Never write down your password on your desk, paper or anywhere else
    - o 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"

4. Using SBM online services in Public Places (Cyber Cafés or free wireless access points)

- **DO NOT** access unsecure public Wi-Fi. Using an unsecured public Wi-Fi would allow unauthorized people to intercept any information while you are online.
- **AVOID** using 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 Online Session

- **SIGN OUT** from the online platform 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 SPS page
- 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 online transactions.
- **DO NOT** leave your PC unattended when performing SPS transactions.
- **ALWAYS** logout from online services when not in use.
- **ALWAYS** keep your registered mobile number updated with the bank as OTP (One Time Password) are only to the registered mobile number.

9. Monitor your account regularly

- Check your account statements regularly to protect yourself against frauds

10. SBM Contacts

- Contact SBM Bank (Kenya) Customer Service immediately whenever you notice suspicious activity relating to your online account.
- For more information please call us on +254 730 175 000, + 254 709 800 000 or visit your nearest SBM branch or email us at atyourservice@sbmbank.co.ke

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 purposes and is considered as a good practice.