Security Awareness Guidelines for Customers

Dear customers,
Since we at Safwa Islamic Bank are keen to provide you with our e-services at the highest standards and levels of information security in order to protect our clients confidential information, the bank must take the effective security measures and precautions and carry out the best standards of global information security to protect you from any risks that may occur while using our electronic services.

Our customers are reminded that Safwa Islamic Bank will never send an email containing links or attachments, send a text message or messages through social media or contact you to request confidential information (such as credit card number, ATM card number, the card's pin code, or request information related to the username or passwords to enter your bank account through our e-services such as: online banking and mobile banking). Please do not disclose this information under any circumstances.

In addition to the security implemented in our e-services, we underline the importance of your role in protecting your own banking information. This is why we recommend the following guidelines:

1- Do not disclose/share any of your confidential information:

- Your ATM card number or credit card number.
- Your national ID number.
- Your bank account number.
- The password or username you use for any electronic banking services (including ATM, online banking and mobile banking).

2- Follow guidelines to protect your data for credit cards

- Do not share any personal information related to data from the bank's e-cards (ATM cards or credit cards) and other information such as the card's pin code and the card's number.
- When using your card online, make sure to shop only from trusted and safe websites, keeping in mind that the bank adheres to the international Payment Card Industry Data Security Standard, PCI DSS, which is renewed annually.
- Do not keep the card's password accompanied with the credit card.

3- Follow these security rules to protect your e-services passwords

- Always protect your password and do not write it down or keep it accompanied with your credit card or your username.
- Use a complicated password that is hard for others to guess.
- Passwords should include letters, numbers and special characters.
- we olso recommended not linking the password to anything personal such as birthdays, names or serial numbers.
- Change your password regularly.
- Try to use a different password for every system, application or websites.

4- The importance of knowing the types of threats related to cyber fraud:

4.1 Phishing E-mail

Trolls send false emails/text messages asking users to visit a website similar to the bank's website and ask the users to update their data, such as: username, password, credit card, or bank account number.

4.2 Social Engineering

It is the process of accessing – or trying to access – confidential information. The imposter discloses the customer's information usually by convincing users that the person contacting them is authorized to access such data. For example, this person calls or contacts the user on social media and then introduces himself and tries to convince you that he is a bank representative. Then, he discusses personal details with you and confidential information of your bank accounts.

4.3 Email Spoofing

Sending a fake email asking for confidential or detailed information about your account, or some personal data, such as receiving a fake email in the name of the bank asking your confidential information where the sender is a different person seeking to obtain the customer's confidential banking information.

4.4 SMS Phishing

Type of fraud using text messages through mobile devices. The user is tricked into downloading viruses or other malware or requesting information on a mobile phone or other portable devices.

4.5 Fraud through Malware and Viruses

A type of malware and phishing software installed on the customer's devices without their permission.

4.6 Types of Fraud Related to Mobile Banking

- Mobile Malware - viruses and rootkits placed within traditional online banking applications and designed specifically for the mobile phone market.
- Third-Party Apps - These applications come from third parties with questionable security practices, or fraudsters create applications and load them with malware to enable access to banking information on the customer's mobile device.
- Unsecured Wi-Fi - An unsecured wireless network is a fast way for fraudsters to access mobile devices, either to control or access account information.

5- Instructions related to secure online banking/mobile banking services and fraud protection

- To visit Safwa Islamic Bank's website, always enter the following address in your browser's URL bar (https://www.safwabank.com/ar) and make sure the "https" symbol and the lock icon are present in the address bar, and when moving to the online banking link, Safwa Online (https://ibs.safwabank.com/IBS/index.jsp).
- Do not use any links mentioned in an email or text message to access the online banking service and do not answer any emails or text messages asking you to disclose confidential information.
- Use an internet browser that has good security controls such as pop-up blockers and double-check suspicious websites.
- The official application for Safwa Mobile Banking available only on the App Store and Google Play.
- Every time you complete your online/mobile banking transaction, make sure you sign out, and every time you sign in, check the last login date.

- Create and use your mobile password through the mobile settings, making it automatically lock if not used for a minute or two.
- Make sure there are updated antivirus programs on your personal laptop or the mobile device you use for your online/mobile banking services.
- Do not choose “Remember my password” in your browser to save or remember your username or password on your devices in a way that is understandable by others.
- Avoid using the online/mobile banking service from internet cafes, public places or using Free Wireless Connection.
- In case you changed your mobile number, inform the bank so you can be able to receive your SMS messages and one-time password (OTP) for e-services.

6- How to Protect yourself from ATMs frauds

- Make sure the keypad and the card reader is part of the machine and not externally placed on top of the original keypad.
- Make sure there's a surveillance camera around the keypad or above it.
- When entering the card into the reader, make sure there's a light on card data theft devices block this light.
- Make sure other individuals waiting in line are standing at an acceptable distance from you.
- Make sure no one is watching you while you enter your card's pin code.
- Stand close to the ATM and hide the keypad with your hand when entering your code.
- If you feel the ATM is not functioning normally, press the "Cancel" button, take your card out and inform the bank about that.
- In case your card got "stuck" in the ATM or the machine kept it, or in case it got last, you must immediately inform the bank.
- Don't be in a rush when using the ATM. Carefully place the card and cash in your wallet or purse before leaving the ATM.

7- Safe shopping using electronic cards

- Do not click on email links pretending to be a vendor or shopping websites. Instead, type the vendor's main URL address or shopping website in the browser's URL bar.
- Use the latest browser version as it has better protection features.
- Do not save your information:

Some websites have the "remember for later" feature, which saves your payment information for your next purchase. Cancel this feature to avoid keeping your card number in vendors' databases.

8- Report security suspicions or any online fraud

If you have any suspicions about an unauthorized online security breach of your accounts, or if there was an electronic transaction on your account done by others, you must inform Safwa Islamic Bank immediately by calling the Safwa Islamic Bank customer care line, 064602100, or visiting one of the bank's branches.

Note: these instructions represent the minimum procedures to be followed when using any of the electronic services, and they were issued to increase banking awareness about the use of electronic banking services without the bank taking any responsibility.