BYBLOS BANK SAL
IRAQ

Mobile Banking Application Security Notice

Mobile Banking Security

The security of your smartphone or other mobile device is very important, especially if you're using it for banking. You should pay at least as much attention to your mobile security as you do to your computer security. If your phone is lost or stolen, you should immediately inform the Bank in order to prevent unauthorized access to your accounts, identity theft, or other forms of fraud.

Byblos Bank's Mobile Banking App offers the full encryption and security suite that should be utilized for online banking. However, as with other areas, as technology becomes more advanced, you can never be too safe or too careful.

With this mind, there are certain precautions you should keep in mind when opting to go mobile.

1. Use automatic lock-out. Make sure your device is set to automatically lock itself out after not being used for a specified period of time and, if possible, requires that a strong alphanumeric password be entered in order to unlock it. This will help prevent unauthorized users from accessing the data and resources stored on your device if it is lost or stolen, or if you're not there to supervise its use.

2. Set a strong account password. Do not use your name, birth date, or any other easily identifiable personal information in your password as this might help hackers decipher it. In addition, try to change your password frequently.

3. Do not store personal or other sensitive information on your mobile device. If an unauthorized party accesses your device, you will be more vulnerable if you store personal information such as passwords and account numbers on the device. It is also recommended that you regularly delete the browser history, text messages and files from your device.

4. Stay updated. Just like your desktop or laptop, mobile devices need updates to patch vulnerabilities and fix software issues. Stay informed about such updates and make the necessary changes on a regular basis.

5. Download anti-malware protection for your phone. This software should be able to scan the device, identify and remove malware, and check applications for malware before downloading from application stores.

6. Stay off public Wi-Fi hotspots. Most public Wi-Fi hotspots are not secure, which means anyone connected to the hotspot may be able to monitor what you are doing. Only use secure Wi-Fi (encrypted wireless communications) or your carrier's 3G or 4G data connection. It's also a good idea to disable Wi-Fi whenever it's not in use. This reduces the chance of accidentally connecting to an unsecured or suspect network.

7. Bluetooth can be harmful. In public areas, others can detect your device and access it through Bluetooth. If that happens, you will be sent a message alerting you. However, it is safer to turn Bluetooth off, or put it in non-discoverable mode to make it invisible to unauthenticated devices.

8. Always secure your SIM (subscriber identity module) card with a password. If your mobile device is ever lost or stolen, this will help protect any private and sensitive information.

9. Use care when downloading apps. Download mobile apps only from reputable sources, preferably the Apple Store or Google Play, to avoid downloading applications containing malware or other harmful code.

10. Read the fine print. Take a moment to read an application's privacy policy in order to be aware of what they do with your private information and if the app will expose this data to other users or any potential buyer.

11. Be careful when using social networking applications. These apps may reveal more personal information (mobile numbers, names of trusted friends, etc.) than you want to unintended parties. Be especially careful when using services that track your location.

12. Do not "root" or "jailbreak" your mobile device. "Jailbreaking" is the process of removing the locked features or limitations imposed by your root operating system (e.g. iOS or Android). If you crack the manufacturer's security on your device, you not only invalidate your warranty, but also make your device much more vulnerable to attacks by fraudsters.

13. Make sure you delete all personal details if and when you sell your smartphone. If you sell your smartphone, it's crucial that you delete all personal information first. This can include SMS messages, emails, photographs, contact details and Internet links. Criminals can use such information to commit fraud against you, and/or pretend to be you.

14. Never open attachments or download applications from untrusted sources. Fraudsters use infected documents and applications to spread their malware and compromise

victims' smartphones. Never open an attachment or download an application from a person, website or any other source that you don't know or that you have doubts about.

15. Report the loss or theft of your mobile device. If you lose your device, report it immediately by visiting your branch or calling Customer Service at +961 1 20 50 50 so we can disable your Mobile Banking account and stop any attempt at identity theft.

16. Be ready to wipe your device. If your device is ever lost or stolen, you should know how to remotely wipe it which means removing all of your personal data and restoring it to its factory state. iPhones, iPads, Blackberries and Windows 7 devices come with this capability included in their operating systems, and you can download Android apps that will do it as well.

17. Always log out. When you are finished checking your balance, transferring funds between accounts, or paying a bill, be sure you log out of your account. As part of our security features, the Byblos Bank Mobile App and web page will automatically log you out after five minutes of inactivity, but you should never leave it to chance: a lot can happen in five minutes.