MOBILE BANKING SECURITY TIPS

Boston Private Bank & Trust Company takes great care to safeguard the security of your non-public personal information. More and more people are using their smartphones to manage their bank accounts every day. However, the convenience of mobile banking also brings with it a new set of potential security risks. Through the security of your mobile device and the security practices you adopt for mobile banking, you can help mitigate the risk of online fraud and protect your confidential information. The following are security tips and best practices to keep in mind when accessing your online banking account via a mobile device.

1. PASSWORD-PROTECT AND AUTO-LOCK YOUR PHONE

In addition to the Online Banking application, your mobile device itself should be protected with a password to ensure that no one but you will be able to access your accounts. It is also recommended that you set your phone to auto-lock after a set number of minutes.

2. AVOID STORING CONFIDENTIAL INFORMATION ON YOUR MOBILE DEVICE

Be cautious about what information you store on your mobile device. Saving your passwords on the device is not recommended. Regularly delete text messages and old calendar entries, clear your browser history, and delete files from your phone. In addition, be sure to clear sensitive information prior to disposing of, recycling, selling or giving away your mobile device.

3. TEXT MESSAGING

Text messages are not secure and may be intercepted, which is why you should never send personal, identifying, or confidential information via text message. This feature of our Mobile banking is currently not available, due to the security risks.

4. DOWNLOADING APPLICATIONS

Smartphone applications (apps) may contain malicious content. Be sure to check for a website certificate before downloading apps or files to your mobile device. App stores have different standards for the apps they offer to the public. Google's Android Market is available to all Android application developers, accepting nearly every application a developer submits. The iPhone App Store requires that apps be put through rigorous testing first. It is wise for users to be cautious when downloading apps from the Android Market. Android devices have reported malware intrusions. Read carefully the application's privacy policy to be aware of what they are doing with your private information.

5. MOBILE DEVICE PERFORMANCE

If you download an app and your phone starts performing differently (e.g., responding more slowly to commands or draining its battery more quickly), it could be a sign of malicious code, and it is probably best to take your device to your carrier.

6. REVIEW AND UTILIZE THE SECURITY OPTIONS AVAILABLE ON YOUR DEVICE

Consider additional measures such as security software and antivirus solutions. Refer to your phone's user manual or contact your mobile carrier for more information on these features. Also, be sure to check for and download available software updates regularly on your phone, as these updates may include fixes to any security flaws.

7. PUBLIC WI-FI AND BLUETOOTH CONNECTION

Don't connect to unencrypted Wi-Fi when accessing Online Banking from your mobile device. Most smartphones and tablets can use both wireless Internet and a mobile provider's 3G or 4G network. Avoid using Bluetooth in public places to prevent attackers from taking advantage of that connection by obtaining information, or downloading malicious code to your mobile device.

8. LOG OUT COMPLETELY

Be sure to log out completely every time you finish a mobile banking session. This will prevent someone from having easy access to your information if they get hold of your phone.

9. INFORM YOUR SERVICE PROVIDER IF YOUR MOBILE DEVICE IS LOST OR STOLEN

If your phone is lost or stolen, notify your service provider immediately so they can disable your device and reduce the risk of information being accessed. You may also want to consider logging into Online Banking from a computer to change your password for additional security of your data. Some devices like iPhones and BlackBerrys allow you to remotely wipe your personal data and restore your device to its factory state. For Android devices there are apps that will do this for you. Find out if your device has this option, and write down the steps for remotely wiping your device in case it's ever lost or stolen.