Mobile Device Protection

Create a complex passcode for your mobile device. Avoid using personal information (i.e., names and important dates) in your passcode. Do not share your mobile device passcode with anyone.

Enable available security features, such as an auto-wipe feature after excessive password failures or auto-lock after a specified time frame.

Keep your mobile device's software up-to-date. If your mobile device prompts you to install an operating system or firmware update, review the update and install it as soon as you can to address any identified security vulnerabilities in previous update(s).

Disable features not actively in use, such as Bluetooth, Wi-Fi, and infrared. Set Bluetooth-enabled devices to "non-discoverable" when Bluetooth is enabled.

Utilize antivirus software where applicable (i.e., Androids, Windows, etc.).

Do not root, jailbreak, or otherwise circumvent security controls on your device. Compromised security controls could result in the introduction of malware onto the device.

When finished with the device, lock it to require a passcode before the device can be used again.

Mobile Applications

Download and install mobile applications only from trusted sources authorized by the device manufacturer, such as Apple's App Store, Google Play, or the Windows Store.

Enable mobile device features to block mobile application downloads from unknown sources.

When available, require a passcode to download mobile applications to prevent unauthorized installation.

Protect yourself from fraudulent mobile applications by watching for these signs:

- Typos, poor image quality, or formatting issues.
- Low number of downloads.
- Negative user reviews.

Additionally, review other mobile applications created by the app developer to validate the application's legitimacy.

If possible, create a passcode on any mobile application you install that may have access to your personal information.

When finished with a mobile application, always "Sign Out" or "Log Off" rather than just closing it.

Be On Alert

People are trying to steal your personal information. Remember to be on alert for the following types of threats to your mobile financial services.

Social Engineering

Phishing is a social engineering tactic used to obtain personal information by masquerading as a trustworthy individual through electronic communications. Some specific types of phishing include spoofing, SMiShing, and vishing.

Unsecured Wireless Networks

If you can access an Internet network without entering a password or network key, unauthorized individuals are also able to do so. If you are on an unsecured wireless network, such as a mobile or WiFi hotspot, do not use your mobile device to transmit sensitive data.

Compromised Websites

Watch for potentially compromised websites. If the website has a security error or your browser gives you a warning about the site, use caution. If you go to one web address and are redirected to another, close your mobile device's browser immediately and remember:

When in doubt, don't click.