PARKSTERLING BANK

Mobile Banking Security Tips

With mobile banking usage on the rise so are the cyber security threats for mobile device users. Therefore, it's only natural that security be on the minds of both financial institutions and customers.

Take steps to avoid becoming a victim of fraud. In general, your mobile devices need to be protected just like your PC. You can never be too safe. Here is a list of mobile device security tips to help you protect your valuable private information:

- Consider a screen lock on your mobile device with a password or PIN feature. Many mobile phones offer this option, as well as other customizable security settings, which can help keep your phone and information secure.

- Never respond to urgent email or text message claiming to be from a bank or any company that requests your account information or personal details. Fraudsters may use these request to "phish" for your personal information.

- Always download apps from approved sources like your mobile service provider or mobile device manufacturer's marketplace. Fraudulent mobile apps may capture your personal information and transmit it to their servers. It's always better to start with your banks website to make sure you aren't being scammed.

- Do not use free public Wi-Fi connections for banking transactions. We recommend using your phone carrier's internet connections for enhanced security.

- Disable Bluetooth when not in use. In public areas, others can detect your phone and access it through Bluetooth. Disconnecting Bluetooth, a non-secure connection, helps prevent attackers from obtaining information or sending malicious code into your device.

- Do not store your PIN and personal data on your mobile devices. Remember to backup personal data, such as your contacts, documents, and photos so that they may be restored if your device is lost or stolen.

- You should always take advantage of any security features offered by your mobile device, mobile carrier, or bank. By not using security features, it leaves your personal and financial information open to anyone that may be looking for it.

- Be aware of shoulder surfing while accessing mobile banking. Never leave your mobile device idle while your banking session is still active.

- Learn how to remotely wipe your mobile device. If your device is ever lost or stolen, you should know how and be able to remotely wipe it - which means removing all of your personal data and restoring it to its factory state. These apps can also help you locate and recover your device when lost

- Always accept updates and patches to your device's software as soon as it's available. Just like your desktop or laptop, mobile devices need updates to patch vulnerabilities and fix software issues.

- Be sure you log out of your account when you are finished with your banking activities. You should never leave a chance where an account could be accessed prior to the inactivity auto log out feature takes affect.

- Report a stolen device immediately to law enforcement. Police need to know a device's make, model, and serial number to investigate theft. Write down your device's basic information somewhere secure before taking it out of your home or office.

- Regularly delete text messages and old calendar entries, clear browser history, and delete files. Remove all information prior to disposing of, recycling or donating your device.

- Do not use your full or partial Social Security number as a Personal Identification Number (PIN), user ID or password.