SmartPhone and Mobile Device Security Tips

South Central now offers mobile banking and we thought these tips would be useful to our members.

Lock Your SmartPhone: Set up a screen lock so the phone cannot be accessed or used without a password. Use a real alphanumeric password (not a 4-digit PIN) and ensure the screen is set to lock automatically after a few minutes of being idle.

Don't Leave Your SmartPhone Unattended: Don't leave your SmartPhone sitting around in public spaces. Carry your phone with you whenever possible and if your phone is not with you be sure to securely store it.

Don't Give your phone to strangers: If someone needs to make an emergency call and wants to use your phone think twice. Make the call for them and put it on speaker—you never know what information they could get if they had your phone in their hands.

Is your SmartPhone Up-To-Date: If you have been ignoring the system updates you should update? Many updates include enhancements to device security. When you get an update, you should install.

Use the Find my Phone service: There are free, very easy to use SmartPhone tools available that allow the tracking and wiping for many different types of SmartPhones. These tools allow the user to lock, track or wipe their SmartPhone remotely if lost or stolen. This not only protects your personal data, but it could help you recover a lost or stolen device.

Don't Download Apps from Untrusted Sources: Do not enable the "non-market Apps" setting on your Smartphone. These types of Apps are riddled with vulnerabilities. Only install Apps from the SmartPhone manufacturer's approved online App store.

Do your SmartPhone Apps Due Diligence: Do your homework! Read the permissions screen when you download and install new apps to your SmartPhone. Many Apps will let you know that they are accessing your location, call history, contacts, and other personal data. Realize too when these Apps deliver your SmartPhone information to other third-party companies for other uses.

Watch Attachments: Be careful about opening attachments sent to your SmartPhone by people you don't know. Many attachments are used by hackers to deploy malicious software and viruses.

Encrypt SmartPhone Data: Most new SmartPhones make it relatively simple to encrypt the contents of the phone. This ensures that even if the phone does fall into the wrong hands and is accessed because the screen lock was bypassed, some level of protection still remains for your personal data.

Your SmartPhone is aa Small Computer: Don't think of your SmartPhone as being "just a phone". It is a small l computer with a substantial storage of personal information in addition to phone numbers and contacs.