Banking locally

EVER AFTER

IS KEEPING YOUR INFORMATION SAFE

MOBILE SECURITY- CELL PHONES AND TABLETS

Mobile phones can be a convenient tool for a variety of financial tasks. Here are some security threats that can affect your mobile device:

- Loss or theft
- Malware (viruses)
- Privacy stealing "good" application
- Snooping or access by unauthorized people

Your mobile device is essentially a powerful computer with a small screen. Use the same precautions you would use with your laptop and consider additional basic security precautions which can protect you.

Security Precautions for Android Devices

- Avoid rooting the system. This is a process of modifying the mobile operating system to allow a great deal of customization, but doing so drastically increases the chance of malware threats to your device.
- Don't allow your device to install applications from unknown sources. This is a setting under "Security" in your device.
- Install a trustworthy anti-virus program. Scan your device for viruses on a regular basis.
- Remove applications you don't need. Understand and be picky about the permissions an application wants from you. A flashlight application should not require access to your contacts!
- Set a security lock that is a passphrase or PIN.
- Don't type passwords while people may be watching you or looking over your shoulder (called surfing). Don't leave your device unattended in a public place!
- Don't connect to an unknown or "open" (no security) Wi-Fi network.
- Avoid Phishing and Smsishing.
- Keep your device up-to-date with the latest version of the operating system. This prevents security threats due to software flaws.

Tip: Learn how to locate, lock or even wipe clean, your device should it be lost or stolen. Do this before your device goes missing!

Security precautions for Apple iOS devices (iPhone and iPad)

- Avoid jailbreaking the system.
- Set a security lock that is a passphrase or PIN.
- Don't type passwords while people may be watching or looking over your shoulder (called surfing). Don't leave your device unattended in a public place!
- Don't connect to an unknown or "open" (no security) Wi-Fi network.
- Avoid Phishing and Smsishing.
- Keep your device up-to-date with the latest version of the operating system. This prevents security threats due to software flaws.