USING MOBILE DEVICES SECURELY

Security Precautions

May, 2015

The keys to maintaining the security of applications on your mobile device is to install only from known, trusted, sources and to keep your apps current by installing updates as soon as they are available.

Mobile devices play a critical role in many people's personal and professional lives. The appeal of the mobile device has exploded, with the latest smartphones and tablets often having more capabilities than laptops made just a few years ago. Smartphones and other mobile devices can run thousands of apps, offering convenient and flexible options for business and entertainment. With apps, however, come some level of risk. Use the following tips to help maximize the security of your mobile device.

WHAT IS AN APP?

Think of an "app" as a software program for your mobile device. These programs range in complexity from a simple flashlight application to involved navigational systems or medical reference guides. Apps are often developed by third parties, and prices range from free to several hundred dollars. Apps allow you to customize your mobile device to your specific set of wants and needs. Many companies, including banks and financial institutions, offer apps to their clients designed to enhance the client experience.

Are all apps safe?

Apps are created by third party developers and are seldom created by the makers of your mobile device. This means that security features can vary widely, and criminals may try to take advantage of the strong demand to create apps that look legitimate, but contain malicious code or viruses. Installing unsafe apps could result in cyber criminals taking control of your device, including your personal information.

What can be done to improve the security of your mobile device?

By understanding and avoiding the potential dangers of mobile device apps you can greatly reduce your risk. The following tips can help you operate your mobile device securely.

- **Know your sources!** The first step to avoiding dangerous apps is to make sure you only download them from a known, trusted source. Be aware that this will reduce your risk, but may not completely eliminate it. Even well-known sources may contain some malicious apps. As a general rule, avoid apps that are brand new, have a limited number of downloads, or have little to no reviews or comments. The longer an app has been available, the more likely it is to be safe. Likewise, reading reviews will often help identify problems in advance.
- **Keep up your defenses.** Keep your apps updated and remove apps that you no longer use. Avoid the temptation to "jailbreak" your mobile device – this often negates your mobile device's built in security controls and can void your warranty or support contracts.
- **Pay attention to privacy controls.** Apps often request that you grant certain privileges and permissions. Depending on your device, you will most likely be prompted before granting permission. Take a moment to think about what the app is requesting access to – for example,

allowing an app to know your location by using geo-location services may result in public postings that list your whereabouts, allowing anyone to know where you are or where you've been. Apps that request access to your contacts or other personal information for no logical reason might be a red flag. If you are uneasy with the access the app is requesting, keep searching until you find another app that suits your purposes and does not ask for privileges that make you uncomfortable.

- **Be wary of in-app purchases.** Many apps allow the use of "in app purchases", whether for additional features, removal of advertising, or new content. For your own protection, do not store your app store credentials on your device. Configuring your device to require a password every time the in-app feature is activated will help to protect you against misuse, including from criminals who may have remotely hacked your device.