Monthly Security Tips NEWSLETTER

February 2013

How Do I Protect the Information on My Smartphone?

From the Desk of Paul Federighi, Chief Information Security Officer

We've come to depend on our smartphones so heavily it is hard to remember what we did before we had them. If you have a smartphone, you now carry a fully functional computer in your pocket or purse. That's a tremendous amount of information at your fingertips! Therefore, it is paramount that you safeguard the smartphone.

Common Risks for Smartphones
Take a moment to consider each of these areas:

- **Loss of device and information theft.** Smartphones are small and can easily be lost or stolen. Unauthorized users may access your accounts, address lists, photos, and more to scam, harm or embarrass you or your friends; they may leverage stored passwords to access your bank and credit card accounts, steal your money or make credit card charges; and gain access to sensitive material.

- **Social Engineering.** A common mobile threat is social engineering. Whether via text message, image, or application to download, an incoming communication may be an attempt to gain access to your information. A current example consists of a text message that comes from an unknown number, telling you that if you click on the link provided, you'll have access to thousands of free ringtones. If this sounds too good to be true, that's because it is. The link is in fact a malicious link. Clicking on it will compromise the security of your smartphone.

- **TMI (Too Much Information).** Guidelines for protecting privacy, safety, and reputation when sharing via computers also apply when sharing via smartphones. Mobile devices enable instantaneous capturing, posting, and distribution of images, videos, and information. They may also broadcast location information.

- **Public Wi-Fi.** Smartphones are susceptible to malware and hacking when leveraging unsecured public networks.

- **Bluetooth and Near Field Communications (NFC).** Bluetooth is a wireless network technology that uses short-wave radio transmissions to transmit voice and data. NFC allows for smartphones to communicate with each other by simply touching another smartphone, or being in proximity to another smartphone with NFC capabilities or a NFC device. Risks with using NFC and Bluetooth include eavesdropping, through which the cyber criminal can intercept data transmission, such as credit card numbers. NFC also has the risk of transferring viruses or other malware from one NFC-enabled device to another.

Simple Steps to Protect Your Smartphone:

1. **Update the operating system.** Smartphones are computing devices that need to be updated. Updates often provide you with enhanced functionality and enriched features, as well as fixes to critical security vulnerabilities. Your smartphone manufacturer should notify you whenever an update is available.

2. **Use of security software is a must.** As the smartphone market is increasing, so too is the amount of malware designed to attack smartphones. The software security solutions that are available for

desktops and laptops are not as widely available for smartphones. A key protection is to use mobile security software and keep it up-to-date. Many of these programs can also locate a missing or stolen phone, will back up your data, and even remotely wipe all data from the phone if it is reported stolen.

3. **Password-protect your device.** Enable strong password protection on your device and include a timeout requiring authentication after a period of inactivity. Secure the smartphone with a *unique* password – not the default one it came with. Do not share your password with others.

4. **Think before you click, download, forward, or open.** Before responding, registering, downloading or providing information, get the facts. No matter how tempting the text, image, or application is, if the download isn't from a legitimate app store or the site of a trusted company, don't engage with the message.

5. **Understand the terms of use.** Some applications claim extensive rights to accessing and leveraging your personal information. If the app requires more access to your account and/or device than is needed to run the service, do not continue. In addition, be aware that terms can change over time. Review your terms of use often.

6. **Be cautious with public Wi-Fi.** Many smartphone users use free Wi-Fi hotspots to access data (and keep their phone plan costs down). There are numerous threats associated with Wi-Fi hotspots. To be safe, avoid logging into accounts, especially financial accounts, when using public wireless networks.

7. **Disable Bluetooth and Near Field Communication (NFC) capabilities when not in use.** Capabilities such as Bluetooth and NFC can provide ease and convenience in using your smartphone. They can also provide an easy way for a nearby, unauthorized user to gain access to your data. Turn these features off when they are not required.

8. **Enable encryption.** Enabling encryption on your smartphone is one of the best ways to safeguard information stored on the device, thwarting unauthorized access.

9. **Securely dispose of your device.** With the constant changes and upgrades in the smartphone market, many are upgrading their devices on a regular basis. It is important that you wipe the information from your smartphone before disposal. Additionally, make sure any SD cards are removed and erased. If you are not redeploying the SIM card to another device, then make sure your personal information stored on the SIM card is erased or destroyed.

For More Information:
For additional information about securing mobile devices, please utilize the following resources:

- **About.com 14 Ways to Find a Stolen or Lost iPhone: http://ipod.about.com/od/iphonetroubleshooting/tp/14-Ways-To-Find-A-Lost-Or-Stolen-Iphone.htm**
- **FTC – How to Dispose Your Mobile Device Securely: http://www.consumer.ftc.gov/articles/0200-disposing-your-mobile-device**
- **University of Northern Colorado: http://www.unco.edu/cybersecurity/students/mobile.html**
- **US-CERT – Cyber Threats to Mobile Phones: http://www.us-cert.gov/reading_room/cyber_threats_to_mobile_phones.pdf**
- **Sophos – Android Tool: http://www.sophos.com/androidsecurity**
- **Microsoft – Secure Your Smartphone: http://www.microsoft.com/security/online-privacy/mobile-phone-safety.aspx**

Brought to you by:

MS-ISAC MULTI-STATE Information Sharing & Analysis Center™
A DIVISION OF CENTER FOR INTERNET SECURITY