State of Oklahoma
Monthly Cyber Security Tips Bulletin

March 2012 Volume 7, Issue 3

Mobile Apps: How To Use Them Safely

From the Desk of CPT Jeff Elliott, Oklahoma Office of Homeland Security

The use of mobile applications (apps) is increasing in parallel with the increased use in mobile devices. According to Gartner, "Worldwide mobile application store revenue is projected to surpass $15.1 billion in 2011… and by 2014 over 185 billion applications will have been downloaded from mobile app stores." The continued growth of mobile apps requires a spotlight on security. The risks include access to information such as physical location or contacts lists, as well as the ability for the apps to download malware, such as keyloggers or programs that eavesdrop on phone calls and text messages. Hackers are quickly learning how to harvest legitimate applications and repackage them with malicious code before selling/offering them on various channels. The Institute of Electrical and Electronics Engineers (IEEE), a global technical professional association, predicts that 2012 will see an upsurge in cell phone hacking through the use of mobile applications on smartphones.

What steps can users take to minimize risk when it comes to using mobile device apps? Here are a few tips:

- **Make sure you actually need an app.** Every time you download an app you open yourself to potential vulnerabilities. Only download those apps you deem necessary with the understanding of the risks involved.

- **Be careful about which app store you use.** If you do decide to download an app, be aware of which app store you use. App stores have different standards for which apps they will offer to the public. Some app stores require apps to be put through rigorous testing first, while other stores accept all apps.

- **Do research and check the source.** If you're downloading an app, it is wise to do research on the application itself, the sponsoring company, and/or the developer's website. Be cautious about downloading new applications, as they may contain coding bugs that haven't yet been addressed. Most app markets post user reviews on the apps that they offer. Look for apps that have a high number of reviews. Take time to read the app's privacy policy. Check to see if the app needs access to and will report your position via GPS and will it expose your private and personal information to other users or any potential buyer of that data? You want to be aware of what apps are doing with your location and private data.

- **Password-protect your mobile device.** Your mobile device should be protected with a strong password. Make sure that the passwords are not stored in your device. Do not enable the apps to remember your password for your device and set your device to auto-lock after a few minutes.

- **Learn how to remotely wipe your mobile device.** If your device has a remote wipe feature you should enable it. If the device is lost or stolen, this will allow you to remotely remove all of your personal data and restore it to its factory settings.

- **Don't use public Wi-Fi when performing financial transactions.** Most mobile devices can use both wireless Internet and a mobile provider's 3G or 4G network. Use only 3G or 4G networks for any secure transactions such as banking.

- **Be alert to changes in your mobile device's performance.** If you download an app, and your device starts performing differently (for example- responding slowly to commands or draining its battery faster) that could be a sign that malicious code is present on the device.

- **Update Apps.** Update all apps when notified.

- **Disable Bluetooth settings on your mobile device whenever it is not in use**. If left on, someone could potentially pair to your device and obtain information or take over your device.

- **Follow your organization's policies**. If your mobile device is provided as part of your job, be sure to follow the rules and procedures established by your organization.

Resources for more information:

Multi-State Information Sharing and Analysis Center
http://msisac.cisecurity.org/newsletters/

Gartner
http://www.gartner.com/it/page.jsp?id=1529214

Tips for safe use of geo-location apps
http://lastwatchdog.com/isaca-backs-regulation-location-based-apps

National Cyber Security Alliance
www.Staysafeonline.org

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Brought to you by:

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