OUCH! | January 2015

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

Securely Using Mobile Apps

Overview

Mobile devices, such as tablets and smartphones, have become one of the primary technologies we use in both our personal and professional lives. What makes mobile devices so versatile are the millions of apps we can choose from. These apps enable us to be more productive, instantly communicate and share with others, train and educate or just have more fun. However, with the power of all these mobile apps come risks. Here are some steps you can take to securely use and maintain your mobile apps.

Guest Editor

Chris Crowley in an independent consultant, certified SANS instructor and course author. He is active on Twitter **@CCrowMontance** and on Google plus: **+ChrisCrowley**.

Obtaining Mobile Apps

The first step is making sure you always download them from a safe, trusted source. Remember, just about anyone can create a mobile app, so you have to be careful where you get them from. Cyber criminals have honed their skills at creating and distributing infected mobile apps that appear to be legitimate. If you install one of these infected apps, these criminals can take control of your mobile device to read your emails, listen to your conversations and harvest your contacts. By downloading apps from only well-known, trusted sources, you reduce the chance of installing an infected app. What you may not realize is the brand of mobile device you use determines your options.

For Apple devices, such as an iPad or iPhone, you can only download mobile apps from a managed environment: the Apple App Store. The advantage to this is Apple does a security check of both the mobile apps and their authors. While Apple cannot catch all the bad guys or all the infected mobile apps, this managed environment helps to dramatically reduce the risk of you installing an infected app. In addition, if Apple does find an app in its store that it believes is infected, it will quickly remove the mobile app. Windows Phone uses a similar approach to managing applications.

Android mobile devices are different. Android gives you more flexibility by being able to download a mobile app from anywhere on the Internet. However, with this flexibility comes more responsibility. You have to be more careful about what mobile apps you download and install, as not all of them are being reviewed. Google does maintain a managed mobile app store similar to Apple's, called Google Play. The mobile apps you download from Google Play have had some basic checks. As such, we recommend you download your mobile apps for Android devices only from Google Play. Avoid downloading Android mobile apps from other websites, as anyone, including cyber criminals, can easily create and distribute malicious mobile apps and trick you into infecting your mobile device. As an additional protection, consider installing anti-virus on your mobile device.

The key to securely using mobile apps is to install apps only from trusted sources, make sure your apps are updated and you verified the permissions.

To reduce your risk even more, avoid apps that are brand new, that few people have downloaded or that have very few positive comments. The longer an app has been available or the more positive comments it has, the more likely that app can be trusted. In addition, install only the apps you need and use. Ask yourself, "Do I really need this app?" Not only does each app potentially bring new vulnerabilities, but also new privacy issues. If you stop using an app, remove it from your mobile device. (You can always add it back later if you find you need it.)

Finally, you may be tempted to jailbreak or root your mobile device. This is the process of hacking into it and installing unapproved apps or changing existing, built-in functionality. We highly recommend against jailbreaking or rooting, as it not only bypasses or eliminates many of the security controls built into your mobile device, but often also voids warranties and support contracts.

Permissions

Once you have installed a mobile app from a trusted source, the next step is making sure it is safely configured and protecting your privacy. Installing and/or configuring mobile apps often requires that you grant certain permissions. Always think before authorizing any access, "Does your app really need those permissions to do its stated job?" For example, some apps use geo-location services. If you allow an app to always know your location, you may be allowing the creator of that app to track your movements; perhaps they can even sell that information to others. If you do not wish to grant the permissions an app is requesting, shop around for another app that meets your requirements. Remember, you have lots of choices out there. Apple devices allow some permissions to be changed in Settings or at runtime, such as access to geo-location information. Windows and Android mobile devices are different. They present you with an all-or-nothing approach. If you do not grant all of the specified permissions, you can't install the app.

Updating Apps

Mobile apps, just like your computer and mobile device operating system, must be updated in order to remain current. Criminals are constantly searching for and finding weaknesses in apps. They then develop attacks to exploit these weaknesses. The developers that created your app also create and release updates to fix these weaknesses and protect your devices. The more often you check for and install updates, the better. Most platforms allow you to configure your system to update mobile apps automatically. We recommend this setting. If this is not possible, then we recommend you check at least every two weeks for updates to your mobile apps. However, when your apps are updated, always make sure you verify any new permissions they might require.

Securing The Human Blog

Be sure to frequent the STH Blog for recent articles and trends on security awareness. This month, we cover key topics for Electric Utilities. More at http://www.securingthehuman.org/info/173402.

Resources

Social Engineering:	http://www.securingthehuman.org/ouch/2014#november2014
Disposing Your Mobile Device:	http://www.securingthehuman.org/ouch/2014#june2014
Securing Your New Tablet:	http://www.securingthehuman.org/ouch/2013#december2013
Common Security Terms:	http://www.securingthehuman.org/resources/security-terms
SEC575: Mobile Device Security Course:	http://www.sans.org/sec575

License

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus