The Monthly Security Awareness Newsletter for Everyone

OUCH!

IN THIS ISSUE...

Securely Using Mobile Apps

Overview

Mobile devices, such as tablets, smartphones, and watches, 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 comes risks. Here are some steps you can take to securely use and make the most of your mobile apps.

Guest Editor

Joshua Wright is the technical director at Counter Hack and a senior instructor with the SANS Institute. He is the author of SEC575: Mobile Device Security and Ethical Hacking and Hacking Exposed: Wireless. Reach Josh on Twitter **@joswr1ght**.

Obtaining Mobile Apps

The first step is making sure you always download mobile apps from a safe, trusted source. Cyber criminals have mastered their skills at creating and distributing infected mobile apps that appear to be legitimate. If you install one of these infected apps, criminals can take complete control of your mobile device. 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 downloading apps.

For Apple devices, such as an iPad or iPhone, only download mobile apps from the Apple App Store. The advantage to this is Apple does a security check of all mobile apps before they are made available. While Apple cannot catch all the infected mobile apps, this managed environment helps to dramatically reduce the risk of 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.

Securely Using Mobile Apps

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 which mobile apps you download and install, as not all of them are 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 passed some basic security 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, install anti-virus on your mobile device when possible.

The key to securely using mobile apps is to install apps only from trusted sources, to install updates when available, and to grant only the required app permissions.

Regardless of which device you are using, an additional step you can take is to 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, the more people that have used it, and 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, never jailbreak or root your mobile device. This is the process of hacking into it and installing unapproved apps or changing existing, built-in functionality. This 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, make sure it is safely configured and protecting your privacy. Always think before allowing a mobile app access: do you want to grant the app the permission it asks for, and does the app really need it? For example, some apps use geo-location services. If you allow an app to always know your location, you

Securely Using Mobile Apps

may be allowing the creator of that app to track your movements, even allowing the app author to sell that information to others. If you do not wish to grant the permissions, deny the permission request or shop around for another app that meets your requirements. Remember, you have lots of choices out there.

Updating Apps

Mobile apps, just like your computer and mobile device operating system, must be updated to stay 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 devices 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. Finally, when your apps are updated, always make sure you verify any new permissions they might require.

Subscribe To OUCH!

Receive OUCH! monthly in your email inbox. Join the community and subscribe to the OUCH! security awareness newsletter at https://securingthehuman.sans.org/ouch.

Resources

Social Engineering:	https://securingthehuman.sans.org/ouch/2017#january2017
Disposing Your Mobile Device:	https://securingthehuman.sans.org/ouch/2016#december2016
Securing Your New Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016
OUCH Archives & Translations:	https://securingthehuman.sans.org/ouch/archives
Mobile Device Security Course:	https://sans.org/sec575

License