OUCH! | February 2012

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

- Obtaining Apps
- Configuring & Using Apps
- Updating Apps
- In-App Purchases

Securing Your Mobile Device Apps

GUEST EDITOR

Kevin Johnson is the guest editor for this issue. Kevin is a senior security consultant at Secure Ideas, runs MySecurityScanner.com, and is a senior instructor with the SANS Institute. You can learn more about his work at www.secureideas.net and www.mysecurityscanner.com.

OVERVIEW

Mobile devices have become one of the primary tools we use in both our personal and professional lives. One of the things that makes mobile devices so powerful is that there are thousands of apps we can select from and use. However, with the tremendous power and flexibility of apps come a number of risks you must be aware of. In this newsletter we cover the dangers of mobile device apps and how you can install, use, and maintain them securely.

OBTAINING APPS

The first step in using apps is making sure you always download them from a secure, trusted source. Cyber criminals will create malicious apps that look real, but which may be infected with viruses or worms. If you inadvertently install one of these apps, cyber criminals can take control of your mobile device. By downloading apps from only well-known, trusted sources you reduce the chance of installing an infected app. However, even in well-known online app markets, some malicious apps can still be found. This is especially true for devices like the Android where the app markets are not tightly controlled. To reduce your risk, avoid apps that are brand new, that few people have downloaded, or that have very few comments. The longer an app has been available or the more positive comments it has, the more likely that app can be trusted. Finally, install only the apps you need and use. Each additional app brings the potential for new vulnerabilities, so if you stop using an app, remove it from your mobile device.

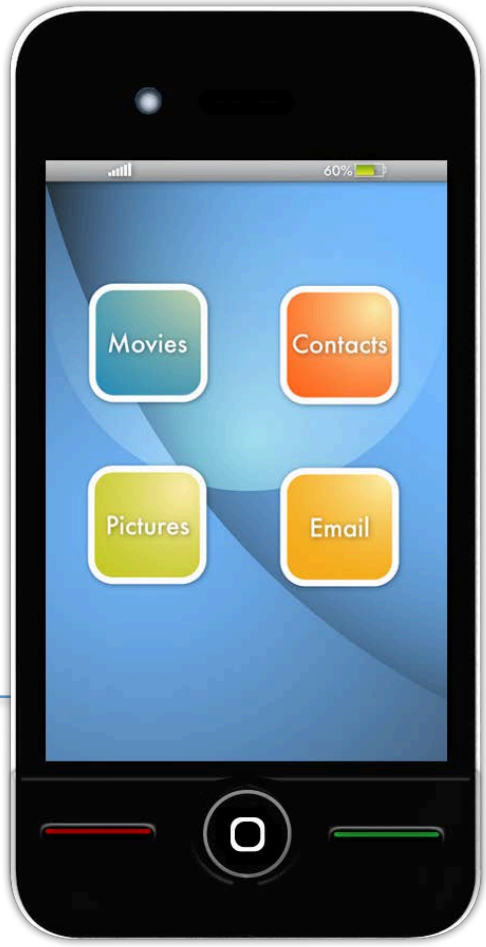
In addition, you may be tempted to jailbreak or root your own mobile device, the process of hacking into it and installing unapproved apps or changing existing functionality. We highly recommend against this, as jailbreaking not only bypasses or eliminates many of the security controls built into your mobile device but often voids any warranties or support contracts.

Securing Your Mobile Device Apps

CONFIGURING & USING APPS

Once you have installed an app from a trusted source, the next step is making sure it is safely configured and protecting your privacy as well. Installing and/or configuring certain applications requires that you grant certain privileges and permissions. Depending on the device, these applications will prompt you before authorizing. Always think before authorizing any access, does your app really need those permissions? For example, some apps use geo-location services. If you allow an app to know your location, you may be allowing the creator of that app to track your movements. In addition, any public postings you make may include your location, allowing anyone to know where you are or prove where you have been. If you do not like the permissions an app is requesting, simply find another app that better fits your requirements.

Be careful when using apps that request or store sensitive information. Even if the app is legitimate, there is no guarantee that the developer used good coding practices to protect your information while stored on the device or while transmitted over the Internet. Applications that consolidate sensitive information can be very convenient, but they are also targets for cyber criminals. Read the detailed description about the app and reviews from other users to see if there have been any security issues.



The key to maintaining secure mobile device apps is install apps only from trusted, secure sources and make sure they are updated.

UPDATING APPS

Apps, just like your computer and mobile device operating system, must be updated in order to remain current. Bad guys are constantly searching for and finding weaknesses in apps. They then develop attacks to exploit these weaknesses. The app 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. We recommend that you monitor your app stores and update your apps at least once a month. In addition, some apps can be set to update

Securing Your Mobile Device Apps

automatically, but please note that this may also automatically grant additional permissions if requested by that app.

IN-APP PURCHASES

Many applications today allow you to purchase additional features, new content, or the removal of advertising. A common mistake some people make is to store their app store credentials locally on their device, allowing them to easily make future purchases within an application. We highly recommend you do not allow your mobile device to save your app store credentials, log-in information, or payment information. Although convenient, this information may be available to, or misused by, anyone who has access to your mobile device, including the bad guys if your device has been remotely hacked. An alternative is to use gift cards or one-time use virtual credit card numbers instead.

CONCLUSION

We strongly encourage you to follow all the best practices discussed here. Mobile devices and apps are still a relatively new and fast growing field. In addition, one of the challenges we all face is that there are few options available for security software to help protect you and your apps. You are the best defense for your mobile devices.

RESOURCES

Some of the links shown below have been shortened for greater readability using the TinyURL service. To mitigate security issues, OUCH! always uses TinyURL's preview feature, which shows you the ultimate destination of the link and asks your permission before proceeding to it.

Sophos Webcast on Android Security:
http://preview.tinyurl.com/73q5u76

5 Ways to Protect Your Mobile Apps:
http://preview.tinyurl.com/5wpghmp

iPhone Security Overview:
http://preview.tinyurl.com/783hg2v

iPhone App Insecurity:
http://preview.tinyurl.com/3w5a5cc

Common Security Terms:
http://preview.tinyurl.com/6wkpae5

SANS Tip of the Day:
http://preview.tinyurl.com/6s2wrkp

LEARN MORE

Subscribe to the monthly OUCH! security awareness newsletter, access the OUCH! archives, and learn more about SANS security awareness solutions by visiting us at http://www.securingthehuman.org