Securely Using Mobile Apps

Overview

Mobile devices, such as tablets, smartphones, and smartwatches, have become one of the primary technologies we use in both our personal and professional lives. What makes these devices so powerful are the thousands of apps we can choose from. These apps enable us to be more productive, communicate and share with others, train and educate, or just have more fun. Here are steps you can take to securely use and make the most of today's mobile apps.

Obtaining Safe Mobile Apps

Cyber criminals have mastered their skills at creating and distributing malicious apps that appear to be legitimate. If you install one of these apps, criminals can often take complete control of your mobile device or data. This is why you want to ensure you only download safe mobile apps from trusted sources. What you may not realize is that the brand of mobile device you use determines your options for downloading apps.

For Apple devices, only download mobile apps from the Apple App Store. The advantage here is that Apple does a security check of all mobile apps before they are made available to customers. While Apple cannot catch all malicious apps, this managed environment dramatically reduces the risk of downloading one. In addition, if Apple does find an app that it believes is malicious, it will quickly remove it.

For Android devices, only download mobile apps from Google Play, which is maintained by Google. Similar to Apple, Google does a security check of all apps before they are made available to customers. The difference with Android devices is that you can also enable certain options that allow you to download mobile apps from other sources. We highly recommend against this since anyone, including cyber criminals, can easily create and distribute malicious mobile apps and trick you into infecting your mobile device.
Regardless of which brand you are using, research an app before downloading it. Look at how long the mobile app has been available, how many people have used it, and who the vendor is.

The longer an app has been publicly available, the more people that have used and left positive comments about it, and the more often the app vendors update it, the more likely the app can be trusted. In addition, install only 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 or no longer find it useful, remove it from your mobile device (you can always add it back later if you find you truly need it).

Apps Privacy and Permissions

Once installed, make sure the app is protecting your privacy. Does that app really need access to your location, microphone, or contacts? When you enable permissions, you may be allowing the creator of that app to track you, even allowing them to share or sell your information to others. If you do not wish to grant these permissions, simply deny the permission request, grant the app the permission only when it's actively being used, 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. Criminals are constantly searching for and finding new weaknesses in apps and developing ways to exploit these weaknesses. The app's developers 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 automatically update mobile apps. We highly recommend enabling this setting.

Mobile apps are key to making the most of your devices. Just be careful of the ones you select and make sure you use them safely and securely.

Guest Editor

Domenica Crognale is a quality assurance engineer and a certified instructor with the SANS Institute. She is a co-author of FO585: Smartphone Analysis In-Depth. Reach Domenica on Twitter @domenicacrognal.

Resources

The Power of Updating: https://www.sans.org/newsletters/ouch/the-power-of-updating/
Privacy: https://www.sans.org/newsletters/ouch/privacy/
Translated for the Community by: