Securing Your Mobile Devices

Overview

Mobile devices are an amazing and easy way to communicate with friends, shop or bank online, watch movies, play games, and perform a myriad of other activities. Since these devices are such an important part of your life, it is essential to keep you and your devices safe and secure.

Securing Your Devices

It may surprise you to know that the biggest risk to your mobile device is most likely not cyber criminals but you. You are far more likely to lose or forget a mobile device than have someone hack into it. The number one thing you should do to protect your device is enable automatic screen locking when the device is idle. This means that to use your device, you have to unlock the screen with a strong passcode, your face, or your fingerprint. This helps ensure that it is much harder for anyone else to access your information if your device is lost or stolen. As a bonus, for most mobile devices, enabling the screen lock also enables encryption, helping protect the data stored on the device.

Here are several more tips to help protect your devices:

1. **Updating**: Enable automatic updating on your devices, so they are always running the latest version of the operating system and apps. Attackers are always looking for new weaknesses in software, and vendors are constantly releasing updates and patches to fix them. Keeping your devices up to date makes them much harder to hack. When choosing a new Android device, look at the vendor's commitment to keeping the device updated. Apple iOS devices are updated by the company itself, while Android mobile devices are updated by the vendor that sold you the device, and not all vendors actively update their devices. If you are using an old device that is no longer supported or cannot be updated, consider purchasing a new device that is fully supported.

2. **Tracking**: Install or enable trusted software to remotely track your mobile device over the Internet. This way, you can connect to it over the Internet and find its location if your device is lost or stolen or remotely wipe all of your information in a worst-case situation.

3. **Trusted Mobile Apps**: Only install apps you need and stick to trusted sources. For Apple iOS devices such as iPads or iPhones, that means Apple's App Store. For Android devices, use Google Play; for Amazon tablets, utilize the Amazon App Store. While you may be able to install apps from other sites, these are not vetted and are far more likely to be infected or outright malicious, either of which could compromise your privacy. Also, check to make sure the app has lots of positive reviews and is actively updated by the vendor before downloading it. Stay away from brand new apps, apps with few reviews, or apps which are rarely updated.

4. **Privacy Options**: Mobile devices collect extensive information about you, especially since you take them everywhere you go. Thoroughly review your device's privacy settings, including location tracking, and make sure sensitive notifications (such as verification codes) don't appear on-screen when the device is locked.

5. **Work**: Be sure any mobile device you use for work is authorized for work use. When at work, be extra careful and never take any pictures or video that may accidentally include sensitive information, such as pictures of whiteboards or computer screens.

Your mobile devices are a powerful tool – one that we want you to enjoy and use. Just following these few simple steps can go a long way to keeping you and your devices secure.

Guest Editor

Jeroen Beckers is a mobile security expert at NVISO, co-author of the OWASP MASVS and MSTG, instructor for the SANS institute and author of the SEC575: Mobile Device Security and Ethical hacking course. You can find Jeroen via LinkedIn on https://www.linkedin.com/in/beckersjeroen/.

Resources

Updating: https://www.sans.org/newsletters/ouch/the-power-of-updating
Securely Using Mobile Apps: https://www.sans.org/newsletters/ouch/securely-using-mobile-apps/
Messaging / Smishing Attacks: https://www.sans.org/newsletters/ouch/messaging-smishing-attacks
Making Passwords Simple: https://www.sans.org/newsletters/ouch/making-passwords-simple
Vishing - Phone Call Attacks and Scams: https://www.sans.org/newsletters/ouch/vishing

Translated for the Community by: