The Monthly Security Awareness Newsletter for Everyone

Securing Your Mobile Devices

Overview

Your 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 your devices are such an important part of your life, here are some simple steps 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 not hackers, but most likely you. You are far more likely to lose or forget a mobile device then have someone hack into it. The number one thing you should do to protect your devices is enable automatic locking of the screen, often called a screen lock. This means every time you want to use your device you first have to unlock the screen, such as with a strong passcode or your fingerprint. This helps ensure that no one can access your device if it is lost or stolen. Here are several more tips to help protect your devices:

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 new updates and patches to fix them. By always running the latest operating system and mobile apps, you make it much harder for anyone to hack into your devices.

Tracking

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

Trusted Apps

Only download apps you need and from trusted sources. For iPads or iPhones, that means download apps from the Apple App Store. For Android, download apps from Google Play; for Amazon tablets, stick with the Amazon App Store. While you may be able to download apps from other sites, these are not vetted and are far more likely to be infected. Also, before downloading an app, check to make sure it has lots of positive reviews and is actively updated by the vendor. Stay away from brand new apps, apps with few reviews, or ones that are rarely updated. Finally, regardless of where you got your app, once you no longer need or actively use the app, we recommend you delete it from your device.

Privacy Options

When installing a new app, make sure you review the privacy options. For example, does the app you just downloaded really need to have access to all your friends' and contacts' information? We also recommend you disable location tracking for everything, then enable location for only the apps you feel need it. If you are uncomfortable with the permission requirements of an app, find a different one that meets your needs. In addition, periodically check the permissions to ensure they have not changed.

Backups

Always back up your data. For mobile devices, a great deal of your information is often backed up automatically, such as your photos or messages. However, backups also store your configurations, apps, and other device information, making it much easier to recover from a lost device or transition to a new one.

Work

When at work, be extra careful and never take any pictures or video that may accidently 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.

Resources

Passphrases:	https://www.sans.org/u/A3E
Backup/Recovery:	https://www.sans.org/u/A3z
Disposing of Your Mobile Device:	https://www.sans.org/u/A3u
Securely Using Mobile Apps:	https://www.sans.org/u/A3p
SANS Security Tip of the Day:	https://www.sans.org/tip_of_the_day.php

License

OUCH! is published by SANS Securing The Human and is distributed under the Creative Commons BY-NC-ND 4.0 license. You are free to share or distribute this newsletter as long as you do not sell or modify it. For past editions or translated versions, visit www.sans.org/security-awareness/ouch-newsletter. Editorial Board: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley