OUCH! | January 2016

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

- Securing Your Tablet
- Keeping It Secure

Securing Your New Tablet

Overview

Congratulations on your new tablet! This technology is a powerful and convenient way to communicate with others, shop online, watch movies, play games and perform a myriad of other activities. Since your tablet will most likely become an important part of your life, even perhaps replacing your computer, here are some key steps you should take to keep your tablet and your information safe and secure.

Guest Editor

Lori Rosenberg has extensive experience in developing Information Security educational materials and training for employees and customers, and is passionate about finding fresh and engaging methods to share that knowledge. You can find her on Twitter as **@InfoSecLori**.

Securing Your Tablet

It may surprise you to know that the biggest risk to your tablet is not hackers; it is most likely you. You are far more likely to lose, forget or have your tablet stolen than have someone hack into it. The number one thing you should do to protect your tablet is enable automatic locking of the screen. This means every time you want to use your tablet, you first have to unlock the screen with a strong passcode, swiping pattern or your fingerprint. This ensures that if your tablet is lost or stolen no one can access it, protecting all of your personal information, your mobile apps and anything else on there. Once you have automatic screen lock enabled, here are some additional tips to help protect your new tablet:

1. Install or enable software to remotely track your new tablet over the Internet. This way, if your tablet is lost or stolen, you can potentially connect to it over the Internet and find its location, or in a worst-case situation, remotely wipe all of your information on it.
2. Update your device and enable automatic updating so it is always running the latest version of the operating system. 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 the latest version of your mobile apps, you make it much harder for anyone to hack into your tablet.

Securing Your New Tablet

3. Pay attention when configuring your tablet for the first time, especially the privacy options. One of the biggest privacy issues with your tablet is the ability for others to track and know your location. We recommend you disable location tracking for everything, then re-enable location for only the apps you feel need it. For some apps, it is important to be able to track your location, such as mapping software or finding a local restaurant, but most of your apps do not need real-time location information.
4. Most tablets and apps store your information in the Cloud. As such, ensure you understand where your data is and how it is secured. For example, the last thing you want is for your private pictures to be shared on the Internet for the entire world to see, complete with geo-location information embedded in them. By default, disable any sharing of any information in the Cloud, then enable it only when you want to share something specific.
5. Tablets are increasingly synchronizing your apps with other devices, such as your smartphone or laptop. Synchronization can be a wonderful feature, but be careful of what apps or features you allow to synchronize. If you have synchronization enabled, don't be surprised to see the sites you visited and the tabs you created on your tablet's browser appear in your browser at work.

The best way to secure your tablet is to enable screen locking, review privacy settings and keep your tablet updated.

Keeping It Secure

Once you have your tablet secured, you want to be sure it stays that way. Here are some key steps to keeping your tablet secure long-term:

- Never jailbreak or hack into your own tablet. This will bypass and render a tremendous number of security controls useless and make your tablet far more vulnerable to attacks.

Securing Your New Tablet

- Only download apps you need and from trusted sources. For iPads, only download apps from iTunes. These apps are screened by Apple before they are made available. For Google, we recommend you download apps from just Google Play. For Amazon tablets, we recommend you stick with the Amazon App Store. While you can download apps from other sites, these are not vetted and could be infected. Finally, regardless of where you got your app, once you no longer need or actively use it, we recommend you delete it from your tablet.
- When installing a new app, make sure you review and set the privacy options, just like you did when initially configuring your new tablet. Be careful of what you allow each app to access. For example, does the app you just downloaded really need to have access to all of your friend and contact information? If you are uncomfortable with the permission requirements of an app, find a different one that meets your needs. In addition, regularly check the permissions to ensure they have not changed.

Your tablet is a powerful tool, one that we want you to enjoy and use. Just remembering these few simple steps can go a long way to keeping you and your new tablet secure.

Gartner Magic Quadrant: SANS Institute Is a Leader

SANS Institute has been named a Leader in the 2015 Gartner Magic Quadrant for Security Awareness Computer-Based Training Vendors. Download the complimentary report at: https://sans.org/u/bIY.

Resources

Securely Using Mobile Apps:	https://www.securingthehuman.org/ouch/2015#january2015
Passphrases:	https://www.securingthehuman.org/ouch/2015#april2015
Using the Cloud Securely:	https://www.securingthehuman.org/ouch/2014#september2014
Disposing of Your Mobile Device:	https://www.securingthehuman.org/ouch/2014#june2014
SANS Security Tip of the Day:	https://www.sans.org/tip_of_the_day.php

License