OUCH! | December 2013

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE..

- Securing Your Tablet
- Keeping Your Tablet Secure

Securing Your New Tablet

Your New Tablet

Congratulations on your new tablet. This technology is a powerful and convenient way to communicate with others, shop online, read, listen to music, game and perform a myriad of other activities. Since this new tool may become an important part of your daily life, we strongly encourage you to take some simple steps to help keep it safe and secure.

Guest Editor

Chad Tilbury is the guest editor of this issue. He has extensive experience investigating computer crimes and is the co-author of the FOR408 Windows Forensics and FOR508 Advanced Forensics and Incident Response classes at the SANS Institute. You can find him on Twitter as **@chadtilbury**, or on his blog, **http://forensicmethods.com**.

Securing Your Tablet

The first step is to set a passcode or some other screen locking mechanism. Tablets are easy to take wherever you go, which also means they are easy to lose or have stolen. To help prevent your information from falling into the wrong hands, be sure you lock your tablet screen with some type of hard-to-guess PIN, passcode or swiping motions. In newer devices, there may be some type of biometric authentication, such as a fingerprint reader. Use the strongest method your tablet supports, and be sure to set your tablet so that it locks automatically after a short idle time.

Next, update your tablet so it has the latest version of its operating system. Bad guys are constantly finding new weaknesses in software, and vendors are constantly releasing new updates and patches to fix them. By running the latest operating system, you make it harder for anyone to hack into your tablet.

Pay attention when configuring your tablet for the first time. The most important configuration choices will be your privacy and Cloud options. Privacy is about protecting your personal information. One of your tablet's biggest privacy issues is its ability to know and track your location. We recommend that you go into the privacy features and disable location tracking for everything, then enable it on an app-by-app basis. For some apps, it is important to be able to track your location (such as mapping software or finding a local restaurant near you), but the majority of apps do not need real-time location information.

Securing Your New Tablet

The other important option is Cloud storage. Cloud services such as Apple's iCloud, Microsoft's Skydrive, Dropbox or Google Drive allow you to store your data on servers through the Internet. Most tablets have built-in options for automatically storing just about anything in the Cloud, including documents, pictures and videos. Think about the sensitivity of your data and decide whether it is appropriate to store it in the Cloud. Make sure you understand how your data will be protected (such as by a password) and how you can control who will have access to it. The last thing you want is for the private pictures you just took to be posted on the Internet without your knowledge, complete with their geo-location information embedded.

The best way to secure your tablet is to use some type of screen or passcode lock, run the latest version of the operating system and be mindful of your privacy and Cloud options.

Be aware that tablets are increasingly synchronizing your apps with other devices, like your smartphone or laptop. This is common with many applications (including Google's Chrome), is pervasive in Windows 8 and is one of the most widely used features of iCloud. Device synchronization can be a wonderful feature, but if you have it enabled, don't be surprised to see the sites you visited or the tabs you created on your tablet's browser appear in your browser at work.

Keeping Your Tablet Secure

Once you have your tablet secured, you want to be sure it stays that way. Here are some simple steps for you to consider as you continue to use your tablet:

- Keep your tablet operating system and apps current and running their latest version. Many tablets now automatically update your apps, a feature we encourage you to enable.

- Do not jailbreak or hack into your own tablet. This will bypass and render a tremendous number of security controls useless, making your tablet far more vulnerable to attacks.

Securing Your New Tablet

- Only download apps you need, and only download them from trusted sources. For iPads, this is simple as only downloading apps from iTunes. These apps are screened by Apple before they are made available. For Google, we recommend you limit your apps to those found on Google Play. While you can download apps from other sites, they are usually not vetted and could be created with malicious intent. Finally, regardless of where you got your app, we recommend you remove it from your tablet once you no longer need or actively use it.

- 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 information you allow the app to access, or what you allow the app to do with that information. For example, does the app you just downloaded really need access to all of your contacts?

- Be sure to install or configure software that allows you to remotely track, lock or erase your tablet in case it is ever lost or stolen.

Become a Security Professional - Jan, 2014

Join us in the "Big Easy". SANS Security East 2014 will be held from January 20-25 in New Orleans. Start the year off right by choosing from outstanding, cutting-edge courses for cybersecurity and infosec professionals presented by our top-rated instructors. For more information, visit www.sans.org/event/security-east-2014/welcome.

Resources

Syncing Chrome:
http://www.techrepublic.com/blog/google-in-the-enterprise/chrome-sync-configure-once-work-everywhere/
Dangers of Cloud Computing:
http://www.businessnewsdaily.com/5215-dangers-cloud-computing.html
Common Security Terms:
http://www.securingthehuman.org/resources/security-terms
SANS Security Tip of the Day:
https://www.sans.org/tip_of_the_day.php

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis