December 2015
Volume 10, Issue 12

Getting Your Device and Checking It Twice

Center for Internet Security

Center for Internet Security
Monthly Security Tips Newsletter

From the Desk of Thomas F. Duffy, Chair, MS-ISAC

In last month's newsletter, we talked about how you can minimize your risk of identity theft and malicious cyber activity while doing your online holiday shopping. In this month's issue, we'll focus on another aspect of the holiday season: that new device you get or give during the holidays. Whether it's a smartphone, laptop, desktop, tablet, or another device, check out the below tips to help protect your new technology and secure your personal data.

1. **Configure your device with security in mind.** The "out-of-the-box" configurations of many devices and system components are default settings often geared more toward ease-of-use than security or protecting your information. Enable security settings on your device, and as you install software and apps, pay particular attention to those that control information sharing.

2. **Lock the device**. Locking your device with a strong PIN or password makes unauthorized access to your information more difficult. *Passwords are more secure than PINs.* If you have an Android device and want to use a lock screen pattern, make sure the pattern includes at least 7 points and doubles back over itself (e.g. at least 2 turns). If you use the fingerprint lock, remember that if your device is lost or stolen, you can't change or replace your fingerprints, like you can a password or PIN. So be careful with your device and make extra sure to protect your biometric information. Additionally, make sure that your device automatically locks after a period of inactivity – preferably between 30 seconds and two minutes. This way, if you misplace your device, you minimize the opportunity for someone to access your personal information.

3. **Regularly apply updates**. Manufacturers and application developers update their code to fix weaknesses and push out the updates and patches. Enable settings to automatically apply these patches to ensure that you're fixing the identified weaknesses in the applications, especially your operating system, web browser, and apps.

4. **Install antivirus software.** Install antivirus software if it is available for your device and enable automatic updating of the antivirus software to incorporate the most recently identified threats.

5. **Disable unwanted and unneeded services**. Capabilities such as Bluetooth, network connections and Near Field Communications provide ease and convenience in using your smartphone. They can also provide an easy way for a nearby, unauthorized user to gain access to your data. Turn these features off when they are not needed. Also consider disabling or uninstalling other features or apps that you no longer use.

6. **Be careful downloading apps.** Apps provide a lot of wonderful capabilities for your device, but they are also a common way that malicious actors disseminate malware or gather information about you. Always make sure you trust the app provider and download the app from the Google Play Store, Apple's App Store, or other trusted source, as they proactively remove known malicious apps to protect users. Be proactive and make sure that you read the privacy statement, review permissions, check the app reviews, and look online to see if any security company has identified the app as malicious.

7. **Set up a non-privileged account for general web use.** Privileged (such as Administrator or Root) accounts allow you to make changes in how your device operates, but a compromised administrator account provides attackers with the authority to access anything on your device. Use a non-privileged account when browsing websites and checking emails.

8. **Enable encryption**. Encryption makes it hard for attackers who have gained access to your device to obtain access to your information. Turn on encryption features.

9. **Maintain your device's security**. Remember that setting your device to be secure is great, but you have to keep those settings, as well. It may be tempting to do away with some of the security, such as a lock screen password, or allowing the settings to change when you get an app update, but that puts your device and information at risk.

By using caution and following these tips, you can help secure your new device and protect your information. Have a safe, secure, and joyous holiday season!

How to create a strong password:
http://msisac.cisecurity.org/whitepaper/documents/Security%20Primer%20-%20Securing%20Login%20Credentials.pdf

Advice for connecting a new computer to the Internet:
https://www.us-cert.gov/ncas/tips/ST15-003

Safe online shopping tips:
http://msisac.cisecurity.org/newsletters/2015-11.cfm

Provided By:

MS-ISAC MULTI-STATE Information Sharing & Analysis Center™

STOP | THINK CONNECT™