

Make Your List and Check It Twice: Tips for Securing Your New Computer or Device



Enterprise Information Security Office

Monthly Security Tips Newsletter

From the Desk of Deborah A. Snyder, Acting Chief Information Security Officer

In our November 2014 newsletter issue we talked about how you can minimize your risk of cyber crime while shopping online. In this month's issue, we'll focus on another aspect of the holiday season. Did you purchase or receive a new device or computer for the holidays? Do you know how to make sure it is as secure as possible?

Below are some helpful tips to keep in mind:

- **Configure Your Device**

The "out-of-the-box" configurations of many devices and system components are default settings often geared more toward ease-of-use and extra features rather than securing your device to protect your information. Enable security settings, paying particular attention to those that control information sharing.

- **Turn on Your Firewall**

Firewalls provide an essential function of protecting your computer or device from potentially malicious actors. Without a firewall, you might be exposing your personal information to any computer on the Internet.

- **Enable Encryption**

Encryption makes it hard for attackers who have gained access to your device to obtain access to your information.

- **Lock the Device**

Locking your device with a strong PIN/password makes unauthorized access to your information more difficult. Make sure your computer or device automatically locks after five minutes of inactivity. By doing this, if you misplace your device, you minimize the opportunity for someone to access your personal information.

- **Regularly Apply Updates**

Manufacturers and application developers update their code to fix weaknesses and push out the updates and patches. To ensure you're fixing the identified weaknesses in the applications, especially your operating system, web browser, and associated third party applications, enable settings to automatically apply these patches.

- **Install Antivirus Software**

To protect from known viruses, install antivirus software if it is available for your device. Enable automatic updating of the antivirus software to incorporate the most recently identified threats.

- **Be Careful When Downloading Applications**

When downloading a new application to your device, you are potentially providing that application with a lot of information about you, some of which you may not want to share. Be proactive: make sure you read the privacy statement, review permissions, check the application reviews, and look online to see if any security company has identified the application as malicious. A good way to prevent accidental downloading of malware is to use a trusted store instead of third party stores. Google Play Store and Apple's App Store proactively remove known malicious applications to protect users.

- **Disable Unwanted Services/Calling**

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.

- **Set Up a Non-Privileged Account for General Web Use**

Privileged accounts (such as Administrator or Root) allow users to make changes and access processes and functions that are not needed on a daily basis. A compromised administrative account provides attackers with the authority to access anything on your computer or possibly even on your network. Provide one more layer of defense by setting up a non-privileged account for use in browsing websites and checking emails.

By using caution and following the above tips, you can help secure your new computer or device and protect your information.

Look for the January newsletter which will focus on the cyber security trends and issues you need to know about in 2015.

Provided By:



CENTER FOR
INTERNET SECURITY



MULTI-STATE
Information Sharing
& Analysis Center™

The information provided in the Monthly Security Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.



STOP | THINK | CONNECT™