January 2015
Volume 8, Issue 1

**Make Your List and Check it Twice:**
**Follow these tips for securing your new computer or device**

# Washington County IT Department

In last month's newsletter, we talked about how you can minimize your risk of cyber crime while doing your online holiday shopping. In this month's issue, we'll focus on another aspect of the holiday season: you may be purchasing or receiving a new device or computer for the holidays, but do you know how to make sure it is as secure as possible?

Below are some tips for protecting your new technology, securing your personal data and spreading some cyber holiday cheer.

- **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 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. It's a powerful tool that you should consider implementing.

- **Lock the device**. Locking your device with a strong PIN/password makes unauthorized access to your information more difficult. Additionally, make sure that your device automatically locks after five minutes of inactivity. This way, 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. 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 associated third party apps.

- **Install antivirus software.** Install antivirus software if it is available for your device to protect from known viruses. Additionally, enable automatic updating of the antivirus software to incorporate the most recently identified threats.

- **Be careful downloading apps.** When downloading a new app to your device, you are potentially providing that app with a lot of information about you, some of which you may not want to share. 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. 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 apps 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 (such as Administrator or Root) accounts 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 your network. Setting up a non-privileged account for use in browsing websites and checking emails provides one more layer of defense.

By using caution and following these tips, you can help secure your new computer or device, and protect your information. Look for the February newsletter, which will focus on the cyber security trends and issues you need to know about in 2015.

**Provided By:**

CENTER FOR INTERNET SECURITY

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



STOP | THINK | CONNECT™