December 2016
Volume 11, Issue 12

New Device? Check Your CyberSecurity!

Town of Westwood Massachusetts

~~Monthly Security Tips Newsletter~~

~~*ert your agency name and contact info here*~~

MULTI-STATE Information Sharing & Analysis Center™

~~*Insert your logo here*~~

From the ~~Desk of Thomas F. Duffy, Chair, MS-ISAC~~Information Technology Department

Last month 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 tips below to help you protect your new technology and secure your personal data.

- **Configure your device with security in mind.** The "out-of-the-box" configurations of many devices and software 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.
- **Remember to secure your Internet of Things (IoT) devices.** Internet of Things devices include smart home thermostats, home surveillance cameras, smart refrigerators, lights, and many other examples. These need to be secured just like your phones, tablets, and laptops. One way to do this is to change the default password that comes pre-configured on the device to a strong password of your own choosing. This makes it much harder for cyber criminals to compromise your household devices.
- **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.
- **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 and should be at least 8 characters long combining upper and lower case letters, numbers, and symbols. If you have an

Formatted: Font: +Body (Cambria), Font color: Auto
Formatted: Normal
Formatted: Font: 16 pt, Bold, Font color: Text 1
Formatted: Left

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). Additionally, make sure that your device automatically locks after a brief 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.

- **Regularly apply updates**. Manufacturers and application developers update their code to fix weaknesses and push out the updates. Enable settings to automatically apply these updates to ensure that you're fixing the identified weaknesses in the applications.
- **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.
- **Disable unwanted and unneeded services**. Capabilities such as Bluetooth, network connections, mobile wallets, 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.
- **Be careful when downloading apps.** Apps provide a lot of wonderful capabilities for your device, but they are 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.
- **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.
- **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, as featured in our previous newsletter:
https://msisac.cisecurity.org/newsletters/2016-11.cfm

Provided By:

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.