Volume 14, Issue 12 • Dec. 2019

Monthly Security Tips Newsletter

From the desk of
Thomas F. Duffy

MS-ISAC Chair

10 Tips to Securely Configure Your New Devices

The holiday season is upon us, which means shopping for the latest gadget is in full swing. With the massive number of discounts that are available this year, it makes sense for you to buy that latest smart device, right? However, as impressive as the latest iPhone or gaming computer might be, ensuring you're able to properly secure these devices is more important than ever! Any device that connects to the internet is potentially vulnerable and could become compromised.

Here are several tips to keep in mind that can help you securely configure your new devices:

Secure Configuration Tips

1 Adjust Factory-Default Configurations on Hardware and Change Default Passwords

Passwords are a common form of authentication and are often the only barrier between cybercriminals and your personal information. Some internet-enabled devices are configured with default passwords to simplify setup. But did you know those passwords can easily be found online? To better secure your digital devices it's important to change the factory-set default password. Be sure to replace it with a strong and unique password or passphrase for each account.

2 Secure your Wi-Fi Network with Encryption

Your home's wireless router is the primary entrance for cybercriminals to access your connected devices. To enhance your defenses, use Wi-Fi Protected Access 3 (WPA3). WPA3 is currently the strongest form of encryption for Wi-Fi. Other methods are outdated and more vulnerable to exploitation.

3 Double Your Login Protection

Enable multi-factor authentication (MFA) to ensure that only the person who has access to your account is you. If MFA is an option, enable it by using a trusted mobile device such as your smartphone, an authenticator app, or a secure token. For instance, with an iPhone you can utilize your screen lock feature with a pin or password.

4 Disable Location Services and Remote Connectivity

Location services might allow anyone to see where you are at any given time. Consider disabling this feature when you are not using your device to further secure your private information. Additionally, most mobile devices are equipped with wireless technologies such as Bluetooth that can be used to connect to other devices or computers. Consider disabling these features when not in use as well!

5 Safeguard Against Eavesdropping

Disconnect digital assistants, such as your Amazon Alexa, when not in use. Limit conversation near baby monitors, audio recordable toys, and digital assistants. Be sure to cover cameras on toys, laptops, and monitoring devices when they are not in use.

6 Don’t Broadcast Your Wi-Fi Network Name

To prevent outsiders from easily accessing your network, avoid publicizing your Wi-Fi network name, or service set identifier (SSID). All Wi-Fi routers allow users to disable broadcasting their device’s SSID. Doing so will make it more difficult for attackers to find a network. At the very least, change your SSID to something unique. Leaving it as the manufacturer’s default could allow a potential attacker to identify the type of router and possibly exploit any known vulnerabilities.

7 Install a Network Firewall

Install a firewall at the boundary of your home network to defend against external threats. A firewall can block malicious traffic from entering your home network and alert you to potentially dangerous activity. Most wireless routers come with a configurable, built-in network firewall that includes features such as access controls, web-filtering, and denial-of-service (DoS) defense, that you can tailor to fit your networking environment. Keep in mind that some firewall features, including the firewall itself, may be turned off by default. Ensuring that your firewall is on and all the settings are properly configured will strengthen the security of your network.

Please Note: Your internet service provider (ISP) may be able to help you determine whether your firewall has the most appropriate settings for your particular equipment and environment.

8 Install Firewalls on Network Devices

In addition to a network firewall, consider installing a firewall on all computers connected to your network. Often referred to as host or software-based, these firewalls inspect and filter a computer’s inbound and outbound network traffic based on a predetermined policy or set of rules. Most modern Windows and Linux operating systems come with a built-in, customizable, and feature-rich firewall. Additionally, most vendors bundle their antivirus software with additional security features such as parental controls, email protection, and malicious website blocking.

9 Remove Unnecessary Services and Software & Install Antivirus Software

Disable all unnecessary services to reduce the attack surface of your network and devices, including your router. Unused or unwanted services and software can create security holes on a device’s system, which could lead to an increased attack surface of your network environment. Additionally, a reputable antivirus software application is an important protective measure against known malicious threats. It can automatically detect, quarantine, and remove various types of malware, such as viruses, worms, and ransomware. Many antivirus solutions are extremely easy to install and intuitive to use, allowing for automatic virus definition updates to ensure maximum protection against the latest threats.

10 Update and Patch Regularly

Manufacturers will issue updates as they discover vulnerabilities in their products. The perfect example being all of the update notifications you receive on your iPhone! Configuring your device to receive automatic updates makes this easier for many devices, such as computers, phones, tablets, and other smart devices. However, if you need to manually update your device, make sure you are only applying updates directly from the manufacturer (i.e. Apple), as third-party sites and applications are unreliable and can result in an infected device.

Additional Resources:
https://www.nsa.gov
https://niccs.us-cert.gov/

MS-ISAC
Multi-State Information
Sharing & Analysis Center

STOP | THINK
CONNECT™

The information provided in the MS-ISAC 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.