April 2018
Volume 13, Issue 4

Securing Devices by Making Simple Changes

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

I'm connected. You're connected. We're all connected!

We are more connected than ever before. According to ABI Research, there will be over 30 billion devices connected on the Internet by 2020. Today, our everyday devices are connected to the world including laptops, mobile phones, fitness trackers, smart televisions, home security systems, thermostats, and refrigerators. Additionally, let us not forget the devices that connect everything else together, such as routers, access points, and modems.

Many people may not consider their connected devices to be a security threat, but they absolutely can be. One of the issues with such devices is that many of them do not come configured with security in mind and connecting an unsecure device to your network is like leaving the back door to your house unlocked as it gives attackers access to your personal information. Manufacturers develop products to be more accessible, more user friendly, and to make our lives more integrated. However, that also means we are less secure if these devices are not probably configured. Unfortunately, some devices completely lack the option or ability to configure them, making it nearly impossible to secure them. Unsecure devices also give threat actors the means to propagate their attacks onto others by using your insecure devices to attack other networks and devices. Therefore, not only can your unsecure devices present a risk to you, but they can also become a risk to others who can be victims of an attack from your compromised devices.

Do Your Research

You should do your research before purchasing a connected device, especially a device that may allow someone access into your home, such as a surveillance camera or home security system. Check the online reviews and look at the company's website to determine if there are warnings about the security of the device and if the company issues updates/patches to fix security concerns.

What Can You Do to Secure Your Devices?

So, what can you do to enjoy the functionality of your connected devices and remain more secure at the same time?

When you first receive your device, check the default settings and choose the more secure options, such as enabling a password or changing the default password to something only you

know. Below is a list of these basic recommendations and some effective ones that may be less obvious choices.

- Network access or Internet access may be enabled on a device by default. Disable network/Internet access for devices that do not need it.
- Update the device operating system or firmware. The default operating software installed on a device may be out of date and/or contain many vulnerabilities. Updating or patching your device's software will reduce the chances of a successful attack.
- Wireless access points (APs) are oftentimes configured to broadcast the SSID, or network name, Consider changing these settings to turn this feature off, which can better secure your WiFi network.
- Create two different WiFi networks on your wireless router, if your router supports it. Creating separate WiFi networks, using different SSIDs, allows for the ability to separate smart devices from other networked computers, smart phones and tablets. The goal of the separation is to limit the impact a compromised smart home device will have on the rest of the devices on the network.
- Oftentimes, Wireless access points or routers are set up by default to not use encryption and to not require a password. It is always recommended to turn on WPA2 encryption for your wireless networks, and to establish a strong password with our next recommendation in mind.
- Change passwords on all network devices, especially from default "admin" accounts, and be sure to use strong passwords of at least 8 characters including uppercase and lowercase letters, special characters, and numbers.
- Many mobile devices have no PIN or unlock pattern (where you swipe your finger in a specific pattern on the screen) enabled when sold. Be sure to enable PINs or unlock patterns for all your mobile devices to secure them from unwanted entry by others.
- Automatic updates are often disabled by default. Be sure to turn on this setting to ensure your device receives important security updates when they are released.
- Many mobile devices support remotely wiping the device if the device is lost or stolen. Be sure to enable the remote wipe functionality in case the device is ever lost or stolen.
- Turn off location services if not needed.
- Cameras and audio input may be enabled by default on certain devices and applications, giving an attacker access to surveillance. Disable these features if not needed.
- Replace unsecure devices with more secure ones.

MS-ISAC
Multi-State Information Sharing & Analysis Center

STOP | THINK CONNECT™