December 2018
Volume 13, Issue 12

Security and Privacy in the Connected Home

Stay cyber-safe with your Internet of Things (IoT) devices!

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

Did you ever wonder what it would be like to have smart home? You could remotely change the temperature in your house, you could tell your lights to come on, or ask your refrigerator if you need to get milk at the grocery store, all from your smart home device or smartphone. You could play video games and access all your streaming services from one device, or know who is at your door from your connected doorbell.

The Internet of Things (IoT) is introducing these features into our homes by rapidly applying connectivity to everyday appliances and home features. As IoT devices become a part of our daily lives, and likely will become part of many more homes as holiday gifts, we need to take a look at the security risks and privacy concerns this smart technology introduces into our lives.

Personal Digital Assistants

Many people have a personal digital assistant like an Amazon Echo or Google Home. These devices analyze your past commands to try to anticipate your needs. These may also be linked to accounts used to purchase goods or services; make changes in your house such as turning off alarms, turning on the lights, or adjusting the temperature; or be linked to other accounts so they can tell you your schedule or read your email. Amazon Echo even has the ability to provide a pet-sitter with instructions, which is a give-away that you are not home.

Keeping these devices secure is especially important given that they may allow someone with access to the device to complete purchases using the owner's accounts, identify key information, or find out more about you.

Smart Thermostats and Other Smart Home Devices

Many homeowners are beginning to opt for a digital thermostat that allows them to control the temperature in their home remotely using an app. While digital thermostats do come at a premium, the vendor also makes money on data it collects on usage and habits. Smart light bulbs and smart doorbells also allow for great levels of data collection by the manufacturer.

IoT manufacturers entice consumers with convenience and functionality by promising the world of the future through devices like those listed above. All the while, cybercriminals are finding that they can use these devices as pathways into your home network to steal your data and find out more about you. And yes, that includes using digital information to determine if the house is unoccupied and safe to rob.

Gaming Consoles

Sony PlayStation 4, Microsoft Xbox One, Nintendo Switch, and many other gaming consoles are in millions of homes across the United States. These devices rely on Internet connectivity to provide different forms of entertainment and include streaming video, interactive gaming, voice chat features, and apps that keep both the system and applications up-to-date. One major risk is that many gaming consoles require subscriptions and user accounts for accessing online content such as games and streaming services. This makes the console another device associated with an account that holds your personal and payment information for the purposes of renewing these subscriptions.

Here are a few tips to follow in building your smart home with IoT devices:

1. If you don't need to connect a device to the Internet, don't. If a device isn't connected, it isn't as big of a cybersecurity risk.
2. Isolate IoT devices from other devices on your network by creating a separate Wi-Fi network just for them. This protects your other devices if your connected IoT devices are compromised.
3. Research the privacy, security, and accessibility options that are available for customizing your device. You may find some options that provide greater security and privacy if you opt in. One example is that a device may offer multi-factor authentication (MFA) where you use your traditional password and username combination with the added step of receiving a verification code or providing a fingerprint through a scanner. If MFA is available, it's worth using.
4. Always update your devices and apply patches when available. When selecting which IoT devices to purchase, ensure they offer patching and updates from the manufacturer to keep them up-to-date. Enable auto-updates on any IoT devices that support them.
5. Setup a separate unique, strong password for every device. Don't share credentials across devices.
6. Replace devices when they are no longer supported by the vendor, as security flaws will remain unpatched.
7. Turn off Universal Plug and Play if it is available on the device. You don't want the device having this ease of connectivity with so little control.
8. When requested to provide information to use a device, do not provide personally identifiable information (PII), like Social Security Numbers and dates of birth. If you must share PII to use the device, you may want to consider a different make or model or keeping it off your home network.

Remember these tips over the holidays as you receive and give gifts. This will ensure you don't give cybercriminals the holiday gift of your sensitive data!

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.