OUCH! | August 2018

OUCH!

SANS SECURITY AWARENESS

The Monthly Security Awareness Newsletter for Everyone

Smart Home Devices

What Are Smart Home Devices?

Traditionally, only a few of your devices at home could connect to the Internet, such as your laptop, smartphone, or gaming console. However, today there are more and more devices connecting to the Internet, from your lightbulbs and speakers to your TV, door locks, and even your car. Soon, almost every device in your house could be connected to the Internet. These connected devices are often called the Internet of Things (IoT) or smart home devices. While these connected devices bring a great deal of convenience, they also bring unique dangers.

What's the Problem?

The more devices that are connected to your home's network, the more that can go wrong. Hackers can program your devices to attack others, vendors can collect extensive information on your activities, or your devices could become infected and lock you out. Many of the companies making these devices have no experience with cyber security and see security as a cost. As a result, many of the devices you purchase have little or no security built into them. For example, some devices have default passwords that are well known or you cannot update or configure them.

How Can I Protect Myself?

So what can you do? We definitely want you to safely and securely leverage connected devices. These devices can provide wonderful features that make your life simpler. In addition, as the technology grows, you may have no choice but to use smart devices. Here are key steps you can take to protect yourself.

Connect Only What You Need: The simplest way to secure a device is to not connect it to the Internet. If you don't need your device to be online, don't connect it to your Wi-Fi network. Do you really need your toaster sending notifications to your phone?

Know What You Have Connected: What devices do you have connected to your home network? Not sure or can't remember? Turn off your wireless network and see what is no longer working. It may not catch everything, but you'll be surprised at how many devices you forgot.

Keep Updated: Just like your computer and mobile devices, it's critical to keep any and all of your devices up-to-date. If your device has the option to automatically update, enable that.

Passwords: Change the passwords on your devices to unique, strong passphrases only you know. You will most likely only have to enter them once. Can't remember all your passphrases? Don't worry, neither can we. Consider using a password manager to securely store them all.

Privacy Options: If your device allows you to configure privacy options, limit the amount of information it collects or shares. One option is to simply disable any information sharing capabilities.

Vendors: Buy your devices from a company that you know and trust. Look for products that support security, such as allowing you to enable automatic updating, change the default password, and modify privacy settings.

Always Listening: If a device can take your voice commands, it is constantly listening. For example, your Alexa and Google Home devices can record sensitive conversations. Consider that when you determine where to place the devices in your home and review the privacy options.

Guest Network. Consider putting your smart home devices on a separate "Guest" Wi-Fi network rather than the primary Wi-Fi network you use for your computers and mobile devices. This way, if any smart device is infected, your computers or mobile devices on your main network remain safe.

There is no reason to be afraid of new technologies, but do understand the risk they pose. By taking these few, simple steps you can help create a far more secure smart home.

Subscribe to OUCH! and receive the latest security tips in your email every month - www.sans.org/security-awareness/ouch-newsletter.

Guest Editor

Robert M. Lee *(@RobertMLee) is a SANS Certified Instructor and author of FOR578 - Cyber Threat Intelligence and ICS515 - ICS Active Defense and Incident Response. Robert is also the CEO and founder of the industrial cybersecurity firm Dragos.*

Resources

Passphrases:	https://www.sans.org/u/GEB
Password Managers:	https://www.sans.org/u/GEG
Securing Your Home Network:	https://www.sans.org/u/GEL