December 2019

LONGWOOD UNIVERSITY

INFORMATION SECURITY

Get Smart! Mitigating Risks in Connected Devices

Smart/IoT devices may be the panacea for consumer convenience. Do you want to know and change the temperature of your house or even your fridge remotely? There's an app for that. Such devices also raise extreme privacy concerns about the data collected about you. Devices can track or discern details about your life based on usage and interaction. And that data could potentially be aggregated with data coming from other smart devices, painting a fairly robust and accurate profile of you and your life. My fitness-tracking device serves as my wake-up alarm. Not only does it track the time that I set for the alarm, it also tracks my interaction when I shut it off. Maybe your coffee maker tracks when you start the brew (mine doesn't because I'm Coffee Old School). My car tracks what time I start it, how far I drive it, and the GPS location where I park it. These data points are provided to me as the consumer but are also presumably stored by the device provider. It's only 9:00 a.m. and my smart world already has collected or observed several key privacy factoids about me. And where data exist, risk to data exposure also exists.

Devices geared toward consumers will continue to push convenience over privacy, and consumers will continue to call for greater connectivity and convenience. That means more connected devices and ongoing evolution for more information, interaction, integration, and automation. It's no longer a question of whether your home devices should be connected. Instead, we need to proactively assess the risks of such connectivity. When those risks are greater than our threshold risk tolerance, we need to take steps to minimize those risks.

Continued on page 3...

Inside this issue

Special points of interest

- Additional access may require additional training in Securing the Human; be prepared to finish new modules as they're assigned.
- Keep your eyes out for changes to our security training next year!

Holiday Safety Tips

The holiday break is just around the corner, and many people will be traveling, shopping, and bustling to and fro with devices in tow. Here are some important do's and don'ts for the holiday season.

Things to Do

- Protect your device with a PIN: six characters is best. Use a different PIN when traveling abroad.
- Hover over hyperlinks and think before you click.
- Disable Auto-Connect and Bluetooth when traveling.
- Consider a privacy screen if using your laptop in public.
- Back up important files.
- Ensure anti-virus software is updated.

Continued on page 4...

The best way to avoid getting a computer virus is to avoid clicking on links or opening attachments in suspicious emails.

Viruses

A computer virus is designed to re-create itself and distribute copies to other files, programs, or computers. Here are some things you need to know about viruses:

- Each virus has an infection mechanism. Viruses can insert themselves into host programs or data files.
- Many viruses have a "trigger"—such as a user opening a file or clicking on an attachment—that causes the program to execute.
- There are two major types of viruses: compiled viruses (executed by an operating system) and interpreted viruses (executed by an application).
- Never use a USB drive or other removable media if you don't know its origin. It could be infected with a virus!
- The best way to avoid getting a computer virus is to avoid clicking on links or opening attachments in suspicious emails.

Mitigating Risks, Con't.

Take the following steps to protect yourself when you start using a new device:

- **When you bring home a new consumer device, check to see if it's transmitting.** Ask whether you need that device to be connected. What are the advantages of having your fridge broadcast the whereabouts of your cheese? Is the potential to activate remote maintenance with the device provider important to you? Do you want to interact with that device remotely? Then by all means, keep that connection. If you don't need the maintenance options or to monitor or interact with the device remotely, turn off the device's connectivity.
- **Periodically scan your networks to make sure you know and manage what's online.** If you want devices to be connected, be proactive. Find out how they connect; how devices are patched; what the default security settings are; and what data are collected and how/when/where the data are transmitted. Protect your home wireless network(s) with strong password management, active maintenance practices, and vigilance.
- **Use the same cybersecurity hygiene on your smart devices that you use on your computer.** While it may be revolutionary that your car is now essentially a computer on wheels, it's still just a computer. You don't have to become a cybersecurity expert, but you may want to find a few trusted sources of security advice for consumers.

It's time to get smart about your devices, manage them appropriately, and reap the rewards of their convenience.

Kim Milford is the Executive Director at the REN-ISAC.

Resources

- Learn more about securing IoT home devices with this SANS OUCH Newsletter.
- Review the Department of Homeland Security Internet of Things Tip Card.
- Download NCSA's infographic Your Privacy in a Growing Internet of Me.
- Learn about the types of data your connected car might collect.
- Become Cyber Savvy… Smart Tips in an IoT World.

Holiday Safety Tips, Continued

The Office of Information Security is responsible for developing and implementing campus-wide policies, controls and procedures to protect the university's information technology resources and systems from intentional or inadvertent modification, disclosure or destruction, as well as monitoring user adherence to these policies.

Things to Avoid

- Using a USB drive you find at the airport. It could be infected with malware!
- Plugging your device directly into a public USB port to charge it—use your device’s electrical plug instead.
- Posting your vacation pics online while traveling. If you publically announce that you are traveling, you leave yourself vulnerable to criminals who are looking for empty houses.
- Using public Wi-Fi for personal business, such as banking or making purchases. Cybercriminals can easily get your information over a public connection!
- Using ATM machines in heavily-trafficked tourist areas.

Longwood University

Information Technology Services
French Hall
201 High Street
Farmville, VA 23909
(434) 395-4357
(434) 395-2034

Fax: (434) 395-2035