OUCH! | May 2016

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

- What is the Internet of Things (IoT)
- Issues With IoT
- Protecting Your IoT Devices

Internet of Things (IoT)

What Is the Internet of Things (IoT)

In the past, technology was relatively simple; you just connected your computer to the Internet and used it for your daily activities. However, technology became more advanced when mobile devices came into our lives, devices such as smartphones and tablets. These devices put the power of desktop computers into our pockets. While far more mobile, these devices also brought their own, unique security challenges. The next big technical advancement is the Internet of Things. The Internet of Things, often shortened to IoT, is all about connecting everyday devices to the Internet, devices from doorbells and light bulbs to toy dolls and thermostats. These connected devices can make our lives much simpler; for example, having your lights automatically activate as your phone recognizes when you get close to home. The IoT market is moving at an amazing pace, with new devices appearing every week. However, like mobile devices, IoT devices also come with their own individual security issues. In this newsletter, we help you understand what those risks are and what you can do to secure your IoT devices, your home, and your family.

Guest Editor

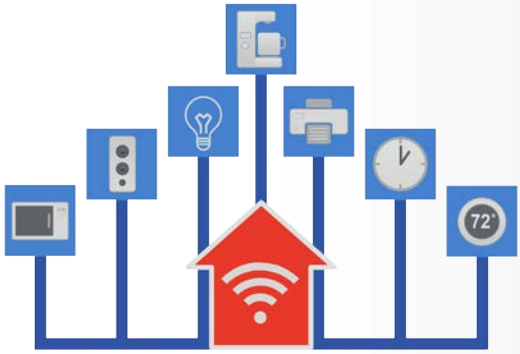
James Lyne (**@jameslyne**) is global head of security research at the security firm Sophos. A self-professed 'massive geek,' his technical expertise spans a variety of the security domains. He is a certified instructor at the SANS institute and often a headline presenter at industry conferences.

Issues With IoT

The power of IoT is that most of these devices are simple. For example, you simply plug your coffee machine in and it asks to connect to your home Wi-Fi network. However, all that simplicity comes at a cost. The biggest problem with IoT devices is that many of the companies making them have no experience with security. Instead, their expertise is manufacturing household appliances. Or perhaps they are a startup trying to develop a product the most efficient, fastest way possible, such as on Kickstarter. These organizations are focusing on profits, not cyber security. As a result, many IoT devices purchased today have little or no security built into them. For example, some have default passwords that are well known, perhaps even posted on the Internet, and cannot be changed.

Internet of Things (IoT)

In addition, many of these devices have no option or ability to configure them; you're stuck with whatever was shipped. To make matters worse, many of these devices can be difficult to update or may not even have the capability. As a result, many of the IoT devices you are using can quickly become out of date with known vulnerabilities that cannot be fixed, leaving you permanently vulnerable.



Know what IoT devices you have connected to your network, isolate them when possible, keep them updated, and protect them with strong passphrases.

Protecting Your IoT Devices

So what can you do? We definitely want you to leverage the power of IoT devices securely and effectively. These devices can provide wonderful features that can make your life simpler, help save money, and increase the physical security of your home. In addition, as the technology grows, you may have no choice but to purchase or use IoT devices. Here are some steps you can take to protect your IoT devices and yourself:

- Connect Only What You Need: The simplest way to secure an IoT 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.
- Separate Wi-Fi network: If you do need your IoT devices online, consider creating a separate Wi-Fi network just for them. Many Wi-Fi access points have the ability to create additional networks, such as a Guest network. Another option is to purchase an additional Wi-Fi access point just for IoT devices. This keeps your IoT devices on an isolated network, where they cannot be used to harm or attack any computer or mobile devices connected to your primary home network (which is still the main interest of cyber criminals).
- Update When Possible: Just like your PC and mobile devices, keep your IoT devices up to date. If your IoT device has the option to automatically update, enable that.
- Strong Passwords: Change any passwords on your IoT device to a unique, strong passphrase only you know. Can't remember all of your passphrases? Don't worry, neither can we. Consider using a password manager to securely store all of them.

Internet of Things (IoT)

- Privacy Options: If your IoT device allows you to configure privacy options, limit the amount of information it shares. One option is to simply disable any information sharing capabilities.
- Consider Replacement: At some point, you may want to replace an IoT device when your existing one has too many known vulnerabilities that cannot be fixed or there are newer devices that have far more security built into them.

There is no one size fits all for every device, so it is worth checking for best practices and any publications on how to secure them. Unfortunately, most IoT devices were not developed with cyber security in mind, so many manufacturers do not provide much security information. But as awareness for cyber security grows, we hope to see more and more IoT vendors build security into their devices and provide more information on how to protect and update them.

Meeting NERC CIP Training Requirements

SANS has developed training for electric utility organizations subject to the NERC CIP Reliability Standards. Learn how SANS can help you meet the training requirements in NERC CIP-004 and CIP-003.

http://securingthehuman.sans.org/u/gY8

Resources

Passphrases:	https://securingthehuman.sans.org/ouch/2015#april2015
Password Managers:	https://securingthehuman.sans.org/ouch/2015#october2015
Securing Your New Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016
Securing Your Home Network:	https://securingthehuman.sans.org/ouch/2016#february2016

License