Information Security Newsletter

August 2017

Connected Home Devices: The Internet of Things (IoT)

From the Desk of Milind Samant, ISO

What is the Internet of Things (IoT)?

We have become more connected than ever before. A little over ten years ago, we only accessed the Internet through a laptop or a desktop computer. Then, we added phones and tablets to our list of connected devices. Today, we have even smaller connected devices, such as fitness trackers and smart watches. According to ABI Research, there will be over 30 billion devices connected to the Internet by 2020. The list of Internet connected devices, or "things", keeps growing. Kevin Ashton, cofounder and executive director of the Auto-ID Center at the Massachusetts Institute of Technology (MIT), first mentioned the term Internet of Things (IoT) in 1999, but the first device to be connected to the Internet was actually a Coke machine at Carnegie Mellon University in the early 1980s. Programmers could connect to the machine over the Internet, check the status of the machine, and determine whether there would be a cold drink waiting for them. Today, IoT consists of everyday devices that are connected to the Internet, such as fitness trackers, vehicles, smart televisions, doorbells, light bulbs, home security systems, thermostats, and refrigerators. Basically, if it is not a computer, smartphone or tablet, *and* it connects to the Internet, it can be called an IoT device.

What are the issues with IoT devices?

Many people know they should install anti-virus (AV) software on their computers and be careful of what websites they visit or software they download. Unfortunately, most people probably do not consider their IoT devices to be a security threat. These devices are more accessible and make our lives more integrated, but many of the companies behind these new devices are not designing them with security in mind. For example, many IoT devices have default passwords that are well known and cannot be changed easily. They also can be difficult or impossible to update to mitigate known vulnerabilities, or have no settings to customize security.

How can we secure our IoT device?

So, what can we do to enjoy the functionality of IoT devices and remain more secure at the same time? The following tips may help you in these endeavors:

- Know what IoT devices are connected to the network. It is possible that there are devices connected to your network that you do not know about.

- Isolate IoT devices from other devices on the network by creating a separate Wi-Fi network just for them. This protects your other devices if your connected IoT devices are compromised.
- Update the device's software, if possible. If you update your device regularly, this will reduce the chances of a successful attack.
- Replace default passwords with unique and strong ones of your choosing. Passwords should have upper and lower case characters, numbers, and special characters, with at least 8 total characters.
- Configure security and privacy options, such as enabling encryption and limiting the information your devices share.

Resources:

https://www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne/

http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

Wishing you all a very
Busy & Happy Fall 2017 Semester!

Reminders….

- ***Set a strong password:*** *Use at least 8 characters in upper and lower case, numbers, and symbols.*
- ***K*eep your device locked**: Use a password, pin, pattern, or fingerprint lock when you are not actively using it.
- ***When in doubt, contact the Service Desk at*** servicedesk@oldwestbury.edu ***or call X3098.***

Provided By:

Information Technology Services **Division of Business & Finance** **Evan Kobolakis, CIO** **Len Davis, Sr. Vice President & CFO**	**MS-ISAC** Multi-State Information Sharing & Analysis Center	SUNY OLD WESTBURY OWN YOUR FUTURE

The information provided in the Monthly Information Security Newsletter is intended to increase the data security awareness of SUNY Old Westbury end users and to help them behave in a more secure manner within SUNY Old Westbury work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the SUNY Old Westbury's overall cyber security posture.

Disclaimer: These links are provided because they have information that may be useful. The SUNY Old Westbury ITS Department 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.