

Information Security Newsletter

December 2018



Stay Cyber-Safe With Your
Internet of Things (IoT) Devices!

From the Desk of Milind Samant, ISO

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. 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 digital 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.

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. Isolate IoT devices from other devices on your home network by creating a separate Wi-Fi network just for them. This protects your other devices if your connected IoT devices are compromised.
2. 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.
3. Always update your devices and apply patches when available. Enable auto-updates on any IoT devices that support them.
4. 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!

Reminders....

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

Provided By:

<p>Information Technology Services Division of Business & Finance Evan Kobolakis, CIO Len Davis, Sr. Vice President & CFO</p>	 <p>NATIONAL CYBER SECURITY ALLIANCE</p>	 <p>SUNY OLD WESTBURY OWN YOUR FUTURE</p>
---	---	--

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.