CYBERSECURITY AWARENESS MONTH

Everywhere you look you see some mention of "IOT". IOT refers to the "Internet of Things". Examples of common IOT devices (beside laptops, tablets, smart phones and smart watches) are: Echo Plus, Google Home Controller, Doorbell Cams, Smart Home Locks, Smoke Alarms, Thermostats, Universal Remotes, air quality monitors, etc.

Smart Devices Need Smart Security

IoT devices started to become more and more popular beginning around 2015 and ever since the technology has been a controversial subject. Both the FBI and the CIA have released statements telling the publish that these devices are as dangerous as they are useful. When you think about these dangers, the first thing that comes to mind is cybercrime.

Cybercriminals are more than able to place malware on your devices, which can lead to stealing your personal information and a lot worse than that. Below are three best practices when it comes to securing your IoT devices.

Passwords. You hear this day in and day out, but it can't be stressed enough how important this step is, given the fact that people have the tendency to forget about it. Do not use default passwords. This is STEP ONE of setting up any IoT device.

Secured connections. If you want to get the most out of your IoT devices, investigate using a virtual private network (VPN). This is one of the most effective way to securely connect your device to the Internet.

Updates. No manufacturer ever will assure you that the device that they're selling is one hundred percent secure. That's why they always work on improving their products and regularly release updates. And it's your job to make sure that you install those updates as soon as you can.

Research. Look into security for the device before you buy. This is a part of that decision of how to mitigate risk in balancing what you gain from the device vs the risks of the device.

Fast Facts on Cybersecurity

The number of cellular Internet of Things (IoT) connections is expected to reach **3.5 billion** in 2023 – increasing with an annual growth rate of 30%. (Ericsson)

63% of people find connected devices 'creepy' in the way they collect data about people and their behaviors. (Consumers International & Internet Society)

Within 5 minutes, connected devices are attacked and are targeted by specific exploits in 24 hours. (NETSCOUT).

IoT Security: The Good, The Bad, and the Ugly

By the end of last year, there were more than 26 billion IOT devices in the world. Smart speakers, without a doubt dominated the market, with manufacturers racing each other to bring even more innovation into this lucrative business.

The good news is that the creation of these devices brings us new functionality, time savings and amazing opportunities.

Illinois Department of Innovation & Technology

Need to report a security issue?

The Department of Innovation & Technology (DoIT) is committed to protecting our customers. If you have found a vulnerability or security issue, we ask that you submit a detailed description of the issue to us at: DoIT.Security@illinois.gov.