Make sure your Gifts are Secure

What is the Internet of Things?

Internet of Things (IoT), refers to the connection of devices (other than computers and smartphones) to the Internet. Those who have been gifted, or gifted themselves with an IoT device, and started to use it in their everyday life hopefully have taken precautions to protect it from being hacked. Hackers have hijacked baby monitors and spied on people using webcams, for example.

Today more and more IoT devices are connecting to the Internet:

- Lightbulbs
- Locks on your door
- Tablets
- Wearable fit devices
- Kitchen appliances
- Baby monitors
- Security cameras
- Smart thermostats
- Televisions that connect to the Internet
- Cars

All of these IoT devices are susceptible to hacking in the same way that mobile devices and laptops are, so they must be included as part of the overall security routine at home. This is important because many IoT devices ship with little or no security measures. This opens them up to being targets for hackers who can break into the home network through a connected device.

How can you Protect Yourself?

Connect only what you need:

The simplest way to secure a 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. Do you really need your toaster sending you notifications to your phone?

Know What You Have Connected:

What devices do you have connected to your home network? Not sure or can’t remember? Turn off your wireless network and see what is no longer working.

Keep Updated:

Just like your computer and mobile devices, it’s critical to keep any and all of your devices up to date. If your device has the option to automatically update, enable that.

Privacy Options:

If your device allows you to configure privacy options, limit the amount of information it collects or shares. One option is to simply disable any information sharing capabilities

Always Listening:

If a device can take your voice commands it is constantly listening. For example, your Alexa and Google Home devices can record sensitive conversations. Consider that when you determine where to place the devices in your home and review the privacy options.

Guest Network:

Consider putting your Smart Home devices on a separate “Guest” WiFi network rather than the primary WiFi network you use for your computers and mobile devices. This way if any Smart Device is infected, your computers or mobile devices on your main network remain safe.

Change the default password:

Most people don't even know that many IoT devices have default passwords that should be changed to a strong password prior to use. A strong password should be as long as possible, unique yet easy to remember, never shared with anyone, and changed regularly. Never use the default security settings, always use the highest settings possible, and include complex passwords that contain alphanumeric and non-alphanumeric characters. Change the default password on your router!

Disable remote or universal plug and play:

Most internet-connected IoT devices come out of the box ready for action (and immediately connect to them). Read the information and instructions that came with the device to find out if it is plug and play and if so, turn it off. As a best practice only connect to secure networks.

To learn more about holiday scams, please visit our website.