

Staying Safe with Connected Devices and the Internet of Things

Author : Cat

Date : December 14, 2015

If I had asked you to connect to the 'internet' a few years ago, you would have opened a browser window on your computer or handheld device. Today we can connect to the internet using any number of devices from wearables (e.g. FitBits) to thermostats to kitchen refrigerators. Collectively all these devices and connections are known as the Internet of Things, or IoT. By 2020, it is predicted that we will have 50 billion IoT devices - which includes 90% of our cars.

How many connected items do you have in your home? Typical homes have phones, computers, tablets and likely TVs. Additionally there are gaming systems, health monitors, kitchen appliances, door locks, security systems, lighting, temperature controls and smoke detectors. The up side is the ability to control all of these items remotely or automatically. The down side is that all the usage information is being recorded and stored for analysis. The fact that your coffee maker turns on at 6:35 am or that you have a high score on a video game may not be deemed 'private' but what about your photos, your health information or where you drive every day?

Though most of the devices are quite safe and use your personal data to improve your experience, there are some vulnerabilities for which you should be aware. Here are 4 areas of IoT that you need to know about:

Kids on Devices

In November 2015, [VTech](#), a popular toy company was hacked, revealing the accounts of nearly 5 million parents as well as the information on their kids. Also in 2015, Hello Barbie was released. A talking Barbie doll that includes a microphone that records kids questions and then processes the answers on a server in the cloud. That means a child's private information is being sent to a foreign computer. Just because a toy or game is targeted at children does not mean that information is any more protected than any other system.

Tip: *If your children are using anything that connects to your WiFi then make sure the information being sent back and forth is not private. Include as little personal data (birthdays, names) as possible.*

Health Monitors and Wearables

Wearables that monitor the number of steps you take or your heart rate have become incredibly popular. These devices provide motivation through data, but be aware that the companies that control these devices also maintain your data. What happens in 10 years when you apply for health insurance and it is revealed, via your wearable data, that you did not exercise much in 2018 or didn't get enough sleep. Could you be denied insurance? Maybe.

Tip: *Use wearable tech to help you get going but limit the use for 24 hour monitoring that could lead to an intimate portrait of your health that you may not want to share.*

Your Routines

When you have a smart house and a smart car, it can do everything for you; Start your breakfast, plan your day's driving route, turn down the temperature of your house while you are out or video your pets. All this automation makes you predictable and outlines the minutia of your day. My grocery store knows what days I shop and Netflix knows when I watch TV. What would happen if someone had all the data on your daily activities? Could you tell when you are away? On the positive, you can also use the same systems to make people think you are home when you are not.

Tip: *Keep visible automated home systems, like lighting, the same each day. Most modern systems lights go on with the onset dusk, not by hour. Limit all day GPS tracking systems when possible.*

Connected Systems

When you connect multiple items to the same WiFi, you lose the protection of a secure WiFi network. There are cases where hackers have hacked one connected item and then gained access to other connected items in the same house. Over time, there will be ways to protect against this but right now you need to protect yourself.

Tip: *Your connected devices within your home are only as safe as your weakest link. Make sure the items you add to your WiFi are trusted sources.*

Enjoy your connected devices and the amazing benefits they provide. Also be aware of the information they are using. Have fun, stay safe.