VA
U.S. Department of Veterans Affairs
Office of Information and Technology

CSAM
Cybersecurity Awareness Month
Do your part. #BeCyberSmart.

The Internet of Things: Smart Devices Need Smart Security

Published Sept 28, 2020

Author: Kelly Wright, Office of Information Security; Robin Froelich, Data Loss Prevention

The Internet of Things or IoT are systems or networks of interconnected "smart devices" that are considered non-traditional because they don't fit in the category of computers, tablets, or mobile phones. Many types of physical objects such as IP cameras used for security, Internet-connected televisions, smart refrigerators, smart crockpots, smart door locks, and smart cars are all IoT devices. Because these items are connected to the Internet, like computers and other mobile devices, they can be hacked. While hackers might not want to hack your refrigerator or crockpot, they may hack into your car. Just imagine what would happen if someone took control of your car as you were driving down the road!

Smart devices make your life easier by allowing a few clicks to unlock your door, change the movie you are watching or look in the refrigerator while at the store. But how does all this work? Smart devices collect information to perform the functions you use such as the suggesting websites to visit and entering your passwords. Your smart phone and home network stores all that information, which makes your life easier by allowing you to skip some steps that are commonly repeated. The main point here is that the more you are connected to various apps and devices, the more ways your information can be shared or stolen. Unfortunately, profit can be made using that information from ads that popup on your smartphone to identity theft.

Here is a question for you, how often have you clicked the "I agree" link without reading the user agreement? By clicking that link, you may be sharing your information or allowing unneeded access to other apps or devices.

So how can you keep your information safe? Here's a great checklist that can help you keep your smart devices safe and secure:

- □ Install Internet security software on your computers, tablets, and smartphones
- □ Use multifactor authentication to secure your devices. If multifactor authentication is not available, be sure to use strong, unique passwords on all device accounts, Wi-Fi networks, and connected devices
- □ Change your passwords frequently
- □ Always read the user agreements that come with the apps and devices you use
- □ Do research before you buy; check to see if there are known security/privacy issues
- □ Know the data your apps and devices are storing; is it necessary?
- □ Only enable functions that are necessary; does the app or device need to connect to the Internet?
- □ Does the app or device need to access other apps or devices?
- □ Check the apps or devices website for updates frequently
- □ Never leave your smartphone unattended

Remember, when you use Smart Devices you need Smart Security. #BeCyberSmart