Computer Crime Investigative Unit
U.S. Army Criminal Investigation Command

Cybercrime Prevention Flyer

Contact Information:
Cyber Criminal Intelligence Program
27130 Telegraph Road
Quantico, Virginia 22134

Phone: 571.305.4482 [DSN 240]
Fax: 571.305.4189 [DSN 240]

Email

CCIU Web Page

CID LOOKOUT
ON POINT FOR THE ARMY

DISTRIBUTION:
This document is authorized for the widest release without restriction.

"DO WHAT HAS TO BE DONE"

CPF 0009-18-CID361-9H **26 November 2018**

The Internet of Things Watered My Garden

It's great! But maybe not always.

The Internet of Things is an interconnected collection of automated devices (*things*) that gather, organize, analyze, and synthesize data in order to intelligently interact and improve your quality of life. A *thing* could be a home thermostat that monitors weather forecasts and adjusts your home's temperature so you are comfy when you arrive. A *thing* could monitor zones in your garden and water each zone according to local environmental conditions and the unique needs of particular plants.

By one estimate, there will be 12 billion *things* on the internet by 2020; many households will have hundreds of *things* on their local network alone. Keeping all those *things* updated and patched might become so onerous that few people will do so.

> The entrenchment of the Internet of Things (IoT) into every facet of our existence has established itself as both a superb innovation and a security minefield. The sheer number of connected devices in any one system presents numerous points of entry for nefarious purposes.
>
> Gary Eastwood
> Network World
> June 27, 20117

As it is now, updating the router, two desktop computers, three laptops, two gaming consoles, and five smart phones currently on your home network, each with its unique and complex password, is already difficult enough. Now imagine the challenge of updating and maintaining a network of hundreds of *things*. Then, consider that you might have more *things* – four or five times more *things.*

Although another device added to your network will not increase your vulnerability all that much, adding three smart televisions, six security cameras, four smart deadbolt locks, two video doorbells, twenty two remotely controllable mood lights, twelve Bluetooth speakers…(you get the idea) probably will.

Certainly, some of the *things* will make your life easier and the added convenience might make the extra effort worthy of your time. But never lose sight of the fact that the *things* on the Internet of Things are computers.

They might be big or small, complex or simple, expensive or cheap but they are still computers. They communicate across the internet with other *things* and there are lots of *things*. And, similar to your desktops and laptops, those *things* can be compromised by nefarious people and used to do bad things. Each device on your network is an entry point of vulnerability – a point from which a cybercriminal can compromise your network and access personal information.

Like your smart watch – the one that records your heart rate, breathing and other life functions, tells you when it is time to sleep, knows when you are asleep, and in which room you are sleeping so your smart thermostat can tell your smart HVAC system to adjust the temperature in that room to your personal preference, giving you that better night's sleep you have always wanted.

You might not care that a cybercriminal knows your smart refrigerator is out of mayonnaise or you half-and-half is expired. But you probably do care that a cybercriminal could monitor your heart rate, know what room you are in and know when you are asleep. You probably do care that a cybercriminal could compromise your smart deadbolt locks and unlock your front door.

Presumably, you are already in the habit of safe computing – using antivirus protection, updating operating systems and software, and protecting every computer device you own with complex and unique passwords. If you are not, you should be.

Many of the ideas for securing your Internet of Things devices are quite standard: password protect your devices, change default passwords, do not use the same password for all of your devices, use a reputable anti-virus product and set it to scan on a schedule, activate encryption on your router, and many others. You have undoubtedly seen and heard of most of these before. But, there are some specific ideas for the *things.*

Securing Your *Things* on the Internet of Things

- Make certain the device you are about to buy can be updated. Avoid those that cannot be updated – and there are some.
- Try to pick *things* that are easy to update. You are less likely to update your rooftop weather station if you have to carry your laptop up there with you.
- Do your research and buy products from manufacturers that are likely to persist. If the *thing* you buy today becomes abandonware tomorrow – updates may never be available.
- Update your *things* when you install them. The *thing* you purchase today was probably mass-produced months ago. Right out of the box, the operating system is likely out-of-date.
- Turn off your *things* when you're not using them.
- If your smart device does not need to be connected, do not connect it. Your smart HVAC thermostat works fine even if you cannot control it from a different hemisphere.

IoT in the News

Common Internet of Things Expose Consumers to Exploitation – Internet Crime Complaint Center

Cyber Actors Use IoT to Pursue Malicious Activities – Internet Crime Complaint Center

Securing Your Internet of Things Devices – Cybersecurity Unit, USDOJ

Five Reasons Device Makers Can't Secure IoT – Network World

IoT Devices Will Outnumber the World's Population in 2017 – ZDNet

Your Smart Lock Can Probably be Hacked – CNet

Criminals Hacked a Fish Tank to Steal Casino Customer Data – Forbes

ICE

CCIU uses the Interactive Customer Evaluation (ICE) system. Please click on the ICE logo and take a moment to provide feedback.

Disclaimer: The appearance of hyperlinks in this Cybercrime Prevention Flyer (CPF), along with the views and opinions of authors, products or services contained therein do not constitute endorsement by CID. These sites are used solely for authorized activities and information that support the organization's mission. CID does not exercise any editorial control over the information you may find at these link locations.