INTERNET OF THINGS: IS OUR "SMART" WORLD SECURE?

The "Internet of Things" is the term that describes all of the appliances and devices that connect to the internet and to each other on your home network. This new technology is embraced for its convenience and ease by individuals and families. Even children know how to use the home's digital assistant to listen to a favorite song. On a broader scale, communities tap into the Internet of Things to track parking meter violations and snow plows. But each device connected to your network offers a new point of entry to attackers if the devices aren't adequately secured. Learn steps you may take to mitigate the risks while enjoying the benefits of smart devices.

HOW IT WORKS

How many devices do you have connected to the internet? Estimates put the number of devices that compose the Internet of Things in the billions and growing. These devices have embedded chips, sensors, software and network connectivity to support the collection of data, the exchange of data and the analysis of data, often for the purpose of solving a problem: the house is too hot or too cold, the front door needs to be locked after you've already left for the office, a pacemaker sends vital data to a healthcare provider to ensure a patient's well-being.

Unfortunately, cybercriminals are always on the prowl to exploit any vulnerabilities and to take advantage of consumers. Data being collected and shared by your devices creates a honey pot of information for identity thieves and other cybercriminals, potentially including bank account information.

Security is part of the product development process, but technology changes. Manufacturers are challenged to be nimble and diligent in keeping products aligned with those changes before going to market or after through upgrades.

WHO IS IMPACTED

Anyone with a device that is connected to the internet is potentially at risk. No connected device is too small to be compromised. According to news reports, hackers attempted to collect data from an undisclosed casino in North America, tapping into the casino network via fish tank sensors. The sensors were connected to a casino computer to regulate the temperature and cleanliness of the tank.[1]

No device is off limits to cybercriminals, including children's toys that are connected to the internet. In 2019, a little girl was frightened when a hacker spoke through the baby monitor in her bedroom, claiming to be Santa Claus.[2]

WHAT ACTIONS CAN YOU TAKE?

When it comes to connected devices, proceed with caution using basic cybersecurity good hygiene, including the tips below:

Research the product and the manufacturer prior to purchase to understand how the brand prioritizes security. One indication is a history of the manufacturer offering security patches or software updates.

Change the default settings (username, passwords) that come with your device. If you cannot change the default setting, consider purchasing a different brand that permits you to do so.

Keep track of all the devices connected to your network and the type of data being collected.

Use a separate network for your smart devices. If cybercriminals should find a way in to your connected devices, they can't access the information on your personal computer, such as bank account information, if it's on a different network.

Use strong passwords. Set up each device with a unique password and opt for one-time passcodes and/or biometrics when available.

Install security patches and software updates from manufacturers' websites in a timely manner.

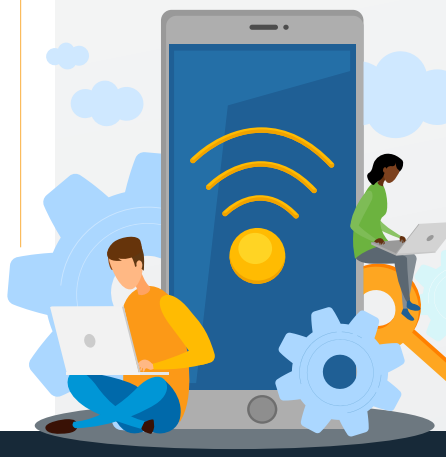
Protect your cellphone or tablet. It is important not to lose these items when they are loaded with apps that control your devices.

Do not use public Wi-Fi when remotely activating or checking your device.

Disable features that you are not using. Features such as remote access and voice control can be enabled if/when the need arises.

Disconnect any device from your network when not in use.

Each device connected to your network offers a new point of entry to attackers if the devices aren't adequately secured.



1 Schiffer, Alex. "How a fish tank helped hack a casino." *Washington Post*, Nash Holdings. 7/21/17. https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/ Accessed 8/4/20.

2 Vigdor, Neil. "Somebody's Watching: Hackers Breach Ring Home Security Cameras." *New York Times*. 12/15/19. https://www.nytimes.com/2019/12/15/us/Hacked-ring-home-security-cameras.html. Accessed 8/4/20

CON PDF 0720 0161

PNC BANK