THE ARIZONA REPUBLIC
azcentral.com

Internet of Things increases risk of cyberthreats, FBI says

http://www.azcentral.com/story/money/business/tech/2015/09/24/internet-things-increases-risk-cyberthreats-fbi-says/72744454/

Mark Pribish, Special for The Republic | azcentral.com | September 24, 2015

Businesses and consumers using Web-connected devices to the Internet of Things increase their risk of cyberthreats, according to the FBI.(Photo: Getty Images/iStockphoto)

It's fascinating that we can now adjust our thermostat in Arizona from Europe, monitor Grandma so we know instantly if she needs help or even track our vitals and insulin levels during a 5K run with the help of a cellphone, software and the Web. These are examples of the Internet of Things, and as you'll see, examples of added ID-theft dangers.

Businesses and consumers using Web-connected devices to the Internet of Things increase their risk of cyberthreats, according to the FBI.

"The rapid development and adoption of new Web-connected smart devices is drastically increasing the cyberthreat landscape that businesses and consumers must now face each day," according to John Iannarelli, the recently retired assistant special agent in charge of the FBI's Phoenix division.

IoT devices "present unique security risks to consumers," Iannarelli said. "For example, if a hacker gains access to your smart refrigerator, it could serve as a conduit to any other device connected to your home network, such as your home security system or personal computer."

Devices with default passwords or open Wi-Fi connections are an easy target for cybercriminals pretending to be you and ready to exploit your name for their gain.

The FBI lists IoT devices that could be compromised. They include:

- Automated devices that remotely or automatically adjust lighting or HVAC.
- Security systems, such as security alarms or Wi-Fi cameras, including video monitors used in nursery and day-care settings.
- Medical devices, such as wireless heart monitors or insulin dispensers.
- Thermostats.
- Wearables, such as fitness devices.
- Lighting modules that activate or deactivate lights.
- Smart appliances, such as smart refrigerators and TVs.
- Office equipment, such as printers.
- Entertainment devices to control music or television from a mobile device.
- Fuel monitoring systems.

Now, here are ways, per the FBI, to reduce your chance of being a victim or reduce the impact of an IoT breach.

- Isolate IoT devices on their own protected networks.
- Disable UPnP on routers.
- Consider whether IoT devices are ideal for their intended purpose.
- Purchase IoT devices from manufacturers with a track record of providing secure devices.
- When available, update IoT devices with security patches.
- If a device comes with a default password or an open Wi-Fi connection, consumers should change the password and only allow it operate on a home network with a secured Wi-Fi router.
- Use current best practices when connecting IoT devices to wireless networks and when connecting remotely to an IoT device.
- Patients should be informed about the capabilities of any medical devices prescribed for at-home use. If the device is capable of remote operation or transmission of data, it could be a target for a malicious actor.
- Ensure all default passwords are changed to strong passwords. Do not use the default password determined by the device manufacturer.

“While the IoT offers convenience and efficiency, the IoT will always be targeted by ID-theft criminals and hackers,” Iannarelli said.

Mark's Most Important: The Internet of Things can enhance life but is also a giant opportunity for ID criminals. Follow the FBI’s guidance to protect yourself.

Mark Pribish is vice president and ID-theft practice leader at Merchants Information Solutions Inc., an ID theft-background screening company based in Phoenix. Contact him at markpribish@merchantsinfo.com.