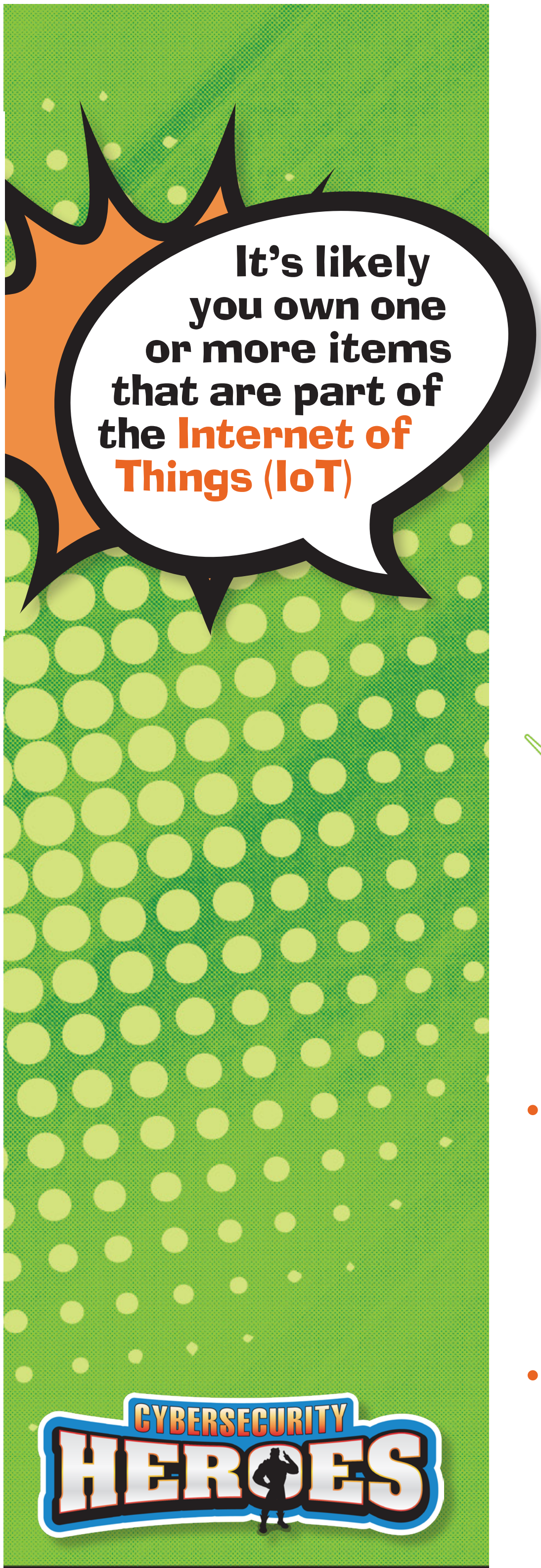
# 3 FACTS ABOUT THE INTERNET OF THINGS

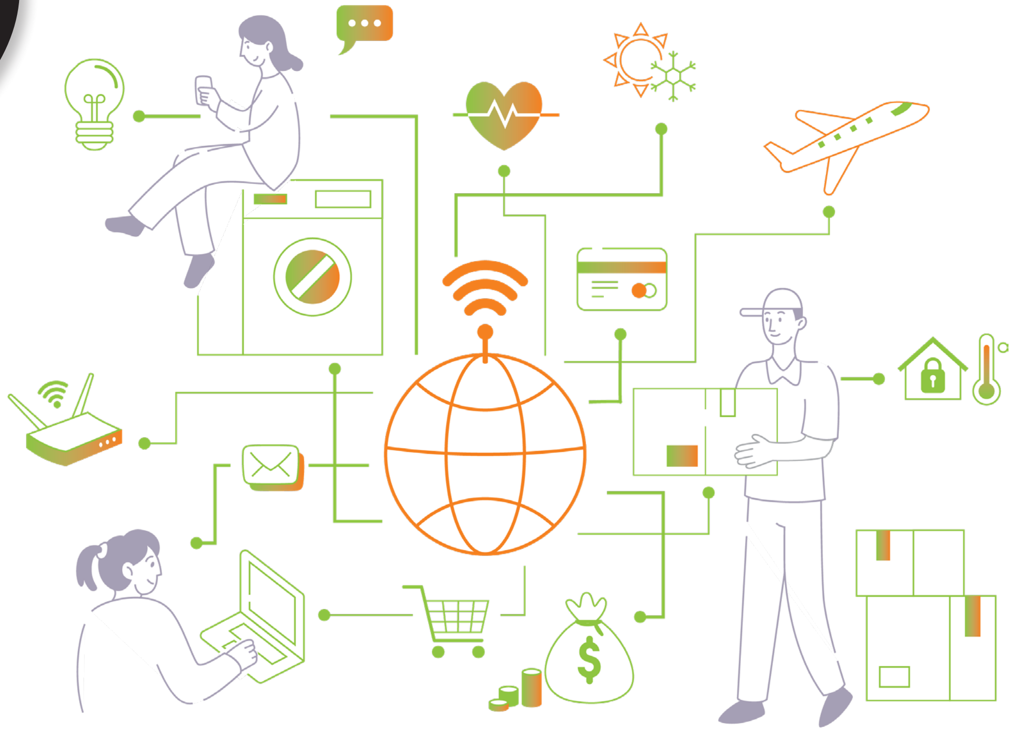
## How to adequately protect yourself


It's likely you own one or more items that are part of the Internet of Things (IoT)
CYBERSECURITY HEROES

proofpoint.

**The Internet of Things or IoT** is a collective term is used to describe a growing number of consumer, medical, and business items that are used to sense, control, and communicate data and activities. The IoT has undoubtedly made life easier for many people and organizations. From fitness trackers and medical monitors, to Wi-Fi-enabled appliances and smart TVs, to industrial sensors and commercial security systems, internet connectivity has made traditionally "dumb" devices "smart."

That connectivity allows data to travel quickly and easily between IoT and "parent" devices (like laptops and smartphones), automating monitoring and documentation. Capabilities like these deliver convenience and, over time, potential cost savings:



- **Consumers can take better control of their health and homes.** For example, they can automatically track and record exercise patterns, remotely adjust thermostat settings for comfort and energy savings, and check on their pets or front porches while they're at work.
- **Organizations can reduce waste and improve regulation of isolated devices and processes.** For example, they can use sensors to automatically adjust lighting and environmental controls, and remotely diagnose equipment problems and identify necessary repairs.
- **Healthcare providers can streamline delivery of services.** For example, medical practitioners can observe key health indicators and, if necessary, make adjustments to implanted devices while patients relax at home.

With IoT devices, the convenience factor is clear—but the risk of using these devices is less obvious. Many people are not aware of the privacy and security concerns associated with IoT devices—or how to adequately protect themselves. Our three facts can help you better understand IoT issues and best practices for safe use of these devices.

# Fact #1

## Many Known Cyberattacks Have Taken Advantage of IoT Vulnerabilities

It's important to realize that IoT risks are not hypothetical; many documented security incidents have stemmed from exploits of device vulnerabilities. These breaches have affected organizations and consumers alike, in ways like the following:

- Medical devices like cardiac devices have been exploited. Aside from manipulating output from pediatric heart monitors to negatively impact patient care, there have been instances where cardiac packer shocks could be stopped or changed to directly harm patients.
- Attackers often hack into home security systems, allowing them to take control of accounts, steal personal information, watch videos, listen, and even broadcast threatening messages to people in the home. In some cases, attackers will use stolen information to extort victims.
- Attackers were able to hack thermostats of two apartment buildings in Finland, preventing heating systems from turning on for nearly a week during a period of below-freezing temperatures.
- By hacking WiFi-enabled printers, attackers have been able to look into the printers' memory to access sensitive documents like contracts and medical forms.
- Numerous parents have reported hacking of WiFi-enabled baby monitors, home cameras, and toys. Incidents range from eavesdropping on private conversations, transmission of explicit content into the home, and even a man's voice claiming he was in a baby's room and was going to kidnap the child.
- There have been several instances of hackers infecting thousands of IoT devices—like lighting systems, vending machines, and DVRs—with malicious software in order to create what is known as a "botnet." When attackers create a botnet, they can control an army of devices as a single unit and use that computing power to disrupt internet services, overpower an organization's network, or steal data on a large scale.

This is just the tip of the iceberg with regard to reported attacks—and many more incidents have likely gone unreported. Researchers now have to act quickly to find vulnerabilities in IoT devices–and determine mitigations–before cybercriminals can exploit them.

# Fact #2

## IoT Manufacturers Aren't Held To Specific Security Standards

The IoT Cybersecurity Improvement Act of 2020 requires that all IoT devices used by US government have to comply with the National Institute of Standards and Technology (NIST) requirements for IoT devices. While this should make IoT developers adopt better security practices, a lack of consistent regulation worldwide has allowed manufacturers to prioritize factors such as time-to-market and aggressive price points over cybersecurity safeguards. As a result, many devices are vulnerable to hacking and compromise.

**Here are a few key things to remember:**

- Many devices use simple default passwords and PINs—like "admin" and "1234"—to allow easy, universal access for purchasers. In fact, default passwords for a range of devices can be found via a quick online search. This does simplify administrative access for IoT users—but it also makes access easy for cyberattackers.
- IoT devices frequently ship with known vulnerabilities that manufacturers address at a later date. This means that, out of the box, devices are prone to compromise and aren't secure until software or firmware is updated (a step many consumers skip due to inconvenience or lack of awareness). Even so, a patched device will never be as secure as a device that was built with security in mind.
- Off-brand devices are frequently less secure than devices manufactured by bigger-name companies. Though vulnerabilities have certainly been identified in products with household names, larger players tend to be more attentive to security practices and more invested in closing security loopholes.

# Fact #3

## You Have the Power To Make the IoT More Secure

Better IoT choices = better IoT security. Here are seven relatively simple things you can do to protect your data and devices:

- **Make an inventory of your IoT devices**: The first step to better security is getting a better sense of what IoT devices you have and are responsible for. It might surprise you just how many devices that you have! Understanding what you have can help you to think more critically about what additional IoT devices you do or do not want to purchase.
- **Change default passwords**: If you're not sure how, refer to the device's manual, do an online search, or contact the manufacturer. And if your device is controlled via a cloud service, be smart about your password selection for your account.
- **Check to see if updates are needed before using**: As we noted, IoT devices can be sold with security issues already in place. In addition, because items can sit on shelves for months before they're purchased, bug fixes and updates are often necessary, even for previously secure devices. For guidance, refer to your manual, do an online search, or refer to the manufacturer's website.
- **Keep your device up to date over the long term**: Set up automatic patches and updates whenever possible. If it's not an option, make it a point to check back for updates. Manufacturers patch bugs and flaws on an ongoing basis—and so should you.
- **Stick with known, reputable brands**: Do your research before buying, and recognize that purchasing based on price alone can be risky. Whenever possible, opt for manufacturers that are proactive about security features. For example, look for devices that will not connect to the internet until the default password is changed.
- **Set up a guest WiFi network for your IoT devices when possible**: It's beneficial to isolate home-based IoT devices (like smart TVs, thermostats, and appliances) from PCs and other data-heavy devices (like smartphones) to reduce risk. However, not all IoT devices will work on a guest network, so be sure to research your devices to see if it's possible. If you need advice on how to do this, start with an online search for your home WiFi router model. Many devices make it easy to set up a guest network. Make sure to set up your guest network with a complex password to join.
- **Keep your router's firmware up to date**: The security of your networks, guest and otherwise, are dependent on your router. If you get in the habit of updating your IoT devices, then you should update your router as well. It will help to keep all of your devices safe.