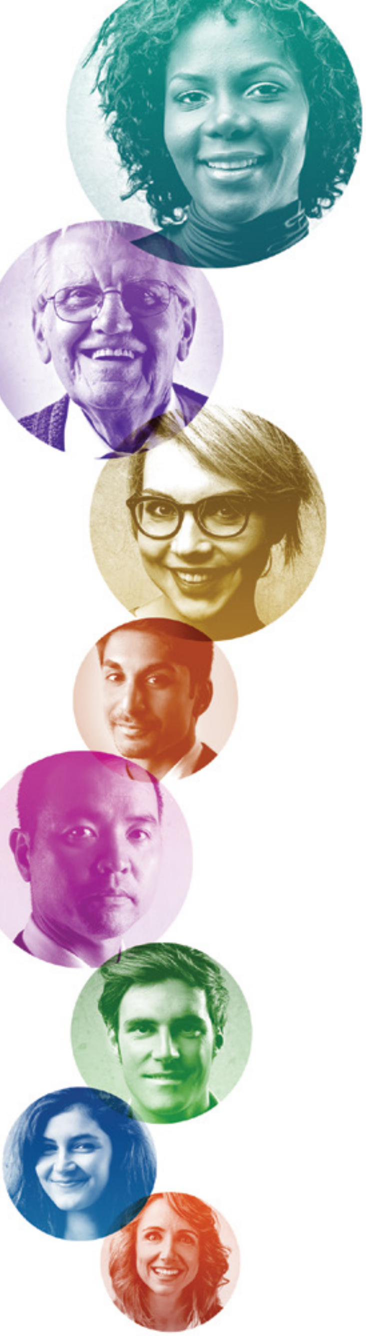

# INTERNET OF THINGS
# TIP CARD

The Internet of Things refers to any object or device that sends and/or receives data automatically via the Internet. This rapidly-expanding set of “things” includes tags (also known as labels or chips that automatically track objects), sensors, and devices that interact with people and share information machine to machine.

## WHY SHOULD WE CARE?

- Cars, appliances, wearables, lighting, healthcare, and home security all contain sensing devices that can talk to another machine and trigger other actions. Examples include: devices that direct your car to an open spot in a parking lot; mechanisms that control energy use in your home; and other tools that track your eating, sleeping, and exercise habits.
- This technology provides a level of convenience to our lives, but it requires that we share more information than ever. The security of this information, and the security of these devices, is not always guaranteed.
- Though many security and resilience risks are not new, the scale of interconnectedness created by the Internet of Things increases the consequences of known risks and creates new ones.

## SIMPLE TIPS

Without a doubt, the Internet of Things makes our lives easier and has many benefits; but we can only reap these benefits if our Internet-enabled devices are secure and trusted. Here are some tips to increase the security of your Internet-enabled devices:

1. **Keep a clean machine.** Like your smartphone or PC, keep any device that connects to the Internet free from viruses and malware. Update the software regularly on the device itself as well as the apps you use to control the device.
2. **Think twice about your device.** Have a solid understanding of how a device works, the nature of its connection to the Internet, and the type of information it stores and transmits.
3. **Secure your network.** Properly secure the wireless network you use to connect Internet-enabled devices.

Stop.Think.Connect.™ is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. The Campaign’s main objective is to help you become more aware of growing cyber threats and arm you with the tools to protect yourself, your family, and your community. For more information visit www.dhs.gov/stopthinkconnect.

Homeland Security

**www.dhs.gov/stopthinkconnect**

STOP | THINK | CONNECT™

OWN › SECURE › PROTECT › IT.

OCTOBER 2019
National Cybersecurity Awareness Month
#BeCyberSmart

# INTERNET OF THINGS

Internet of Things (IoT) or smart devices refers to any object or device that is connected to the Internet. This rapidly expanding set of "things," which can send and receive data, includes cars, appliances, smart watches, lighting, home assistants, home security, and more. #BeCyberSmart to connect with confidence and protect your interconnected world.

## WHY SHOULD WE CARE?

- Cars, appliances, wearables, lighting, healthcare, and home security all contain sensing devices that can talk to another machine and trigger other actions. Examples include devices that direct your car to an open spot in a parking lot; mechanisms that control energy use in your home; and tools that track eating, sleeping, and exercise habits.
- New Internet-connected devices provide a level of convenience in our lives, but they require that we share more information than ever.
- The security of this information, and the security of these devices, is not always guaranteed. Once your device connects to the Internet, you and your device could potentially be vulnerable to all sorts of risks.
- With more connected "things" entering our homes and our workplaces each day, it is important that everyone knows how to secure their digital lives.

## SIMPLE TIPS TO OWN IT.

- **Shake up your password protocol.** Change your device's factory security settings from the default password. This is one of the most important steps to take in the protection of IoT devices. According to NIST guidance, you should consider using the longest password or passphrase permissible. Get creative and create a unique password for your IoT devices. Read the Creating a Password Tip Sheet for more information.
- **Keep tabs on your apps.** Many connected appliances, toys, and devices are supported by a mobile application. Your mobile device could be filled with apps running in the background or using default permissions you never realized you approved—gathering your personal information without your knowledge while also putting your identity and privacy at risk. Check your app permissions and learn to just say "no" to privilege requests that don't make sense. Only download apps from trusted vendors and sources.
- **Secure your network.** Properly secure the wireless network you use to connect Internet-enabled devices. Consider placing these devices on a separate and dedicated network. For more information on how you can secure your network, view the National Security Agency's Cybersecurity Information page.
- **If you connect, you must protect.** Whether it's your computer, smartphone, game device, or other network devices, the best defense is to stay on top of things by updating to the latest security software, web browser, and operating systems. If you have the option to enable automatic updates to defend against the latest risks, turn it on.

For more information about connecting with confidence visit: **https://niccs.us-cert.gov/national-cybersecurity-awareness-month-2019**

CISA CYBER+INFRASTRUCTURE | NATIONAL CYBERSECURITY ALLIANCE | CyberAware