NATIONAL CYBERSECURITY AWARENESS MONTH

DO YOUR PART.
#BECYBERSMART

INTERNET OF THINGS

Now more than ever, consumers spend increasing amounts of time on the Internet. With every social media account you sign up for, every picture you post, and status you update, you are sharing information about yourself with the world. How can you be proactive and "Do Your Part. #BeCyberSmart"? Take these simple steps to connect with confidence and safely navigate the social media world.

Why Should We Care?

- Cars, appliances, fitness trackers and other wearables, lighting, healthcare, home security, and more 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

- **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 IT, Protect IT.** 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.