TIP SHEET

PROTECTING YOUR DIGITAL HOME

PROTECTING YOUR DIGITAL HOME

Every year, more of our home devices, including thermostats, outdoor lighting, door locks, coffee makers, and smoke alarms, are connected to the internet to create a“smart home.” These advances in technology, commonly referred to as the internet of things (IoT), are convenient and may improve efficiency and safety, however they also pose a new set of security risks.

- **Start with your wireless network.** Secure your Wi-Fi network. Your home’s wireless router is the primary entrance for cybercriminals to access all your connected devices. Secure Wi-Fi and digital devices by changing the default password and username. Check your internet provider’s or router manufacturer’s wireless security options. Your internet service provider and router manufacturer may provide information or resources to assist in securing your wireless network.
- **Keep tabs on your apps.** Most connected appliances, toys, and devices are supported by a mobile application. Apps have the ability to gather your personal information while also putting your identity and privacy at risk. Be aware of downloading new, unfamiliar apps or giving default permissions. Check your app permissions and use the “rule of least privilege” to delete apps you no longer need or use.
- **Never click and tell.** Disable location services that allow anyone to see where you are, and where you are not, at any given time. Limit what information you share on social media from home—from personal addresses to where you like to grab coffee. Keep Social Security numbers, account numbers, usernames and passwords private, as well as specific information about yourself, such as your full name, address, birthday, and vacation plans.

KNOW YOUR CYBER BASICS

- **Enable multi-factor authentication (MFA).** to ensure that you are the only person who has access to your account. Use MFA for email, banking, social media, and any other service that requires logging in. If MFA is an option, enable it by using a trusted mobile device such as your smartphone, an authenticator app, or a secure token—a small physical device that can onto hook your key ring.
- If you connect it, you must protect it. Whether it is your computer, smartphone, gaming 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. And, if you are connecting something to your device, such as a universal serial bus (USB) for an external hard drive, make sure your device’s security software scans for viruses and malware. Finally, protect your devices with antivirus software, and be sure to periodically back up any data that cannot be recreated, such as photos or personal documents.

FOLLOW-ON RESOURCES

- Securing Wireless Networks
- Multi-Factor Authentication (MFA) Guide
- Social Media Cybersecurity Tip Sheet
- StaySafeOnline.org
- Report a Cyber Crime