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.

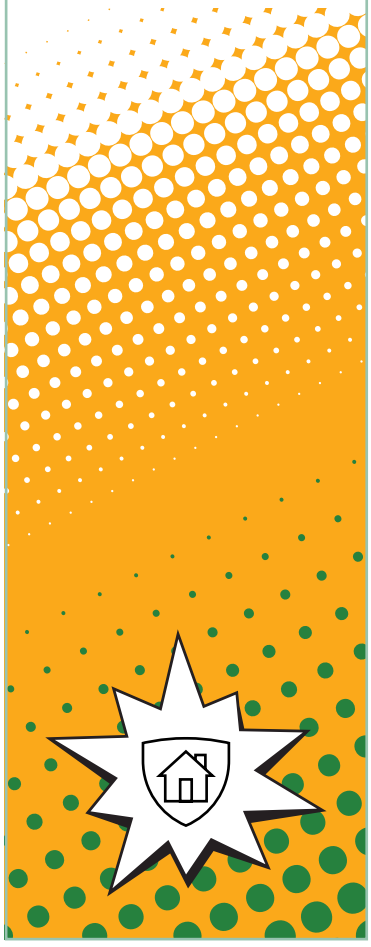
- **Start with your wireless network.** Secure your Wi-Fi network. Your home's wireless router is the primary entrance for cybercriminals to access all your connected devices. Secure Wi-Fi and digital devices by changing the default password and username. Check your internet provider's or router manufacturer's 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



TIP SHEET

BE CYBER SECURE AT HOME

BE CYBER SECURE AT HOME

In 2022, CISA reported that, "Every organization in the United States is at risk from cyber threats that can disrupt essential services and potentially result in impacts to public safety." Businesses face significant financial loss when a cyberattack occurs. Cybercriminals often rely on human error—employees failing to install software patches or clicking on malicious links—to gain access to systems. From the top leadership to the newest employee, cybersecurity requires the vigilance of everyone to keep data, customers, and capital safe and secure.

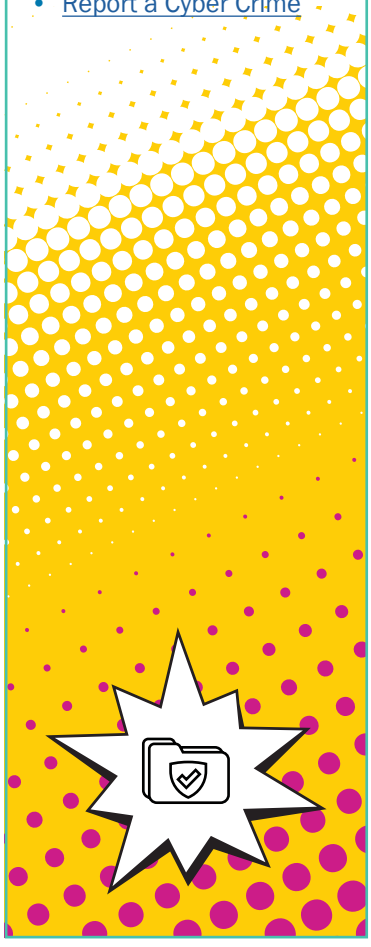
- **Use only approved tools.** Only use organization-approved software and tools for business, including company-provided or approved video conferencing and collaboration tools to initiate and schedule meetings. Unapproved free tools may make your system vulnerable, so check in with your Information Technology (IT) team before using them on your work computer.
- **Secure your meetings.** Take precautions to ensure your virtual meetings are only attended by intended individuals. Plan for what to do if a public meeting is disrupted.
- **Secure your information.** Tailor your security precautions appropriately to the sensitivity of your data. Only share data necessary to accomplish the goals of your meeting.
- **Secure yourself.** Take precautions to avoid unintentionally revealing business and personal information. Ensure home networks are secured.

KNOW YOUR CYBER BASICS

- **Treat business information as personal information.** Business information typically includes a mix of personal and proprietary data. While you may think of trade secrets and company credit accounts, it also includes employee personally identifiable information (PII) through tax forms and payroll accounts. Do not share PII with unknown parties or over unsecured networks.
- **Don't make passwords easy to guess.** As "smart" or data-driven technology evolves, it is important to remember that security measures only work if employees use them correctly. Smart technology runs on data, meaning devices such as smartphones, laptop computers, wireless printers, and other devices are constantly exchanging data to complete tasks. Take proper security precautions and ensure correct configuration to wireless devices in order to prevent data breaches.
- **Stay up to date.** Keep your software updated to the latest version available as per your organization's guidelines. Talk to your organization's IT team about turning on automatic updates, so you don't have to think about it, and set your security software to run regular scans.

FOLLOW-ON RESOURCES

- Telework Essentials Toolkit
- Telework Reference Materials For The At-Home Worker
- Internet of Things Tip Card
- Phishing Tip Sheet
- Social Media Cybersecurity Tip Sheet
- StaySafeOnline.org
- Report a Cyber Crime

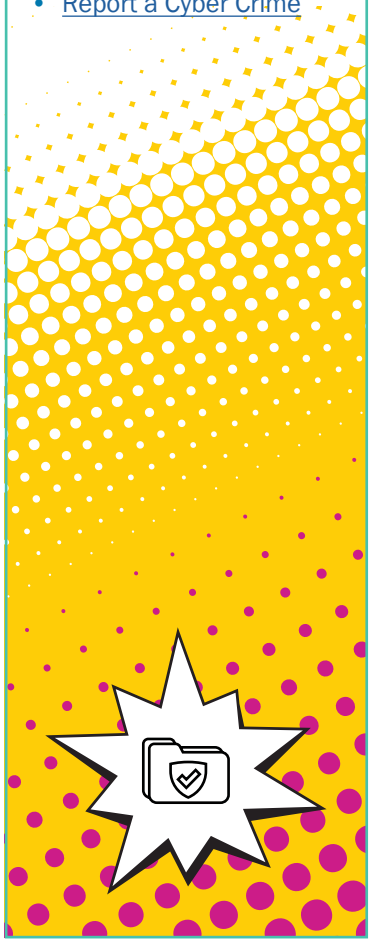


CONTINUED ON NEXT PAGE ▸

- **Follow your company's social media policies.** Employees should avoid oversharing on social media and should not conduct official business, exchange payment, or share PII on social media platforms.
- **Don't trust the sender immediately.** Data breaches can occur even without a cybercriminal hacking into an organization's infrastructure. Many data breaches can be traced back to a single security vulnerability, phishing attempt, or instance of accidental exposure. Be wary of unusual sources, do not click on unknown links, and delete suspicious messages after reporting or forwarding to a supervisor, so that any necessary organizational updates, alerts, or changes can be put into place.

FOLLOW-ON RESOURCES

- Telework Essentials Toolkit
- Telework Reference Matierals For The At-Home Worker
- Internet of Things Tip Card
- Phishing Tip Sheet
- Social Media Cybersecurity Tip Sheet
- StaySafeOnline.org
- Report a Cyber Crime



LEARN MORE DURING CYBERSECURITY AWARENESS MONTH

Thank you for your continued support and commitment to Cybersecurity Awareness Month and helping all Americans stay safe and secure online. Please visit www.cisa.gov/cybersecurity-awareness-month to learn more.