5 STEPS TO PROTECTING YOUR DIGITAL OFFICE

CYBERSECURITY AWARENESS MONTH

More and more of our office devices—including thermostats, door locks, coffee machines, and smoke alarms—are now connected to the Internet. This enables us to control our devices on our smartphones, no matter our location, which in turn can save us time and money while providing convenience and even safety. These advances in technology are innovative and intriguing, however they also pose a new set of security risks. #BeCyberSmart to connect with confidence and protect your digital office.

ADVANTEX

1. **Secure your Wi-Fi Network.**
Your home's wireless router is the primary entrance for cybercriminals to access all of your connected devices. Secure your Wi-Fi network and your digital devices by changing the factory-set default password and username. For more information about protecting your office network, check out the National Security Agency's Cybersecurity Information page.

2. **Double your login protection.**
Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other online accounts 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 hook onto your key ring.

3. **If you connect, you must protect.**
Whether it's your work computer, smartphone, 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're putting something into your device, such as a 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.

4. **Keep tabs on your apps.**
Most connected appliances, toys, and devices are supported by a mobile application. Your mobile device could be filled with suspicious 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 use the "rule of least privilege" to delete what you don't need or no longer use. Learn to just say "no" to privilege requests that don't make sense. Only download apps from trusted vendors and sources.

5. **Never click and tell.**
Limit what information you post on social media—from personal addresses to where you like to grab coffee. What many people don't realize is that these seemingly random details are all that criminals need to know to target you, your business, and your physical belongings—online and in the real world. Keep Social Security numbers, account numbers, and passwords private, as well as specific information about yourself, such as your address, birthday, and even vacation plans. Disable location services that allow anyone to see where you are— and where you aren't—at any given time.