WFG National Title

SAFE
Security Awareness For Everyone

Tipsheet

Protect Your Digital Home (and Connected Devices)

More and more of our home devices - including thermostats, door locks, coffee machines, and smoke alarms - are now connected to the Internet.

We can 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. They can also pose a new set of security risks. In spite of this, you can safely connect with confidence by using the following simple tips. You've heard them before, so take the next step and start using them.

- **Secure your Wi-Fi network.** Your home's wireless router is the primary entrance for cybercriminals to access all of your connected devices. Secure it and your digital devices by changing the factory-set default password and username.
- **Double your login protection.** Enable multi-factor authentication (MFA) to ensure that the only person with access to your account is you. Use it for email, banking, social media (and any other service that requires logging in) by using a trusted mobile device such as your smartphone, an authenticator app, or a secure token you carry that can hook onto your key ring.
- **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. Be sure to set up automatic updates to defend against the latest risks.
- **Protect your devices with antivirus software.** Be sure to periodically back up any data that cannot be recreated, such as photos or personal documents. If you use a USB for an external hard drive, make sure your device's security software scans for viruses and malware before use.
- **Keep tabs on your apps.** Most 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 - putting your identity and privacy at risk. Delete what you don't need or no longer use.
- **Check your app permissions.** Learn to just say "no" to access requests that don't make sense, like your Camera or Microphone. Disable location services that allow anyone to see where you are at any given time.
- **Don't overshare on social media.** Limit what information you post on social media - from personal addresses to where you like to grab coffee, birth dates, and even vacation plans. These seemingly random details can be used to target you or others and your physical belongings, both online and in the real world.

west protect℠