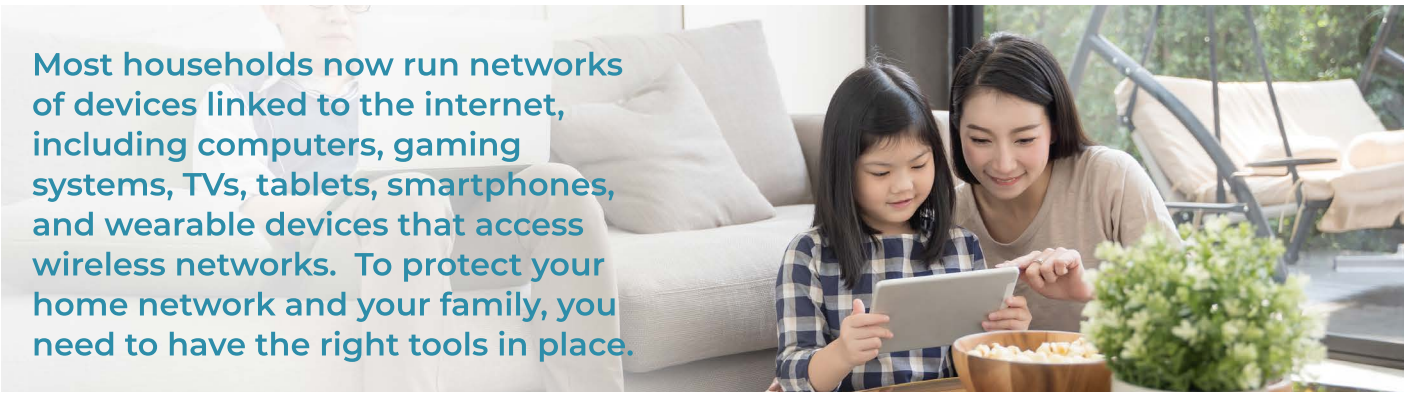
WFG National Title

SAFE Tipsheet

Securing Your Home Network



Most households now run networks of devices linked to the internet, including computers, gaming systems, TVs, tablets, smartphones, and wearable devices that access wireless networks. To protect your home network and your family, you need to have the right tools in place.

The first step is to ensure all of your internet-enabled devices have the latest operating systems, web browsers, and security software - this is the best defense against viruses, malware, and other online threats. Don't forget mobile devices that access your wireless network!

However, unless you secure your router, you're vulnerable to people accessing the information on your computer and potentially using your network to commit cybercrimes.

Ways to Secure your Wireless Router:

- **Change the name of your router:** The default ID – called a Service Set Identifier (SSID) or Extended Service Set Identifier" (ESSID) – is assigned by the manufacturer. Change your router name to one that's unique to you and won't be easily guessed by others.
- **Change the preset phassphrase on your router:** Leaving a default passphrase unchanged makes it much easier for hackers to access your network, so change it as soon as possible.
- **Review security options:** When choosing your router's level of security, opt for WPA2, if available, or WPA – these levels are more secure than the WEP option.
- **Create a guest passphrase:** Some routers allow for guests to use networks via separate guest passphrases. If you have many visitors to your home, it's a good idea to set up a guest network. Your work and personal devices should always be separated.
- **Use a firewall:** Firewalls help keep hackers from using your device to send out your personal information without your permission. While antivirus software scans incoming emails and files, a firewall is like a guard, watching for attempts to access your system and blocking communications with sources you don't permit. Your operating system and/or security software likely comes with a pre-installed firewall, but make sure you turn on these features.

Protect Yourself with these Best Practice Tips:

- **Protect all devices that connect to the internet:** Not just computers, but smartphones, gaming systems, and other web-enabled devices also need protection from viruses and malware.
- **Plug & Scan:** USBs and other external devices can be infected by viruses and malware, so use your security software to scan them.
- **When banking and shopping:** Look for web addresses with "HTTPS://," which means the site takes extra measures to help secure your information. "HTTP://" is not secure.
- **Back it up:** Protect valuable files by making electronic copies and storing them safely.

July 2021