

Securing Your Home Network

A protected home network means your family can use the Internet safely and securely.

Most households now run networks of devices linked to the Internet, including computers, laptops, gaming devices, TVs, tablets, and smartphones that access wireless networks. To protect your home network and your family, you need to have the right tools in place and confidence that family members can use the Internet safely and securely.

The first step is to Keep a Clean Machine and make sure all of your Internet-enabled devices have the latest operating system, web browsers and security software. This includes mobile devices that access your wireless network.

Secure Your Wireless Router

A wireless network means connecting an Internet access point – such as a cable or DSL modem – to a wireless router. Going wireless is a convenient way to allow multiple devices to connect to the Internet from different areas of your home. However, unless you secure your router, you're vulnerable to people accessing information on your computer, using your Internet service for free and potentially using your network to commit cybercrimes.

Here are 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 to a name that is unique to you and won't be easily guessed by others.
- **Change the pre-set password on your router:** When creating a new password, make sure it is long and strong, using a mix of numbers, letters and symbols.
- **Review security options:** When choosing your router's level of security, opt for WPA2, if available, or WPA. They are more secure than the WEP option.
- **Create a guest password:** Some routers allow for guests to use the network via a separate password. If you have many visitors to your home, it's a good idea to set up a guest network.
- **Use a firewall:** Firewalls help keep hackers from using your computer to send out your personal information without your permission. While anti-virus software scans incoming email 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 STOP. THINK. CONNECT. Tips:

- **Keep a clean machine:** Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.
- **Automate software updates:** Many software programs will automatically connect and update to defend against known risks. Turn on automatic updates if that's an available option.

- **Protect all devices that connect to the Internet:** Along with computers, smart phones, 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. Use your security software to scan them.
- **Protect your \$\$:** When banking and shopping, check to be sure the sites is security enabled. Look for web addresses with “https://” or “shttp://”, which means the site takes extra measures to help secure your information. “Http://” is not secure.
- **Back it up:** Protect your valuable work, music, photos, and other digital information by making an electronic copy and storing it safely.

- See more at: <http://www.staysafeonline.org/stay-safe-online/keep-a-clean-machine/securing-your-home-network#sthash.LbrYC3J0.dpuf>