

Tips to Help Secure Your Wireless Network at Home

Today many consumers choosing broadband cable for the fastest Internet service available are also setting up wireless hotspots in their homes using relatively inexpensive and easy-to-install wireless hardware to enjoy the freedom of in-house mobility that wireless provides.

Linking your computer and other devices to a wireless home network is great for convenience, but potentially not so great for security. The same technology that lets you use your laptop in any room of the house could give your neighbor—or a hacker—access to your network and the private information it contains.

The United States Computer Emergency Readiness Team recommends the following tips to minimize the risks to your wireless network:

Change default passwords - Most network devices, including wireless access points, are pre-configured with default administrator passwords to simplify setup. These default passwords are easily found online, so they don't provide any protection. Changing default passwords makes it harder for attackers to take control of the device. Consider using a password that combines both letters and symbols and is no less than eight characters long.

Restrict access - Only allow authorized users to access your network. Each piece of hardware connected to a network has a MAC (media access control) address. You can restrict or allow access to your network by filtering MAC addresses. Consult your user documentation to get specific information about enabling these features. There are also several technologies available that require wireless users to authenticate before accessing the network.

Encrypt the data on your network - WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access) both encrypt information on wireless devices. However, WEP has a number of security issues that make it less effective than WPA, so you should specifically look for gear that supports encryption via WPA. Encrypting the data will help prevent anyone who might be able to access your network from viewing your data.

Protect your SSID - To avoid outsiders easily accessing your network, avoid publicizing your SSID. Consult your user documentation to see if you can change the default SSID to make it more difficult to guess.

Install a firewall - While it is a good security practice to install a firewall on your network, you should also install a firewall directly on your wireless devices (a host-based firewall). Attackers who can directly tap into your wireless network may be able to circumvent your network firewall—a host-based firewall will add a layer of protection to the data on your computer.

Always install active and up-to-date anti-virus software - You can reduce the damage attackers may be able to inflict on your network and wireless computer by installing anti-virus software and keeping your virus definitions up-to-date. Many of these programs also have additional features that may protect against or detect spyware and Trojan horses.

To help protect its customers, Comcast offers the McAfee® Security Suite for no additional charge to Comcast High-Speed Internet subscribers to help keep their computers safe, protected and virus-free. Comcast also offers a comprehensive Security Channel on its consumer portal, Comcast.net, available at www.comcast.net/security. The Comcast Security Channel serves as an online resource to help customers protect themselves from spam, viruses and other online threats. In addition to the Security Channel, the Comcast toolbar is another resource that can be downloaded from www.comcast.net free of charge, which includes spyware detection and removal, pop-up blocker and anti-phishing software.