

10 Tips to Secure your Wi-fi Network

Many persons setting up wireless home networks rush through the job to get their Internet connectivity working as quickly as possible. That's totally understandable. It's also quite risky as numerous security problems can result. Today's [Wi-Fi](#) (Wireless fidelity) networking products don't always help the situation as configuring their security features can be time-consuming and non-intuitive. The recommendations below summarize the steps you should take to improve the security of your home wireless network.

1. [Change Default Administrator Passwords \(and Usernames\)](#)

At the core of most Wi-Fi home networks is an access point or router. To set up these pieces of equipment, manufacturers provide Web pages that allow owners to enter their network address and account information. These Web tools are protected with a login screen (username and password) so that only the rightful owner can do this. However, for any given piece of equipment, the logins provided are simple and very well-known to hackers on the Internet. Change these settings immediately.

2. [Turn on \(Compatible\) WPA / WEP Encryption](#)

All Wi-Fi equipment supports some form of *encryption*. Encryption technology scrambles messages sent over wireless networks so that they cannot be easily read by humans. Several encryption technologies exist for Wi-Fi today. Naturally you will want to pick the strongest form of encryption that works with your wireless network. However, the way these technologies work, all Wi-Fi devices on your network must share the identical encryption settings. Therefore you may need to find a "lowest common demoninator" setting. WPA2 is Most Preferable Encryption type.

3. [Change the Default SSID](#)

Access points and routers all use a network name called the [SSID](#). Manufacturers normally ship their products with the same SSID set. For example, the SSID for Linksys devices is normally "linksys." True, knowing the SSID does not by itself allow your neighbors to break into your network, but it is a start. More importantly, when someone finds a default SSID, they see it is a poorly configured network and are much more likely to attack it. Change the default SSID immediately when configuring wireless security on your network.

4. [Enable MAC Address Filtering](#)

Each piece of Wi-Fi gear possesses a unique identifier called the *physical address* or *MAC address*. Access points and routers keep track of the MAC addresses of all devices that connect to them. Many such products offer the owner an option to key in the MAC addresses of their home equipment, that restricts the network to only allow connections from those devices. Do this, but also know that the feature is not so powerful as it may seem. Hackers and their software programs can fake MAC addresses easily.

5. [Disable SSID Broadcast](#)

In Wi-Fi networking, the wireless access point or router typically broadcasts the network name (SSID) over the air at regular intervals. This feature was designed for businesses and mobile hotspots where Wi-Fi clients may roam in and out of range. In the home, this roaming feature is unnecessary, and it increases the likelihood someone will try to log in to your home network. Fortunately, most Wi-Fi access points allow the SSID broadcast feature to be disabled by the network administrator.

6. [Do Not Auto-Connect to Open Wi-Fi Networks](#)

Connecting to an open Wi-Fi network such as a free wireless hotspot or your neighbor's router exposes your computer to security risks. Although not normally enabled, most computers have a setting available allowing these connections to happen automatically without notifying you (the user). This setting should not be enabled except in temporary situations.

7. [Assign Static IP Addresses to Devices](#)

Most home networkers gravitate toward using *dynamic IP addresses*. [DHCP](#) technology is indeed easy to set up. Unfortunately, this convenience also works to the advantage of network attackers, who can easily obtain valid IP addresses from your network's DHCP pool. Turn off DHCP on the router or access point, set a fixed IP address

range instead, then configure each connected device to match. Use a *private IP address range* (like 10.0.0.x) to prevent computers from being directly reached from the Internet.

8. Enable Firewalls On Each Computer and the Router

Modern network routers contain built-in firewall capability, but the option also exists to disable them. Ensure that your router's firewall is turned on. For extra protection, consider installing and running *personal firewall software* on each computer connected to the router.

9. Position the Router or Access Point Safely

Wi-Fi signals normally reach to the exterior of a home. A small amount of signal leakage outdoors is not a problem, but the further this signal reaches, the easier it is for others to detect and exploit. Wi-Fi signals often reach through neighboring homes and into streets, for example. When installing a wireless home network, the position of the access point or router determines its reach. Try to position these devices near the center of the home rather than near windows to minimize leakage.

10. Turn Off the Network During Extended Periods of Non-Use

The ultimate in wireless security measures, shutting down your network will most certainly prevent outside hackers from breaking in! While impractical to turn off and on the devices frequently, at least consider doing so during travel or extended periods offline. Computer disk drives have been known to suffer from power cycle wear-and-tear, but this is a secondary concern for broadband modems and routers.