

Top 10 Tips for Wireless Networking Security

1. Change your password.

Always make sure you change any passwords that are supplied with your product. These are very well known to hackers. Remember, 'password' is not a password.
MOST IMPORTANTLY, DON'T PUT YOUR PASSWORD ON A POST-IT!!!

2. Get your encryption on.

WPA or WEP are just two of the encryptions methods that permit you to secure all the connections made to your wireless or wi-fi network. This prevents others from connecting and also prevents them from accessing the data you transmit on your wireless network.

3. Change, change, change...

Make sure you change settings like SSID (the name of your network) which are set by the manufacturer. A default setting like the SSID is also a red flag to people that your network is not secured.

4. Use filters.

Every computer you use, even your cellphone, has something called a physical network address referred to as a MAC. Almost every wireless access point or router has an option to permit you to filter by MAC address. This helps you to limit your network to the specific computers you own and use.

5. Don't broadcast.

Most wireless access points and routers will broadcast the network name (the SSID I mentioned before). This is an easy setting to turn off. Keep in mind, though that your PC won't 'see' the network now, but if you can't see it neither can others.

6. Practice safe wi-fi.

Your own computer can be at risk, especially for laptop users. Make sure you turn off any feature that will 'auto-connect' your computer to available networks. Remember, if you can connect to something on a different network, somebody can connect to you.

7. Get fixed.

If you have a very small network with just 1 or 2 computers, you may want to put a fixed IP address on your computer and turn-off the DHCP service which gives that same information to computers trying to connect to your network.

8. Put up some walls.

Always have your wireless access point or router's firewall features turned on. You should also install a personal firewall on your computer to add an additional layer of protection.

9. Location is key.

Wireless signals from your home's network can and do extend outside your walls. Try to keep your wireless access point closest to the center of your house to both give you optimum reception inside your house and reduced signal range outside your house.

10. When all else fails, turn it off.

Sometimes the best solutions are the simplest. If you're not home, or not using your network for extended periods of time, just turn off your wireless access point. It normally doesn't have moving parts like your computer's hard disk.