

Wireless Security

With no cables to run, wireless networks are convenient and easy to install, so business' and now homes with high-speed Internet access are adopting them at a rapid pace. However, wireless networking is inherently risky because it sends information over radio waves. Like signals from your cellular or cordless phones, signals from your wireless network can also be intercepted as well as your internet access could possibly be used by someone your entirely unaware of.

Fortunately, there are several steps you can take to improve wireless security, and the networking industry is working on even stronger measures, which will become available in the future. Meanwhile, you can start with the measures described bellow, so you can enjoy the freedom of wireless networking while lessening the risks of intrusion or unauthorized access.

1. First step is to enable WPA or WEP. WPA and WEP aren't entirely secure as by now virtually everyone knows, but at least it's a first barrier. And best of all, nearly every Wi-Fi certified product ships with basic encryption capabilities (40-bit key WEP) but by default these setting are turned off when shipped and the end user is required to setup the security settings.
2. Change the default password on your access point or wireless router. Any hacker knows the manufacturers' default passwords, and will try them first.
3. Change the default SSID of your product. Most often the access points/wireless routers we found had the manufacturer's default SSID. That is if your access point/wireless router still had the manufacturer's default SSID, you hadn't bothered to change the default password, either.
4. As an added precaution, be sure to change the SSID on a regular basis, so any hacker who may have figured out your network's SSID in the past will have to figure out the SSID again and again. This will deter future intrusion attempts.
5. If your access point supports it, disable "broadcast SSID". As you take your access point out of the box, broadcast SSID is enabled which means that it will accept *any* SSID. By disabling that feature, the SSID configured in the client must match the SSID of the access point.
6. Many access points allow you to control access based on the MAC address of the NIC attempting to associate with it. If the MAC address of your NIC isn't in the table of the access point, you won't associate with it. And while it's true that there are ways of spoofing a MAC address that's been sniffed out of the air, it takes an additional level of sophistication to spoof a MAC address. The downside of deploying MAC address tables is that if you have a lot of access points, maintaining the tables in each access point could be time consuming. Some higher-end, enterprise-level access points have mechanisms for updating these tables across multiple access points of the same brand.
7. If you're setting up a wireless router, think about assigning static IP addresses for your wireless NICs and turn off DHCP. It's true that it's more of an administrative overhead to manage.
8. If you're using a wireless router and have decided to turn off DHCP, also consider changing the IP subnet. Many wireless routers default to the 192.168.1.0 network and use 192.168.1.1 as the default router. We discovered one network that didn't give us an IP address, but we assumed that they were using the defaults. We were right. We configured our notebook with an IP address in the 192.168.1.0 network using 192.168.1.1 as the router address, and we had access to the Internet through their network.
9. Finally, think about locating the access points toward the center of your building rather than near the windows. Plan your coverage to radiate out to the windows, but not beyond. If the access points are located near the windows, a stronger signal will be radiated outside your building making it easier for people to find you.