

## 10 Tips To Secure Your Laptop

Whether you're home or on the road, these security steps will help protect you and your computer from wireless scoundrels.

By David Strom, [InformationWeek](#)

Nov. 24, 2007

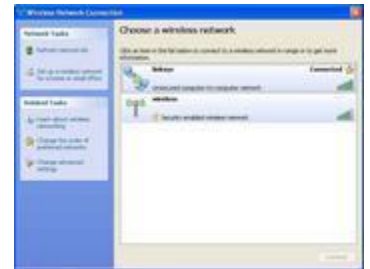
URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=203102748>

As more people use laptops for their primary work PCs, the chances for being compromised because of wireless miscreants loom large. Here are 10 how-to tips to protect yourself and make the best use of a wireless network, whether you are at home, at work, or in between.

### 1. Make sure you are connecting to the right network.

Although this sounds sort of obvious, I've noticed in my travels that there are lots of unscrupulous people who purposely name their wireless connection "Linksys," or some other common vendor's name, in hopes of getting someone who is less than careful to connect to them. The security industry calls these sorts of conditions "[evil twins.](#)"

The issue here is that your laptop is set up to automatically connect to a particular access point's Service Set Identifier (SSID) -- so someone who uses a common name can grab a bunch of users who aren't wary. There are also tools (such as AirJack) that an attacker can use to disconnect users from the right access point and have them then connect to his rogue network. (More information about this exploit is available from [Nomad Mobile Research Centre.](#))



**Avoid peer-to-peer connections, like the Linksys one in this example.**

[\(click for image gallery\)](#)

When you are out on the road, look carefully at the screen that shows the available network connections, and particularly at the different icons next to the connections. The icon that looks like a light beacon indicates an access point, while the one showing two computers with connecting lines indicates a peer-to-peer connection. These peer-to-peer connections are the ones to avoid. There is also a padlock icon that indicates whether or not an access point is running encryption protocols. In the screen shot above (we use Windows XP for our examples), the "wireless" network is an access point running encryption, while we have mistakenly connected to another computer called "Linksys." If you are worried about this, there are several steps that you can take, including disabling automatic connections and using a unique name for your home network. Go to your Wireless Networks panel, click the "Advanced" button and then uncheck "Automatically connect to non-preferred networks" and check "Access point (infrastructure) networks only."

If using SP2, configure every wireless network to *not* connect automatically when the network is in range by going into the "[Connection](#)" box under Wireless Properties.

### 2. Secure your connection.

This next tip is for your own home-based wireless network. If you don't mind having all

your neighbors share your wireless connection, then just ignore this tip and keep your access point running unsecured.

For the rest of us, make sure your home wireless network is secured with WPA2 encryption, if you can. This is the strongest encryption method, and while it is somewhat cumbersome to set up, it is worth the pain to keep prying eyes from examining what is going on over your network. To support WPA2, you'll need to [patch XP](#) (and you need to be running SP2).

To set up WPA2 once you have installed the patch, bring up the wireless network properties sheet and choose WPA2-PSK from the pull-down menu.

If you can't run WPA2 on all of your home machines, then consider some other encryption scheme -- anything is better than nothing. ("Open" in the screen shot below means you aren't running with any encryption.) When you are on the road, if you have a choice, choose the wireless network that is encrypted if you have the appropriate access and a password.

### 3. What's the frequency, Kenneth?

If you want to get the best performance out of your home wireless network, make sure to set up your access point to use a frequency channel that isn't already occupied by one of your neighbors' networks. Of course, this can change from day to day as new people move in or as your neighbors buy new gear, so it is worth checking the airwaves around your home and seeing who is broadcasting on which frequency.

Every wireless adapter comes with monitoring software, but sometimes you have to look around your hard disk to find it. In the sample screen shot on the next page, we use the Linksys monitoring software and see which channel our wireless network is broadcasting on, along with other information such as the kind of encryption being used and the MAC address of the access point itself. The frequency channels are important, because Wi-Fi networks have a limited number of frequency bands that they operate on. Each 802.11 protocol (a, b, g, and n) uses a different combination of frequencies to allow multiple devices to broadcast. (Moonblink offers a nice [graphical depiction of the 802.11b frequencies](#), the most common ones in use today.)

Even though 802.11b has 11 different frequencies, only three of them aren't overlapping: 1, 6, and 11. The issue gets murkier when you add the newer wireless products, because, not only are the frequencies overlapping, but also because the 802.11n products actually can [interfere with your neighbor's older 11b/g equipment](#).

This means that if you live in any high-density wireless area and don't care about what happens to your neighbors, then upgrade to an 802.11n network.

**4. Find the strongest signals.** When you are on the road, you often have a choice about which network to connect to. All other things being equal, choose the one with the strongest signal strength if you can. The stronger the signal, the faster your connection and the less time you have to waste before you have to catch your flight. (Lisa Phifer offers more technical information about how to [measure signal strength](#).)

In years past there was talk about people wiring up their own external antennas based on [potato-chip canisters](#) to boost their signal strength, but as wireless network adapters have become better integrated into laptops, this is getting harder



Select the option to only access infrastructure networks.

[\(click for image gallery\)](#)



Encrypt your home network with WPA2, if possible.

[\(click for image gallery\)](#)



Use a different wireless frequency than your neighbors use.

[\(click for image gallery\)](#)

to do. (You'd have to open up your laptop and see if you can remove the lead wire for the antenna.) The best bet is to use equipment with the newer 802.11g or n adapters, as they have the best reach.

But you don't have to re-wire your laptop; you can also be smart about where you sit to find the best connection. Look around and see where your fellow travelers are located. They might have done the wireless airport site survey already for you. Of course, it would be nice if these Wi-Fi-rich areas were also located near AC power outlets, which are getting to be an endangered species in airports these days. (Another travel tip: carry a three-way tap so you can share your plug with others.)

Also, keep in mind that many airport restaurants and lounges have their own free Wi-Fi -- you can sit in the lounge, or even nearby, and get the best signals there. If you really want to obsess about signal strength, buy something like the [Kensington Wi-Fi Finder Plus](#) that will report on what networks are available nearby without having to open up your laptop.

## 5. Turn off your wireless network adapter when you are on the plane.

You can save battery life, and you are better protected, too. While you are at it, turn off the Bluetooth radios on your laptop for an extra energy boost.

Also, turn off any Windows file shares when you travel. To do this, go to your wireless connection's Properties panel and make sure that "Client for Microsoft Networks" and "File and Printer Sharing for Microsoft Networks" are both unchecked.

Finally, turn off your iTunes sharing arrangements. At many hotels, I am able to browse music libraries and shared directories of other guests, which, while amusing for me, is probably not what they have intended. This is found in iTunes' Preferences, in the Sharing control panel. **6. Use whole disk encryption on your laptop.**

And think about using a better protection scheme for your USB thumb drives, too. You never know when someone will steal your data or break into your car or hotel room and lift the laptop. (That happened to me on one business trip.) I like [PGP Disk](#), but there are [others that cost next to nothing](#) and provide plenty of protection. For an added layer of protection, use a security cable when you leave your laptop in your hotel room.

## 7. If you are having trouble connecting to a network, trying rebooting Windows.

Sometimes Windows just gets confused and a reboot will find a network and connect right up. I don't know why this is the case. Macs don't seem to have this problem.

## 8. Make sure you have a firewall and it is running.

I am using Kaspersky, but there are dozens of different programs that will protect your laptop, including free ones from AVG and Zone Alarm. You need to use them if you don't want to catch any infections when you are out on the road. Windows has had a built-in firewall since XP SP2, but neither that one, nor the one that comes with Vista, is as good as any of the third-party products. The [Firewall Leak Tester](#) Web site is great place to learn more about firewalls and what they do and don't protect.

## 9. Pick your hotspot connection and your supplier carefully.

When I travel, I first try to use the free wired connection at the hotel or a public library. If that isn't possible, then I go someplace that has T-Mobile service, because it has the best security and also supports encrypted connections. A lot of airports now charge you for access, but keep in mind tip #4 about finding a restaurant or other business that has a free connection.



**Turn off file shares while traveling.**

[\(click for image gallery\)](#)



**Disable automatic connections on your wireless network.**

[\(click for image gallery\)](#)

You can typically [purchase an access pass](#) for a few hours, a 24-hour period, or an entire month. Boingo.com for example has plans at \$8 per day and \$22 per month for North American hotspots, and \$39 per month for global coverage. If you are a frequent traveler or know you are going to be on the road for awhile, sign up for a monthly access plan.

## 10. Finally, don't blithely accept SSL certificates and SSH public keys.

Before you accept, make sure you first understand what you are accepting. Don't log on to a public hotspot that presents you with an invalid certificate, and know when to expect the certificate in the logon process.

## Summary

This may all seem like a lot of work simply to roam around the world, but if you follow these 10 tips you will find that you are protected for the majority of situations and can balance protection with the convenience of using a wireless network.

### **[Red Hat Command Center](#)**


Simple, affordable IT systems monitoring. 30 Day Evaluation.  
[redhat.com](http://redhat.com)

### **[Google Intranet Search](#)**

Search your intranet, file shares, and enterprise systems with Google.  
[www.google.com/enterprise](http://www.google.com/enterprise)

### **[MS in Info Tech Degree](#)**

Drexel U. Exec. Ed. 18-month program. Learn More Now!  
[www.iSchool.Drexel.edu](http://www.iSchool.Drexel.edu)

Ads by 

Copyright © 2007 [CMP Media LLC](#)