



Special Report

Using Wi-Fi Safely

By the SWCP staff

Wi-Fi radio connections to the Internet at home, the office, and even in your local coffee shop are no longer a futuristic novelty but a convenience that many users rely upon every day. With ease, however, may come an unrealistic – and even dangerous – feeling of safety.

As you might suspect, broadcasting your personal data through the air is not without its hazards. Consequences can be extremely serious, like having your computer directly accessed by hackers, with your confidential information, documents, and credit card numbers stolen, or your computer hijacked for other illegal activities for which you might be blamed.

In this special edition of the *SWCP Portal*, we'll show you how to limit these risks, both at home and out in the world.

Basic Home and Office Defense

Most of the steps to protect your computer should be implemented from the very moment when you first set it up for Wi-Fi. While it's impossible to guarantee absolute security, these steps may persuade a wireless hacker to choose a somewhat easier target.

- 1. Change your gateway's name and password.** This should be done first thing, but be sure you write them down someplace secure.
- 2. Disable the "ad hoc" mode.** The "ad hoc" mode allows peer-to-peer networking, which could permit rogue users to connect through a legitimate client. Enable "infrastructure" mode only.
- 3. Disable SSID broadcast.** The SSID is basically the network name for the radio access point. In open network mode, your router will invitingly broadcast its presence to the world 10 times a second. Turn it off to prevent neighbors and passersby from accidentally detecting and accessing your network. For home networks, just type the SSID in once during the setup dialog for it to be remembered for future sessions.

4. Turn on the MAC address filter. This is really for advanced users. Most gateways let you restrict access to known MAC addresses, which are unique to each machine (Windows PCs, Apples, and all other makes). By limiting access to pre-defined MAC addresses only, the network is further fortified against rogue clients.

However, as long as you're broadcasting, your wireless network can still be detected. Nearby hackers could capture the data packets as they zip through the air. These packets may reveal SSID and MAC addresses of trusted clients, allowing a hacker to "spoof" the address and pose as an accepted device. Therefore, additional steps to secure your system are necessary.

5. Enable WPA or WPA2 encryption. W-Fi Protected Access encrypts the information traveling between computer and gateway. *This is one of the most important things you can do to safeguard yourself.*

The Internet, designed in a more trusting age, had little thought given to protecting information in transit. The original Wi-Fi encryption scheme was known as WEP, which comes in different strengths. However, the underlying algorithm is fundamentally flawed. Hackers have developed software tools that can now crack even the most advanced form in a few minutes.

WEP is better than nothing, but users are *strongly* advised to use more advanced protocols. WPA builds on WEP encryption by scrambling the key and checking it to ensure it has not been tampered with. WPA2 is even stronger and provides better performance and is thus the currently preferred standard.

Note that both WPA and WPA2 require that *all* wireless devices on your network be set to them. You can't mix WEP and WPA devices. Upgrading from WEP may require newer adapter cards or a firmware update from the manufacturer. And of course, it's always a good idea to change your passkey regularly.

6. Use a firewall, up-to-date anti-virus protection, and regularly check or system updates online. Along with changing passwords, these are all fundamental means of protection that SWCP strongly recommends for ALL users, however you connect – be it broadband or good old dial-up. Many routers have a built-in firewall, as do recent operating systems like Windows XP. Be sure to activate it.

However, it is not a bad idea to install a **software firewall** on your computer for additional protection, especially if it's a laptop you will be connecting to other systems, like public hotspots. Like anti-virus programs, there are excellent free ones available as well as commercial versions online.



Continued on back

Continued from front

Whatever kind of firewall you use, it should be at the most restrictive setting that does not interfere with your activities.

7. Protect data with passwords. With newer operating systems including Windows XP, Vista, and Mac OS X, you can password-protect your entire computer or just selected folders or files. Use special protected directories that only you have access to for your most confidential and sensitive documents.

8. Turn off wireless access when not in use. Inconvenient perhaps, but simple and foolproof. Your computer can't be hacked when it's turned off or not connected. Also, turning off Wi-Fi will extend your laptop's battery runtime.

Public Protection

By their openness and lack of filtering or encryption, public Wi-Fi hotspots in coffee shops, airports, hotels, or wherever, pose special dangers. Lurking hackers can sniff passing network traffic, on the lookout for passwords, credit card numbers, and security vulnerabilities. And they can be difficult if not impossible to spot. Here are a few additional precautions you should take when using a public access hotspot.

1. Beware of "evil twin" hotspots. A truly clever, evil trick for hackers is to set up their own hotspot at the same location that mimics the legitimate access point. They will have an SSID as one would expect so it may be hard to tell them apart, like "STARBUCK2" near a Starbucks.

Evil twins are designed to collect passwords, usernames, even credit card data. This is a version of the classic **man-in-the-middle attack**, which can happen at home as well. Watch for secure sites popping up with a "Self Signed certificate." Unless you get that, you may actually be using a predatory provider. This is a good reason to avoid any temptation to use your neighbor's seemingly wide-open access also.

Do *not* set your wireless card to automatically connect to any available access point it detects, but first check the list of available SSIDs to make certain you are connecting to the right one.

2. Be sure that file-sharing is turned off. At home or work, file-sharing is often used to easily copy files back and forth between networked computers, but it's very dangerous to leave on in public. Use a sticky note if you need to remind yourself.

3. Use web-based email and secure sites. SWCP's free customer web-mail service protects data in transit more than regular email programs. Plus, the messages conveniently stay on our server where you can access them from any location – handy if you use several computers for email.

Email is otherwise transmitted unencrypted and can be sniffed by nearby lurkers. While email encryption sounds good, it's an option only for more advanced users. And to be useful, your correspondent must also be set up in order to read it. It's better simply not to send any really sensitive information ever by email.

Like our web-mail service, many websites, especially commercial ones, have security features. Their addresses begin **https:**, rather than just **http:**. Don't shop online anywhere else.

4. Be aware of the people around you. The range of Wi-Fi is quite limited, but the hacker does not have to sit next to you or even know who or where you are. Still, it pays to be aware of who's looking over your shoulder. Sit with your back to a wall if

possible. Special films can also be placed over your screen to narrow its range of visibility.

Other, even more technical steps can be taken to protect your data such as establishing a VPN, putting your wireless network on its own subnet, and changing internal IP numbers. For these you may need help from your company's IT guru, who should definitely be consulted anyway if you plan to use wireless to access the business' network.

For the steps listed above, however, our excellent Tech Support staff is here to help. Call or email if you have any questions or problems.

Free Net Class Repeats

SWCP offers 3 more sessions of our free "**Introduction to the Internet**" class, covering getting the most from your web browser, email, and other Internet basics. This class is intended for beginners, and focuses on Firefox and Thunderbird, two free Internet applications. It will also cover some basics on staying safe on the Internet, and offer helpful suggestions on how to get less spam.

- Monday, November 19, 2007, 6:00-8:00 pm
- Saturday, December 1, 2007, 9:00-11:00 am
- Thursday, January 24, 2008, 6:00-8:00 pm

Space is limited, so call us at (505) 232-7992 to register today! (Sorry, only open to current SWCP, Thuntek, or NMIA customers at this time.)

Call Us for DSL Speed Changes

Lately, for some reason, Qwest has been disconnecting users who directly request upgrading their DSL service from them. Call us instead. We'll monitor their response to make sure it's done right with no added charges.

Domain Squatters Investigation

ICANN, the Internet governing body, announced that it has launched an investigation into insiders pre-emptively registering desirable domain names, calling the practice "**domain name front running**." As we warned readers last issue, this sort of practice is becoming more widespread all the time. Standards will have to be set, but at the present time, it does not appear as if the practice is actually illegal.

Continue to take care when checking for domain name availability.

Net Notes

The Internet is running out of addresses! Each and every machine online requires a **unique IP address**, a set of four groups of numbers that tell exactly where it belongs. Addresses get reused constantly, but they'll all be taken by 2011. A system using two more sets of digits, expected to replace the current one, should solve the problem for a while.