Securing Your Home Wi-Fi

“How can any data sent into the open air be secure?”

by Pete Choppin

The term "wireless security" may seem a contradiction in terms. After all, how can any data sent into the open air be secure?

It seems like wireless networking is everywhere now. From my workplace to the fast food restaurants and cafés to my home, wireless networks are everywhere. Every time you log on to a public Wi-Fi access point, you are transmitting your login name and password over open airwaves, and often a credit card number as well. How much do we know about wireless security?

A friend of mine recently found out how easy it was to infiltrate a public Wi-Fi network. He was just at the local mall with his laptop looking for a wireless network to jump onto. When he found one, it was of course not secured because it was public. However, he was able to gain access to their wireless network through the router because it was completely open. From there, he had full access to their entire network. Fortunately for the mall, my friend had no malicious intent, but it illustrates how easy it is for Wi-Fi access points and internal networks to be vulnerable—and how security is so lax.

What about home networks? While individual home networks may not be quite as attractive to wireless hackers, do you really want your neighbor stealing your bandwidth, or passersby snooping around your hard disk? Even if you aren't worried about your home network, and don't keep any valuable data on your hard drive, you should still be concerned about bandwidth hijackers.

In perhaps the most shocking Wi-Fi crime to date, a man using a laptop in a moving car was found by Toronto police downloading child pornography thanks to open Wi-Fi nets in a residential neighborhood. Police only stopped him because he was going the wrong way down a one-way street. Worse, if such downloads are traced back to your IP address, you could be charged with a crime yourself. All hackers need is readily downloadable "sniffing" tools, such as those used by "wardrivers." (Hackers who wander the streets with Wi-Fi gear looking for networks to join—most are hobbyists or simple bandwidth seekers, but some are malicious.)

So what can you do to make your wireless net safer? Thankfully, the answer is "a lot." While no network is 100 percent secure, you can make your wireless net just as safe as a wired one, and prevent all but the most dedicated and resourceful crackers from getting in. And it won't cost you anything but a little time.

Here are some down-and-dirty tips to help you keep your private data private.

1. Make sure you are connected to a legitimate access point. This first step is often overlooked, but may be one of the most important. Rogue access points in public areas can have the same SSID (the wireless network ID) as what you'd expect in the area, but really connect directly to hijackers' databases to collect the passwords and usernames you use to sign in. Even worse, they can collect credit card data from people who sign up for new accounts.

2. Encrypt Sensitive Data. As you send e-mails from your laptop to the wireless access point and back, or as you enter your username and password to check your bank account balances, someone nearby can be "sniffing" (intercepting) those packets of data as they fly by. Much of the information—even information that you think should be encrypted—is sent in clear text. That means that the person intercepting those packets may be able to read your e-mails or learn your passwords.

While data sent to and from secure Web sites (those starting with https:) is generally protected, you can also use encryption in other contexts. If you are sending a sensitive file via e-mail, for example, encrypt it first with a password. A very nice encryption program called JavaEncryptor works very well, is easy to use, and it is free. Also, because it is written in Java, it is cross platform (will work with any system).

Security Tips for
Public Wi-Fi Hotspots

1. Make sure you're connected to a legitimate access point.
2. Encrypt files before transferring or emailing them.
3. Use a personal firewall
4. Use anti-virus software.
5. Update your operating system.
6. Be aware of people around you.
7. Use web-based email that employs secure http (https)
8. Password protect your computer and important files

3. Use a personal firewall. A personal firewall will help you restrict the traffic allowed in and out of your computer. This protects you not only from attacks that originate outside of your network, but also those from other computers on the same network. Make sure you take the time to familiarize yourself with the product you choose and configure it properly to get the maximum protection without getting in the way of legitimate traffic and applications.

4. Use antivirus software. When you are on your home network or even on your company network you can operate with a fair assurance that the other machines on the network with you are at least as protected as yours is against viruses and other malicious code. When you connect to a public network you have no such assurance. Suddenly it is more important than ever to have antivirus software installed.

5. Keep your OS and apps up-to-date. It seems that almost every week there's a new "security patch" for various parts of the Windows operating system or Office programs. And it's not just Microsoft. Apple has its own fair share of security updates, as do most utility and business software vendors. Also, most of the malicious viruses and worms that have plagued users recently spread through e-mail, so be especially cautious about opening attachments.

6. Be aware of people around you. When you're at an ATM, you make sure no one can see you type your PIN. Be just as careful about typing in your name and password at a Starbucks. You pay big bucks for that mobile access account. Don't just give away your password.

7. Use Web-based e-mail accounts. Why? Most ISPs these days have a Web-based e-mail system you can use. These Web sites generally use secure sockets layer (SSL) or other security protocols, which protect your data while it's being transmitted. POP mail through Outlook does not.

8. Use strong passwords for personal data. Use strong passwords for sensitive files and folders, as well as for access to your computer as a whole. This is especially important for mobile warriors whose laptops are attractive theft targets. Consider keeping your most important data on an encrypted USB keychain storage device, so even if you lose your

portable device, you won't lose your presentation or e-mail folder.

No network can ever be completely secure, but after you've implemented the recommendations here, wireless hackers will likely choose an easier target.

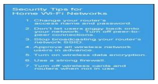
Just as important is securing your home wireless network (and the wired one too!). Here's a step-by-step guide to help make the process as painless as possible.

1. Change your router's name and password. This is always the first line of defense. It's easy for attackers to find out what the default name and password are for various manufacturers. You should make sure you rename the router and assign a strong password for accessing the router configuration software.

2. Enable infrastructure mode only on all access points and clients on the network. Disable the "ad-hoc" mode, which lets clients set up peer-to-peer networks and could allow rogue users to connect to your network through a legitimate wireless client.

3. Disable SSID broadcast. The SSID (Service Set Identifier) is essentially the network name for the wireless portion. With broadcasting off, wireless clients must first know the SSID before they can connect. Experienced hackers can still find such "closed" networks, but at least you will not be openly inviting them. Neighbors or passersby will not see or accidentally connect to your network.

4. Turn on the MAC addressing filter in your wireless router. Each network device (such as a computer, Wi-Fi card, or printer) has a unique MAC (Media Access Control) address, and by allowing access only to pre-defined MAC addresses, you reduce the risk of accidental or rogue clients connecting with or perusing your network resources. This takes the closed network concept a step further.



Security Tips for
Home Wi-Fi Networks

1. Change your router's access name and password.
2. Don't let users piggy back onto your network. Turn off peer-to-peer connections.
3. Stop broadcasting your router's network SSID.
4. Approve all wireless network users in advance.
5. Turn on wireless data encryption.
6. Use a strong firewall.
7. Turn off wireless cards and routers when not in use.

5. Enable WPA (Wi-Fi Protected Access) or WPA2 encryption. Encryption is the next step in the wireless security ladder. You might see an encryption setting on your router called WEP (wireless equivalency protocol); however, its underlying algorithm is flawed and subject to relatively easy cracking. Without going into the gory technical details, it can be broken in minutes. While WEP is better than nothing, it will only keep out the neighbors and opportunistic hackers. For true protection, you need WPA or WPA2.

6. Use a strong firewall. The steps we've discussed so far focus on securing the wireless network, but once your wireless data reaches the access point, it becomes part of the wired net, and subject to any attacks or snooping that might come in through your broadband gateway (or from other users on your local wired net). Furthermore, WEP, WPA and WPA2 encryption apply only to data in the air; as soon as it passes through the Wi-Fi gateway, data is decrypted. Most home networking routers come with built-in firewall capabilities. The firewall is usually a basic port-blocking or packet-filtering firewall that lets you permit or deny incoming traffic on certain ports. (See last week's issue of ComputorEdge for more details on firewalls).

7. Turn off wireless devices when not in use. The final word of advice for home wireless networks is "Turn it off!" While it may seem like a pain, you'll sleep easier knowing that since your gateway, computer, laptop etc. are not turned on, no one can access them. A computer that isn't connected can't be hacked or compromised from the network.

We live in a wireless world today, and although the technology has become more advanced, it is still vulnerable. If you think about it, you are merely sending your personal or sensitive information over a radio signal—not all that different than broadcasting a station from a radio on your desk, and all one needs to receive that signal is a wireless adapter.

It's your data. Keep it safe and secure.

Resources:

What is wardriving and how can you prevent it.

WPA PSK Encryption Step-by-Step Tutorial