Cutting the Cord: The New World of Wi-Fi

IT IS NOT UNUSUAL for some of us to get as many as 500 e-mail messages each in a single day. Granted, we can dispose of many because they are just spam or are messages from listservs that don't require a response. But many of the messages require an answer, and clients expect us to answer quickly. Having a high-speed Internet connection is an absolute necessity if we are going to keep the clients happy and tame the e-mail beast. That's a somewhat manageable task for us in the comfortable work environments we've created at our homes and at our office using cable and T-1 Internet connections.

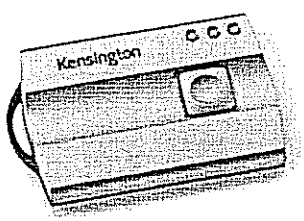
It used to be the case that traveling would seriously set us back in dealing with e-mail and keeping up with sites like AILA InfoNet. When we're on the road, we have less time to deal with e-mail than usual, assuming we can even find a place to actually download mail. So the proliferation of Wi-Fi—high speed wireless Internet access—is a most welcome development. Now it is possible to get online and get a lot of work done—whether we're in an airport, hotel, coffee shop, or even a McDonald's restaurant. Wi-Fi networks have sprung up nearly everywhere, and with an investment of around $50 in a wireless network card for our laptop computers and a subscription to a Wi-Fi service provider, we've become much more productive road warriors.

What is Wi-Fi?

A Wi-Fi network is a wireless network that typically uses radio waves to establish communication between computers and other network devices. Think cordless phones as an analogy. A Wi-Fi network allows basically the same functionality as a wired network, and you can share files, log on to the Internet, as well as print to a remote printer without having to be physically connected to a network.

How Do You Find a Wi-Fi Hotspot?

You probably move through Wi-Fi "hotspots" throughout the day and don't even know it. Think of "hotspots" as Wi-Fi clouds where people with wireless access can log on to the Internet. One research report estimates that over the next three years, the number of hotspots in the United States will grow to 530,000.



Kensington Wi-Fi Finder

How do you find these hotspots? And once you find them, how do you access them? From a technical standpoint, you can detect whether you are in a hotspot simply by turning on your computer and checking your wireless card to see if it detects a connection. We recently purchased a handy little device for about $25. It is about the size of a credit card and can be attached to a keychain hanging from a laptop case. The Kensington Wi-fi Finder (*www.kensington.com/html/3720.html*) lights up when it "sniffs" a hotspot, and you don't even need to boot up your computer.

You also can go on the Web before you leave town to find out where hotspots are located. There are numerous directory listings of free and fee-paid hotspots. Unfortunately, there is no comprehensive list of all the sites, so you'll probably want to check a couple of locations. We ran a basic test using five Web sites in order to offer a quick comparison. Below, in parentheses, is the number of locations found in our home state of Tennessee. Some of the sites will tell you which company offers the service and if the hotspot is free or subscriber-based. Others will only tell you a location.

- *www.wi-fihotspotlist.com* (105)
- *www.hotspot-locations.com* (24)
- *www.wifi411.com* (60)
- *www.wifinder.com* (32)
- *www.wi-fizone.org/zoneFinder.asp* (43)

You also can subscribe to a national service provider and search for locations on its Web site (see more on subscriber services below). The best places to find free hotspots are hotels (particularly hotel lobbies) and cafés (other than those that participate in the national subscriber services, like Starbucks and Borders). But most airports that offer wireless service do so for a fee.

What About a Subscription Service?

While there are thousands of free hotspots around the United States, we subscribe to a pay service mainly because we don't want to spend the time searching for places to log on or to have to travel far out of our way. The service we selected is through T-Mobile. They have wired up thousands of Starbucks, Kinko's, and Borders stores around the country. There seems to be one of these establishments just around the corner from wherever we are. They also have decent coverage in Europe. We pay about $20 a month

Most of the Wi-Fi access points are deliberately left unsecure in order to facilitate easy access. So keep in mind that if you have enabled file sharing, your files and folders could be at risk.

for the service and find the price to be well worthwhile.[2]

There are several other services to consider:

■ Wayport (*www.wayport.com*) is T-Mobile's big competitor. You can find Wayport in a dozen airports, hundreds of hotels, and 75 McDonald's restaurants in New York City and San Francisco.[3] Wayport's rates are about the same as T-Mobile.

■ Verizon (*www.verizonwireless.com*) has found a creative use for 1000+ idle telephone booths in New York City by converting them to wireless access points and offering free wireless service to the company's DSL customers.

■ Other services to consider are Boingo (*www.boingo.com*), AT&T, and MCI. We have chosen to subscribe to one service that generally meets our needs, but we will pay by the hour for another service in a pinch. Roaming is slowly becoming available and will, hopefully, be more common in the future. Right now, AT&T, Boingo, GRIC, iPass, and Wayport have roaming agreements. Wayport also has roaming relationships with some major overseas companies.

What About Security?

Most of the Wi-Fi access points are deliberately left unsecure in order to facilitate easy access. So keep in mind that if you have enabled file sharing, your files and folders could be at risk. The solution to this is to simply turn off this feature or just keep it off while you are on the road.[4] You can use personal firewalls and encryption technologies such as virtual private networks. Finally, some services, like Boingo, use proprietary software that includes security features.

■ Access via Air, Rail, and Sea

Starting this year, airplanes, trains, and cruise ships began deploying wireless networks using a satellite-based Internet connection. Do not expect to see wireless Internet on domestic flights this year, but within the next few years, this might become more common. Right now, British Airways, Japan Airlines, Singapore Airlines, Lufthansa, and SAS offer hotspots in the sky. In Europe, commuter trains are adding Wi-Fi, which is obviously helpful for people who want to work on their daily trips to and from work. And if you have ever paid the outrageous Internet access fees on a cruise ship, Norwegian Cruise Line's $10 per day Wi-Fi rates will sound pretty reasonable (Carnival and Holland America offer similar services, by the way).

■ PDAs and Cell Phones

Wi-Fi works on many Palms, Pocket PCs, and cell phones. Some of these units have Wi-Fi capabilities built in, while others require an SD or CF card (think of these cards as floppy disks for handheld computers). Expect cell phones that can use a Wi-Fi network as a backbone (instead of, or in addition to, normal phone networks) to become available soon. This means that you can make phone calls using the Internet rather than using up your minutes. But if you walk out of a hotspot, your coverage will drop off completely. One day, roaming and continuous hotspot coverage could make this technology compete with the traditional mobile phone networks we use today.

■ Wi-Fi at the Office

Once we figured out how useful it is to use Wi-Fi networks out of the office, we decided to do something not many firms have done. We set up a wireless network in our law office.

Why? First, as indicated above, a wireless network avoids the necessity of running cables in your office or home in order to establish a network. This is particularly useful when you want to add workstations or when you need a workstation in a location where wires cannot be run. Additionally, computers on a wireless network are mobile. Staff can easily relocate with their workstations without having to reconnect them.

The mobility also applies to clients or others who may need Internet access at your office. You can configure your wireless network such that clients who are at your office can access the Internet via the wireless network. It is a popular service we provide to our clients.

Setting up a wireless network is easier than you might think and can be accomplished in a very short period of time. You need, at the minimum, a wireless router or access point and a wireless adapter for your workstation. Adapters come in many formats: PCI cards that you can install in PCs, PCMIA cards for laptops, and USB adapters for any device. Go to your local computer superstore and you'll smile when you find just how cheap the equipment is. You can set up a basic wireless network easily for less than a $200 investment. And you can add computers for about $50 each.

All of these devices are available in multiple wireless formats. The most prevalent ones are 802.11b and 802.11g. The most popular standard is 802.11b and carries bandwidth up to 11 Mbps, about the same as an Ethernet router, hub, or card. The 802.11g format carries bandwidth up to 54 Mbps, and is backwards compatible with 802.11b. That means if you get an 802.11g standard, people with both 802.11b and 802.11g can get on to the network. That's a good thing.

While the 802.11g supports substantially faster file transfer, they both exceed the speed of most Internet services, so there is no big advantage to 802.11g. Both use the 2.4 GHz frequency, which also is used by devises such as cordless phones. So if you use cordless phones, interference could be a problem (the analogy to a cordless phone is actually pretty close!)

To set up your wireless network, first, you will need to add a wireless router →

or access point to your network. A wireless router essentially pulls data from your wired network and then transmits it to your hotspot. The router will provide your wireless signal, manage IP addresses for connectivity, and filter traffic. An access point, on the other hand, only manages wireless signals and can be hooked anywhere into the network. Access points are useful for adding wireless stations to an existing wired network and for extending the range of a wireless network. They also can be used to help get around signal barriers, such as walls and floors. Multiple access points can be used in configuring your wireless network.

Next, you simply need to install the wireless adapters into your workstations, and, voilá! You will have a fully functional wireless network.

■ Addressing Security Issues

Of course, while your network can be setup easily, ignoring security can open your network up to evildoers of all sorts. When you have a wireless network broadcasting, anyone within range can access it. On a recent trip, column author David Jones stayed in a hotel that did not have high-speed Internet access in the rooms. Nevertheless, he was able to get on the Internet thanks to an office building across from his window. He also is able to get to the Internet through three of his neighbors at home (though he would NEVER, NEVER freeload! (Apparently, this is quite the sport in apartment buildings around the country).

In such situations, a hacker may be able to gain access to the associated network just as easily as if he or she were sitting in your office. Under these circumstances, standard security systems may not be adequate. Fortunately, there are a few ways to tighten up your wireless network:

☛ You can simply configure your system so that it does not broadcast that it exists. Since you know what your wireless network is named, broadcasting is not necessary. Similarly, it is a good idea to change your identification and default passwords since hackers are likely to have this information when looking for networks.

☛ Two additional layers of protection are firewalls and encryption. Most wireless routers will include rudimentary firewalls, so it is a good idea to use them to restrict access. Wireless devices also come equipped with encryption capability, such that only authorized persons are able to read it. Wireless devices will have either WEP (Wired Equivalent Privacy) or WPA (Wi-Fi Protected Access) capability.

Whether you use Wi-Fi networks on the road or in your home or office, cutting the cord is worth it. In a few years, everyone will be doing it. But, for right now, the cost is so low and technology is so good that Wi-Fi is definitely worth a look.

Greg Siskind is the author of the ABA's book, *The Lawyer's Guide to Marketing on the Internet*, and a partner in the immigration law firm of Siskind, Susser, Haas & Devine. **David Jones** is a partner in the firm's Memphis office and its resident technology guru.

Notes

[1] Wi-Fi is short for "wireless fidelity." Wi-Fi is a trademark of the Wi-Fi Alliance (formerly the Wireless Ethernet Compatibility Alliance), the trade organization that tests and certifies equipment compliance with the 802.11x standards.

[2] By the way, for a few hours a week, column author Greg Siskind disappears from the office and goes to Borders bookstore around the corner where he can get work done without disruptions from the telephone, co-workers, and family. You would be surprised just how much you can get done hibernating online away from home and office.

[3] You can get free Wi-Fi access for 30 minutes at McDonald's by purchasing one of its value meals.

[4] Go to the Start menu and select the Control Panel; In the Control Panel window, double-click on Network Connections; Right-click on the Local Area Connection icon in the window that appears; From the menu that appears, choose Properties (use the left mouse button to make your selection); Under "*This connection uses the following items*", highlight File and Printer Sharing for Microsoft Networks. *Note: If* File and Printer Sharing for Microsoft Networks *is not listed, then file sharing was not set up on your computer. You may close any open windows and skip the rest of these instructions*; Click Uninstall; When you are asked if you are sure you want to uninstall File and Printer Sharing for Microsoft Networks, click Yes; Click OK or Close to close the Local Area Connection Properties window; If you are asked to restart your computer, click Yes. If you are not asked to restart your computer, from the Start menu, choose Turn Off Computer. In the Turn off Computer window, click the Restart button to restart your computer.