Be Wary About Wi-Fi

With a certain amount of relish, a rep recounted how both he and his wife were able to keep up with work this summer while on vacation in Florida. Through a combination of cell phone use and availability of wireless Internet connections, they kept on top of impending appointments and cleared and responded to e-mail correspondence. In the area of wireless Internet use, however, he discovered he may have been following an unwise path.

According to the rep, he discovered that a hotel near the location he was staying had wireless available. Armed with their laptop, each evening he and his wife would walk down to the hotel, sit around the pool and get some work done. While everything worked out well for the couple, if they had read some recent articles that appeared in business publications they might not have been so willing or anxious to jump on someone else's wireless signal.

Earlier this year in St. Petersburg, Florida, a man was charged by authorities with a third-degree felony after he was arrested for accessing a neighbor's wireless Internet network without permission. The man was charged after his neighbor spotted him outside in his car using a laptop computer. Later that evening the neighbor spotted foreign icons on his home computer screen and suspected that the man in the car was responsible. Ultimately the wi-fi (short for wireless fidelity) pirate was charged with the unauthorized access to a computer network, which applies to all varieties of computer network breaches and allows prosecutors considerable leeway depending upon the severity of the crime. In Florida, the offense carries a potential sentence ranging from probation to five years in prison.

Determining Motive

According to an article that appeared on the Internet at www.cnnmoney.com, the state attorney general's office said, "The sentence we'll seek depends on whether he was accessing the Internet for basic personal use, or using it for pecuniary gain — like identity theft — or other illicit reasons. The man's laptop was confiscated at the time of his apprehension and was to be analyzed by the Florida Department of Law Enforcement."

The question of the legality of using someone else's wireless signal was discussed in a subsequent article on the same web site. Among the comments reported on the subject were:

- "All of this stuff is so new, it's hard to say what the liability issues are."
- "It seems pretty clear that if you 'hack' your neighbor's password then it could be reasonably argued you didn't have authorization."
- "A broad statement concerning the access of unprotected wireless networks as being always legal or illegal simply can't be made. It's just kind of dicey."

Practical Wi-Fi Concerns

Notwithstanding the potential legal considerations, there are some more practical concerns that would-be wi-fi pirates had better be aware of.

"If you have wi-fi and know how to use it, it's a great technology," maintains David A. Milman, founder and CEO of RESCUECOM, a Syracuse, New York-based franchisor in the computer services industry. The company delivers business and sales resources from computer technicians and consultants on a one-hour on-site response basis. "Wi-fi provides computer users the same type of flexibility and efficiency

that cell phone users enjoy. However, there are some concerns that small businesses, such as the typical rep firm, ought to be wary of." Two of those concerns he mentioned are the:

• Typical small rep firm office that has been set up with wi-fi — "With this scenario, you have to be concerned with who will be able to get into your system. Most people who establish wireless networks don't necessarily have someone qualified/certified to do the job for them. As a result, they can be missing some important considerations. Too often your network is open to all. You may wind up with several people getting free Internet service on your signal. With reps in particular this can be dangerous, because people in the office share files with information concerning products, pricing and customer lists. Everything they do is potentially at risk. There's also the danger of spam and adware finding a way on to your system.

• Dangers of searching for and ultimately using other's wi-fi signals on the road — "There are secure ways to use wi-fi on the road. Verizon, for instance, provides a secure broadband connection. Also, most hotels, airports and many coffee shops provide secure signals. Keep in mind, however, that searching for and using others' wi-fi signals can be illegal. If someone catches you doing it, it could be a major problem. I wouldn't do it myself.

"Remember when you take your laptop out on the road, your information is open to the world. Be sure the individual field shares, security settings and login are all set up properly. If you just jump on and your computer is open to the world, people near you can get on to your computer."

He adds that another important consideration is that laptops be properly protected against spam, adware and various viruses.

As a final word of warning, Milman notes that independent manufacturers' representatives are individual businessmen who are very pleased and proud of their accomplishments. "Many times they'll want to complete various technical jobs (i.e., setting up wi-fi) themselves. Sure, that approach can work with a small network, but if they're implementing something more sophisticated, chances are they're going to need some help. They could be opening up their files for the world to see."

For more information on RESCUECOM, visit the company's web site at www.rescuecom.com. ❐