

6 wireless threats to your business

If you think a promiscuous client is a scantily-dressed customer, you're in trouble. And I'm not talking about having an affair.

Think an evil twin is a horror-movie villain? Wrong again. The horror you should be bracing yourself for is not on the silver screen — and it's not from a rolling pin flung at you from across the kitchen, for that matter. Rather, the trouble is in the airwaves and targeted to Wi-Fi users.

Both the "Promiscuous Client" and the "Evil Twin" are two of the latest wireless threats to your small business. If you haven't heard of them, you probably will soon.

"What would happen to your business if your strongest competitor gained access to all of your data?" asks Greg Phillips, chief executive for AirTegrity Wireless, Inc., a Stateline, Nev. wireless security company. "Unfortunately, it is a very real possibility if appropriate controls against these new threats are not exercised."

So what's out there?

- **The Evil Twin.** One of the most popular new threats to Wi-Fi users is the Evil Twin, sometimes referred to as WiPhishing. It's a rogue access point that replicates another network name, such as that of a hot-spot or a secure network. "The Evil Twin waits for a user to mistakenly sign into the wrong access point and captures the user's network data or attacks the computer," says Mike Klein, chief executive of Interlink Networks, Inc, an Ann Arbor, Mich. Wi-Fi security firm for small businesses. Klein recommends using an application like the free LucidLink Wireless Client (www.lucidlink.com), which automatically detects the change of security settings and warns the user to prevent an Evil Twin attack. He says it's also best to stay away from any open, or unsecured, wireless networks.
- **The New War Drivers.** Basically, War Driving is an unauthorized person hacking your company's wireless network. That's a problem if your network is open or not adequately secured. (Is yours? This is probably a good time to check.) "The War Driving threat only affects businesses with unsecured wireless networks," explains Nicholas Miller, chief executive of Cirond Corporation, a Campbell, Calif., wireless security company. "It can affect the security of confidential business data that resides on users laptops." So what's new about this threat? War Driving used to be an obscure pastime for hackers, who would cruise around in their compact cars looking for open networks. But lately, the new war drivers can also be competitors or disgruntled employees, sitting in the parking lot and trying to penetrate your network.
- **The Promiscuous Client.** A close cousin to the Evil Twin, Promiscuous Clients are opportunistic hazards to your business. Instead of associating with an access point that is placed near a public hotspot intentionally, and for malicious purposes, the promiscuous client is simply there for one reason or another, offering an irresistibly strong signal. "802.11 wireless cards often look for a stronger signal to connect to as well as look to hook up with a common SSID name," says Michael Maggio, the president of Newbury Networks, Inc., a Boston IT security firm. (I actually encountered a Promiscuous Client on a recent trip — one offering a terrific signal and speed. Fortunately, my laptop and I

both survived the meeting.) Maggio suggests using a wireless "sniffer" (Microsoft Windows XP has one) that can help you monitor and test your network airspace. "The more you know about your layout — inside your offices, across the hallway, on the floors above and below you, as well as outside your bricks and mortar (business) — the better idea you'll have about where security breaches might occur," he says.

- **Bluesnarfing and Bluejacking.** Your Bluetooth-enabled wireless device can leave you open to a hack attack, too. For example, Bluejacking allows unauthorized users to send a message to your phone. Bluesnarfers can steal data from your phone. But that's only part of the problem. Perhaps the more troubling issue is that these crimes are often untraceable. "The newest threat is the inability to perform forensics on this new technology," says Mark Lobel, director of PricewaterhouseCoopers' security services group. "You can try to stop an employee from doing bad things, but with some of the newest wireless technologies, you can not yet perform the forensics to determine what actually happened." These attacks can really leave you with the "blues," many experts say, so heed this advice: Turn off Bluetooth until you need it.
- **The cell phone virus.** In a recent column, I took a closer look at the growing threat of cell phone infections. Several of the experts I interviewed suggested the worries might be overblown. But in the weeks since the column appeared, says Ted Demopoulos, an IT consultant with Demopoulos Associates, in Durham N.H., a number of new cell phone viruses were identified. "Experts disagree on how serious the cell phone threats are," he says. "But it is wise to take some simple steps to protect against threats." Demopoulos says most small businesses ignore the data on their cell phones. By backing up the numbers, you can assure that they won't be lost if your phone ever succumbs to a virus outbreak.
- **Wireless network viruses.** There are viruses, and then there are wireless viruses. For example, the virus worm MVW-WiFi, which bores into a laptop through a wireless network, sends out wireless probe request packets to find other local wireless networks and then forwards itself to adjacent wireless networks, according to David Sandel, the chief technology officer for NetLabs, LLC, a St. Louis networking company. "Its destructive capabilities are exponential in nature." His advice? Run antivirus software — and keep it updated.

Whether you're using a Bluetooth-enabled Personal Digital Assistant, a cell phone or a laptop, you can steer clear of most trouble by double-checking your security settings. That goes for your small business wireless network, too. Nearly two-thirds of all wireless users are on an unsecured network, according to several surveys. "That's pretty scary," says Scot Zarkewicz, chief executive of SingleClick Systems, a Toms River, N.J., networking company for small businesses. "If there is one point that small businesses should know about wireless networking, it is that encryption is their best form of protection."

But the biggest wireless security threat, by far, isn't a virus or hacker attack. It is complacency, says Gary Morse, president of Razorpoint Security Technologies, Inc., a New York company that describes itself as "professional hackers." "We hear all the time, 'We're not a target,' or, 'We only need to secure the 'important machines,'" he says. "Awareness is the most critical point of fortification. If users are simply aware of what could take place, of what the true risks are, then everything else could be built on that."