

On the Defensive

Protecting your wireless system from Internet interlopers BY KAREN J. BANNAN

Robert Siciliano is a security expert. He is the president of IDTheftSecurity.com and the author of *The Safety Minute: 01*. But even his vast expertise could not keep his network—or

his PC—safe. Several years ago, Siciliano, who has a PC connected to a wireless network, noticed that his high-speed connection was now agonizingly slow. He checked his computer for viruses and spyware, and found neither. He did not worry because his PC was behind a protective firewall, hardware that makes it difficult for hackers to break in. He assumed the slowdown was due to a bad Internet connection, until one day a “computer geek” buddy came over.

“My friend started doing some tests and he told me, ‘You’re broadcasting your wireless connection to everyone.’ He quickly found out that my neighbor was on my network,” says Siciliano. “He had access to my personal files. He was basically stealing my wireless connection, using it 24-7 to download pirated movies and music.”

Siciliano’s experience is not unique. A recent study by the

San Francisco-based Computer Security Institute found that 15 percent of users experienced abuse of wireless networks in 2004. Robert Stephens, founder and chief inspector of Geek Squad, a mobile computer support firm, says the reason is obvious: Wireless equipment is so accessible and easy to set up, consumers are doing it themselves. This means that security provisions, which are built into wireless equipment, are not turned on.

“Wireless gear out of the box isn’t encrypted automatically. To make it work properly, you have to create a password and make sure you put it in every time you log into your wireless network,” he says. “If you don’t, anyone walking around outside your home with a laptop and a wireless card can pick up that signal and get into your PC.”

The practice is so common that there are numerous web sites dedicated to wireless network maps. These sites (such as Worldwidewardrive.com) list the locations of unprotected wireless networks. Visitors simply enter their ZIP codes and receive directions to local unsecured Internet access points.

Fortunately, this problem has several easy fixes. If your wireless connection has a short range and you live far enough away from others, you may not have to make any adjustments. After all, if no one can get to you, there is no need to panic.

You can test your signal by walking around with your laptop. “Most wireless gear has a range of 50 to 75 yards,” says Stephens. “Walk the laptop onto the street. If you can’t get a signal, chances are no one will be able to hack their way into your connection.”

If you are still worried—you live close to others in a condominium or a gated community, or travel often with your PC—defensive measures may be required. Mike Klein, president and CEO of Interlink Networks, an Ann Arbor, Mich., security software developer, recommends hiring an expert. “There are hardware and software solutions out there,” he says. “You can select what you need based on what you do with your PC. If you’re connecting back to your corporate network or keeping confidential data on your PC, you’ll want enterprise-level protection.”

Either way, the \$150 or so you spend will be well worth it, says Steve Fallin, rapid response team director for firewall provider WatchGuard Technologies. “It really boils down to the net effect,” he says. “Do you really want to take the chance on something as important as security?”



Geek Squad, 800.433.5778, www.geeksquad.com

Interlink Networks, 734.821.1200, www.interlinknetworks.com

WatchGuard Technologies, 206.521.8340, www.watchguard.com