can get within range of your network's radio signals. At home, your neighbors can probably see your wireless network. And in an office, kids sitting on a bench outside your building can probably see your wireless network.

- **Freeloaders:** *Freeloaders* are intruders who want to piggyback on your wireless network to get free access to the Internet. If they manage to gain access to your wireless network, they probably won't do anything malicious: They'll just fire up their web browsers and surf the web. These are folks who are too cheap to spend $40 per month on their own broadband connection at home, so they'd rather drive into your parking lot and steal yours.

  Even though freeloaders may be relatively benign, they can be a potential source of trouble. They suck up your bandwidth. They may use your network to download illegal pornography, or they may try to hijack your email server to send spam. And they may start out innocently looking for free Internet access, but their curiosity may grow once they get in, leading them to snoop around your network.

- **Eavesdroppers:** *Eavesdroppers* just like to listen to your network traffic. They don't actually try to gain access via your wireless network — at least, not at first. They just listen. They spy on the packets that you're sending over the wireless network, hoping to find useful information such as passwords or credit card numbers.

- **Spoilers:** A *spoiler* is a hacker who gets his kicks from jamming networks so that they become unusable. A spoiler usually accomplishes this act by flooding the network with meaningless traffic so that legitimate traffic gets lost in the flow. Spoilers may also try to place viruses or worm programs on your network via an unsecured wireless connection.

ROGUE ACCESS POINTS

One of the biggest problems that business networks face is the problem of *rogue access points,* which are access points that suddenly appears on your network out of nowhere. What usually happens is that an employee wants to connect his iPad or smartphone to your company network, but you won't give him the password. So the user stops at Walmart on the way home from work one day, buys a cheap wireless router, and plugs it into your network without asking permission.

Now, in spite of all the elaborate security precautions you've taken to fence in your network, this well-meaning user has opened the barn door. It's *very* unlikely that the user will enable the security features of the wireless access point; in fact, he probably isn't even aware that wireless access devices *have* security features.