WARNING

Beware: Never connect a networked computer to the Internet without first considering the security issues:

- How will you protect yourself and the network from viruses?
- How will you ensure that the sensitive files located on your file server don't suddenly become accessible to the entire world?
- How can you prevent evil hackers from sneaking into your network, stealing your customer file, and selling your customer's credit card data on the black market?

TIP

For answers to these and other Internet-security questions, see the chapters in Part 5.

Plugging in a Wireless Access Point without Asking

For that matter, plugging any device into your network without first getting permission from the network administrator is a big no-no. But wireless access points (WAPs) are particularly insidious. Many users fall for the marketing line that wireless networking is as easy as plugging in one of these devices to the network. Then, your wireless notebook PC or handheld device can instantly join the network.

The trouble is, so can anyone else within about one-quarter mile of the WAP. Therefore, you must employ extra security measures to make sure hackers can't get into your network via a wireless computer located in the parking lot or across the street.

If you think that's unlikely, think again. Several underground websites on the Internet actually display maps of unsecured wireless networks in major cities. For more information about securing a wireless network, see Chapter 8.

Thinking You Can't Work Just Because the Network Is Down

A few years back, I realized that I can't do my job without electricity. Should a power failure occur and I find myself without electricity, I can't even light a candle and work with pencil and paper because the only pencil sharpener I have is electric.