IN THIS CHAPTER

- Understanding what firewalls do
- Examining the different types of firewalls
- Using the built-in Windows firewall
- Looking at virus protection
- Patching your computers

Chapter 20 Hardening Your Network

If your network is connected to the Internet, a whole host of security issues bubble to the surface. You probably connected your network to the Internet so that your network's users could get out to the Internet. Unfortunately, however, your Internet connection is a two-way street. Not only does it enable your network's users to step outside the bounds of your network to access the Internet, but it also enables others to step in and access your network.

And step in they will. The world is filled with hackers who are looking for networks like yours to break into. They may do it just for the fun of it, or they may do it to steal your customer's credit card numbers or to coerce your mail server into sending thousands of spam messages on their behalf. Whatever their motive, rest assured that your network will be broken into if you leave it unprotected.

This chapter presents an overview of three basic techniques for securing your network's Internet connection: controlling access via a firewall, detecting viruses with antivirus software, and fixing security flaws with software patches.

Firewalls

A *firewall* is a security-conscious router that sits between the Internet and your network with a single-minded task: preventing *them* from getting to *you.* The firewall acts as a security guard between the Internet and your local area network (LAN).