

Chapter 1

Preparing Your Online Security Blanket

In This Chapter

- ▶ Uncovering how Norton components work
 - ▶ Understanding who hackers are and what they want
 - ▶ Recognizing common attacks at home and work
 - ▶ Preparing your computer for security applications
 - ▶ Setting up good privacy strategies
-

The term *security* isn't one that leaps to mind when you think about the Internet. You don't connect to the Internet to be secure, after all. You connect in order to learn, to explore, to be entertained. The first thing you think about when you go online is getting your e-mail or visiting a Web site. Chances are you *only* think about security when something goes wrong — or when you are made aware of one of the many threats to your privacy and security that you face from the Internet. You may have purchased this book because your computer has been infected with a virus, or because someone has mentioned that, along with your fast new cable modem or Digital Subscriber Line (DSL), you need to have something called a “firewall” or something called “anti-virus software.”

No matter what your level of experience with viruses, hackers, and spyware, this book will help you defend yourself against them with the help of a powerful and user-friendly suite of software programs called Norton Internet Security (NIS). This chapter gives you an overview of the program and how to take advantage of its many features. You also find out how to prepare your computer by making use of the resources on the Symantec.com Web site.



To find out more about Norton Internet Security or Norton Internet Security Professional, go to the Symantec Products and Services page (www.symantec.com/product) and select the product you're interested in from the drop-down list near the top of the page. You'll go to a page with more specific details about the package you chose and links to a trial version you can download or a version you can purchase online.

Making the Case for Norton Internet Security

Think about how it easy it is to connect to the Internet through your home network. Whether that network consists of a single computer or two or more machines, after you do the initial setup you have no problem downloading software, reading your e-mail, or even listening to Internet radio. The problem is that it's just as easy for technically adept individuals who like to break into remote systems — hackers — to connect to your computer, too, unless you install software like Norton Internet Security, or other security hardware or software.

Norton Internet Security is a suite of software programs, each of which provides a different kind of protection. It's especially designed for home and small business users who need to access the Internet securely. The following sections give you a quick overview of the various component programs and what they do.

Erecting a firewall

A *firewall* is an application that monitors and filters all the traffic going into and out of your connection to the Internet. That connection is commonly called a *gateway*. In the physical (that is, the real) world, a gateway may be nothing more interesting than a modem with a phone line or cable plugged into it. From the perspective of your computer, a gateway is the point at which information enters and leaves your network.

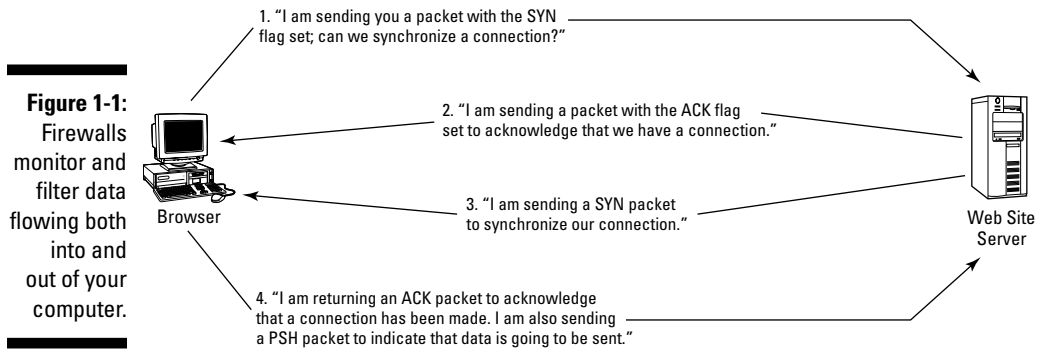
You may already have heard that a firewall is something you need when you get a high-speed connection to the Internet such as a cable modem or Digital Subscriber Line (DSL) connection. Firewalls *can* be complex to configure and maintain. The firewall that's part of Norton Internet Security, and that is called Norton Personal Firewall, automates many of the administrative tasks, however.

Monitoring and directing traffic with firewalls

Communication on the Internet is always a two-way street. When you connect to the Web site of the auction site eBay, for example, your computer and the Web site's servers communicate by exchanging segments of digital information called packets. First, your browser sends requests to the server in the form of one or more packets. The requests flow in the *outbound* direction from your computer. Then, the server responds by acknowledging the requests, and then sending images and text files from the Web site's servers to your computer so they can be displayed by your browser. Those files flow



in the *inbound* direction to your computer. The exchange of messages is illustrated in Figure 1-1.



Two elements mentioned in Figure 1-1 bear explaining. A *packet* is a segment of digital information. Each packet can be broken into different sections, including a header and a data payload. Within the header, a number of different bits of information called *flags* signal to another computer on the network what is being requested. The flags are analyzed by programs such as Norton Personal Firewall in order to recognize and block known types of intrusions.

The fact that data packets flow in two directions between your computer and others on the Internet might seem obvious. But it's important to keep this in mind. When you begin to work with Norton Personal Firewall (a process described in Chapter 2), you'll be asked to set up a series of rules. Those rules determine how the firewall will respond to a particular type of data based on the direction in which it is going. Some rules can restrict information flowing in the inbound direction; others can restrict only outbound data going to a specific computer; other rules can block or allow information flowing in both directions.

Your computer's "secret" conversations

Another important thing to remember is that your computer continually carries on a series of packet exchanges with other computers on the Internet whether you're actually using the machine or not. When you have a connection that is always on, such as a DSL line, you can easily leave your computer connected to Web sites and go off and do other things. I, personally, like to listen to Internet radio. Many radio stations have the capability of sending their signal to listeners on the Internet in a process called *streaming*. I frequently leave the computer connected to a station and listen to it while I'm doing chores around the house. While I'm listening, my computer and the server that provides the data stream are in constant communication, checking with one another to make sure they are still there, to make sure the data is available, to verify that it is being received, and so on.

You may think you're doing a single thing on your computer, but in reality, a variety of different connections have been established or are underway. As I write this, my Web browser is connected to the popular Web site Google, and I'm listening to an Internet radio station. Those are only the obvious things going on. In fact, many more connections have been established, and the computer is listening for connections on virtual openings called ports (see the section "Port scans" for a more detailed explanation of these important network communications elements). In reality, my computer might be connected to an e-mail server and waiting for incoming mail, to another Web site, and to other computers on my home network.

Why worry about packets and all the "behind the scenes" communications your computer makes with others on the Internet? The point is this: These communications often occur in the background without your knowledge. Computers can try to connect to your computer while you are on the Internet and you have an Internet application running. Your computer is sending out responses that may or may not provide those remote computers (and their owners) with information about you and your network. Without a firewall, you don't have any control over such communication. *Hackers* — individuals who try to gain access to other computers on the Internet — can and will probe your computer for openings, and then try to exploit any openings they find. (See "Understanding Hackers," later in this chapter, for more information.) A firewall is essential for anyone who has an always-on connection to the Internet for precisely this reason: The firewall polices traffic in a way that you can't. It's like a sentry on duty, day and night.

Combating viruses

You may wonder why hackers try to connect to other computers they find on the Internet. Many reasons exist, but one is that they want to plant a type of virus called a *Trojan horse* (or other harmful program) on someone else's computer. Viruses come in many varieties and perform many different functions. But in general, they function in a way that's similar to the viruses that make you sick:

- ✔ **They contain segments of code that cause problems.** In the case of a human virus, the code is DNA. Computer codes are what make up computer viruses, and what cause those viruses to do harmful things.
- ✔ **They come in many different forms.** According to the Big Picture Book of Viruses (www.tulane.edu/~dmsander/Big_Virology/BVHomePage.html), there are human, fowl, equine, and many other viruses that affect living creatures. In the world of computing, the term "malware" is often used as a catchall term that includes variations such as viruses, worms, Trojan horses, and other harmful software programs.

- ✔ **They are difficult to detect and infiltrate without your knowledge.** Human viruses can only be seen with the aid of powerful microscopes. If you start sneezing or feeling bad, you can tell you have a virus. Computer viruses can get into your computer as files contained in software you download, or as attachments to e-mail messages that seem harmless. If your computer slows down or stops working, you can tell it has a virus.
- ✔ **They spread.** All viruses have the ability to move from one place to another and duplicate themselves so as to spread the infection. In one type of harmful program called a worm, this is the only function: Worms continue to multiply, consuming disk space and computing resources. Others duplicate by e-mailing themselves to other users whose addresses they find in Microsoft Outlook Express's address book, for example.

Viruses are among the most harmful security threats on the Internet, and anyone who goes online should have some form of virus protection. For whatever reason, a lot of people all over the world seem to take pleasure in phishing: sending e-mail messages to other people with attachments that contain viruses or other malicious programs. I regularly receive several such e-mail messages each week. The body of the message might say, "Your document is attached," "Look at this," or perhaps nothing at all. Anyone who clicks on the attachment to open it will unleash a virus or other program. And people unknowingly cause their own computers to be infected all the time by such means.

Norton AntiVirus takes the uncertainty out of receiving messages with suspicious attachments. It has the capability of recognizing attachments that are likely to contain harmful code; it can even scan the attachments and detect the viruses. It sends up alert messages, such as the one shown in Figure 1-2, before you even open up a message.

Figure 1-2:
Norton
AntiVirus
displays
alert
messages
the moment
a virus is
detected.



After identifying the virus, Norton AntiVirus takes steps to repair it (in other words, to change the code so that it doesn't cause any damage to your files or perform any unauthorized actions). If the file cannot be repaired, AntiVirus stores it in a special file called a quarantine area, where it cannot cause harm to your computer or the files within it.

Norton AntiVirus can protect your computer from viruses and other harmful programs such as worms, macros, and Trojan horses. But the program has to be periodically updated with new information about these programs so it can recognize new ones as hackers develop them. See Chapter 5 for more about how to use Norton AntiVirus.

Blocking unwanted content

Anything that consumes time, disk space, processing power, and browser "energy" detracts from your experience of the Internet. This isn't the way businesses that provide content and services on the Web think, however. They send you e-mail messages you didn't ask for, advertising products you don't necessarily want. They want to advertise other products and services, and frequently, they do so by causing browser windows to pop up (or under) the Web page you really want to see.

Popping Web page pop-ups

One of Norton Internet Security's most welcome features is its capability of preventing pop-up pages from appearing by means of a component called Ad Blocking. Ad Blocking not only stops banner ads and new browser windows from appearing, but stops Flash presentations and other intrusive content, too. It illustrates the fact that Norton Internet Security exists not only to block security but to improve your overall experience of the Internet, which includes giving you more control over what you see online.

See Chapter 6 to find out more about how to use Norton Internet Security to block ads as well as "spyware" and other programs that erode your privacy.

Throwing out spam

Norton Internet Security exists not only to make your experience on the Internet more secure, but more pleasant as well. One of the things that makes cyberspace unpleasant is the amount of unsolicited e-mail messages you receive. The number of messages circulated online appears to be steadily rising, despite legislation in the United States (specifically, the CAN-SPAM Act that's supposed to regulate it). One of Norton Internet Security's component programs, Norton AntiSpam, is designed to cut down on spam before it ever gets to your e-mail inbox. See Chapter 9 for more on AntiSpam, and "Adopting Effective Privacy Strategies," later in this chapter, for details about how you can provide extra control yourself.

Keeping your business secure

A survey conducted by the Business Software Alliance in 2003 found that two-thirds of corporate security professionals surveyed believe that they are likely to experience a major cyber-attack on their organization. However, only 78 percent of those security professionals believe their own organization is prepared to defend against such an attack.

Attacks can come from outside the corporate network. But in many cases, the real threat comes from within. Employees who have been fired or who have an axe to grind against the organization can cause substantially more harm than hackers on the other side of the world. The former employees know what resources the company holds, such as customers' credit card numbers or personal information, or proprietary information about products under development that their competitors might pay to own. They also know which computers hold the information. If the company has neglected to change passwords after the employees have left, they may be able to break in to those computers with virtually no technical expertise.



The 2003 Computer Crime and Security Survey conducted by the Computer Security Institute and the FBI reported that 56 percent of respondents experienced unauthorized use of their network computing resources. The total annual losses resulting from such intrusions amounted to more than \$201 million. You can read more about the 2003 Computer Crime and Security Survey at www.gocsi.com/forms/fbi/pdf.jhtml.

Protecting your children

If you have kids, you already know how they love the Internet. It's an endless playground full of games, amusements, information, and ways to make friends. They take to it quickly and, before long, they know more about cyberspace than you do. The same ease of use and wealth of information can cause problems for both parents and children. Without your knowledge, your children may be exposed to violence, improper images, and other content that they shouldn't know about.

Through a Norton Internet Security component called Parental Control, you gain a measure of control over what your children can see and do online (at least, while they are in your house and using a computer on which Norton Internet Security has been installed). You can block Web sites that seem unsuitable, develop a list of "acceptable" Web sites, and get information about the sites your kids have visited while they are at the computer keyboard. Find out more in Chapter 13.

Understanding Hackers

Sometimes, protection begins with understanding — in the case of security on the Internet, that means understanding what the threat is, what those who threaten you want, and how they work. With some general knowledge at hand, you can take steps to anticipate trouble.

In general, the threats that come to you from the Internet are from hackers. A hacker is someone who is good with computers (though not necessarily a programmer). Such an individual uses any of a number of different ways to gain unauthorized access to computers. Reasons vary widely as to why hackers try to break in to remote systems, the way they attempt such break-ins, and what they hope to find. But with a little general knowledge about who is out there and what they might be after, you can be that much more effective in securing your computer.

“White Hat” hackers

The classic hacker, known as a “white hat,” isn’t necessarily out to do harm or even to steal files. He or she is primarily interested in breaking into systems under controlled conditions with the goal of improving security. (Another type of hacker, called a gray hat, does break-ins in order to discover how things work and open up any sources of knowledge that they can find — and claim credit for it.)

Some hackers (such as the ones who run the Hackers.com Web site (www.hackers.com)) claim to be interested in instructing the public on the ethics of hacking. Unfortunately, such hackers make up only a small number of those who break into other people’s computers. Some less benign variations on the hacker theme are explored below.

Script kiddies

As the name implies, script kiddies tend to be young, but that’s not always the case; they’re beginning hackers. Often, they are looking for a thrill in their spare time, and they use their knowledge of computers (or knowledge they have gleaned from various Web sites devoted to hacking) in order to gain control of remote systems. Some are computer programmers who spread viruses and other malicious scripts and use other techniques to exploit weaknesses in computer systems. Others are primarily interested in breaking into as many computer systems as possible, then claiming credit for it in order to gain attention. They may claim credit by defacing Web sites — in other words leaving messages that can be read by their fellow script kiddies.

Script kiddies, who are sometimes called packet monkeys, can hardly be called harmless. They are known for carrying out Denial of Service attacks in which as many as several hundred computers are infiltrated by a hacker and used to overload a Web site simply by connecting to it so many times that the site's server becomes overloaded and ceases to respond to legitimate requests.



A 14-year-old Canadian script kiddie known as MafiaBoy carried out one of the most notorious attacks ever in February 2000. The attack, called a Denial of Service, prevented visitors from accessing many of the biggest Web sites, including those of Amazon.com, eBay, and Yahoo. The boy was arrested in April 2000. In January 2001, he pleaded guilty to 58 charges related to the attacks. He was eventually sentenced to eight months in a juvenile detention center. As I was writing this book, an 18-year-old German student and computer programmer confessed to creating a virus called Sasser that affected millions of computers around the world. The virus exploited a flaw in the Microsoft Windows operating system and caused computers to repeatedly shut down and reboot.

Thieves

Many hackers can be called “black hats.” Their goal is to steal someone's identity, money, or other goods and services. In Chicago, where I live, hackers recently gained access to the state's database of temporary license plate numbers, apparently hoping to be able to generate fake licenses for autos.

Some very competent hackers attempt to break into banks and military facilities, hoping to steal money, maps, or information. Others try to break into e-commerce Web sites that use encryption to secure data, but these are for the most part difficult targets. These days, the most frequently stolen item on the Internet is personal identity, which is fast becoming an epidemic. If people can get their hands on legitimate Social Security numbers, credit card numbers, and other data, they can make fraudulent purchases that can cost the victim time, energy, and money.

Crackers

Passwords are among the most widespread security measures on the Internet. Everyone who goes online has a password of some sort. Because passwords are so widespread and protect resources that are often highly valuable (such as bank accounts, Internet access accounts, or software programs), they are frequently a target. Crackers are primarily interested in obtaining passwords in order to go online and gain access to systems and data, and to assume your identity.

All too often, a cracker's job is made easy by the fact that an individual user has chosen a ridiculously simple password — or no password at all. Here are examples of passwords you shouldn't use:

- ✓ 123abc
- ✓ MaryJones
- ✓ password
- ✓ administrator

Even if one of these easily-guessed passwords is not used, crackers can still uncover passwords that aren't secure enough. They can use a special password-cracking application that can guess it in one of three ways. It might perform a *dictionary crack*, which runs through all the words contained in the dictionary in rapid succession. It might conduct a brute force crack, which runs through a series of random characters and submits huge numbers of possible passwords to the server very quickly. Finally, it might do a *rule-based crack*, which is performed if the cracker has knowledge about the rule used to create the password.

In the early days of the war with Iraq, it was reported that U.S. intelligence broke into an e-mail account used by Uday Hussein, one of the sons of former Iraqi dictator Saddam Hussein. The password used on the account was reported to be a simple word in the dictionary that was easily cracked.

Demon dialers

Some of the earliest hackers were individuals who tried to abuse not computer networks, but phone systems. They developed and used special devices called black boxes in an effort to make free phone calls. They had a number of goals: They wanted to get something for nothing, they wanted to feel like they were putting one over on "Ma Bell," and they wanted to have a way to connect to bulletin board services by dialing the same number over and over again until a connection was made.

Today, hackers use software that dials phone numbers in rapid succession. But rather than trying to connect to a bulletin board service, such software is used for less benign purposes. Sometimes, software applications called dialers infiltrate computer systems without the owner's permission. They then dial out through the Internet to a 900 number or FTP site, typically to accrue charges. These programs, which are known as "demon dialers," "war dialers," or simply "dialers," can also be used to launch a Denial of Service attack against a remote system.

Computers that have direct connections to the Internet are able to make phone calls online using a technology called Voice Over IP. You might be able to use the technology to save some long-distance phone charges (as long as you are willing to accept some compromises with the quality of the audio).

What intruders want

You might well ask what all these nefarious individuals are looking for, and why they would go through the trouble of breaking into your computer. Some are only looking for valid e-mail addresses: these are the marketers, or the businesses that sell e-mail addresses to bulk mailers who are going to be sending you spam e-mail. (You might even get junk “snail mail,” if your mailing address falls into a marketer’s hands.) That’s the least of your problems, however. Here are some more serious potential pitfalls:

- ✓ Access to your children
- ✓ Your credit card information, so they can make purchases
- ✓ Your e-mail program, so they can distribute viruses or other harmful software as widely as possible
- ✓ Access to your Web browser and those of as many other individuals as possible, so they can launch a coordinated attack on a high-profile Web site (such as Microsoft’s). This is called a Denial of Service attack.
- ✓ Access to your computer system so they can place programs on it, glean information from it, and generally disrupt it.

As this quick survey of hacking’s “cast of characters” indicates, if you want to be really secure you need to be prepared for a variety of attempts to gain access to your computer. The section that follows suggests what to look out for when an attack is underway, and how Norton Internet Security can help you detect it.

Recognizing Garden-Variety Attacks

If you are a home user with a handful of computers on the Internet, you can count yourself lucky. You aren’t likely to run into the most dangerous hackers, who save their talents for breaking into defense systems, universities, and e-commerce Web sites. You’re more likely to experience one of the more common incidents mentioned in the sections that follow.

It's true that Norton Internet Security should, if all of its components are installed correctly and the product is updated on a regular basis, thwart such events before damage occurs. But it's still good to know what to look for. You may be able to take further steps that make your computer even safer. If Norton Personal Firewall notifies you that someone is doing a port scan on your computer, you may want to make sure that vulnerable ports are closed. If Norton AntiVirus detects a virus, you may want to download a new set of virus definitions and do a manual virus scan as described in Chapter 5.

Norton Internet Security can perform a wide range of security functions. But no security application is a cure-all. Like any security program, it can be undone by new attacks, new viruses, unsafe passwords, employee break-ins, or other weaknesses. The descriptions in the following sections will alert you to some potential weak spots you might want to strengthen.

Port scans

Your home has a variety of openings to the outside world. Each opening is set aside so that a different kind of object can pass through. Air and light flow through windows. Mail goes through the mail slot. Gas flows through one set of pipes, and water through another. Information of different sorts flows into and out of your computer.

Depending on the software you have installed, you can send and receive that information using preassigned ports. Chances are you have a Web browser, an e-mail application, and an application that enables you to send and receive instant messages. Data from each of those sources enters and leaves your computer via a virtual opening called a *port*. Don't look on the back of your computer for this sort of port. It isn't a physical opening but an abstract designation that software programs use to communicate with one another over a network.

Problems occur when a computer is "listening" on a port — in other words, waiting to receive a connection on that port — but the port isn't actually being used. Such open, unused ports are vulnerable openings that hackers can exploit. In order to identify open ports, hackers use software that attempts to connect to each port, one after another. This series of connection attempts is called a *port scan*. A port scan isn't an attack in itself, but it can lead to one if the hacker finds an open port.

Ports are especially important because they frequently turn up in the alert messages that Norton Internet Security displays. Certain ports, such as 137 or 53, show up frequently in attack attempts. If you know the port the hacker is trying to access, you can make a reasonable guess what attack is being tried and take steps to protect your computer from further damage.

Some common ports, the Internet communications services that use them, and the kinds of attacks that can occur on those ports are listed in Table 1-1.

Port Number	Type of Service	Protocol Used	Attack
20, 21	File transfers	File Transfer Protocol (FTP)	FTP “bounce” attack
25	Outgoing e-mail	Simple Mail Transfer Protocol	The “cancel” attack or other e-mail attack
53	Domain name lookups	Domain Name Service (DNS)	Buffer over flow attack
80	Web browsing	HyperText Transfer Protocol	NIMDA virus
137	NetBIOS	Name Service	Worms or viruses, or attempts to access shared files

A *protocol* is a set of standard instructions or rules that computers must use when they communicate over a network. Having a standardized set of rules and instructions enables computers from different manufacturers, using different operating systems, to share information and connect to one another. When it comes to firewalls and security, you need to know about two protocols: Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). Along with Internet Protocol (IP), TCP is the fundamental, underlying protocol that makes it possible for computers to exchange information securely by breaking it into uniform and manageable sets of data called *packets*. UDP is a less secure, simpler protocol that is more vulnerable and that is frequently exploited by hackers.

IP address attacks

In order to send a package from one place to another, you need to label it with an address. That way, the delivery person can find the correct destination. Computers on a network need to be able to find one another as well. The “street address” used by computers is called an IP address. Many hackers operate by attempting to locate IP addresses that they can then scan for points of entry.

The IP stands for Internet Protocol, a set of standards that enables computers to locate one another on the Internet or a private network. The version currently in use on the Net is Internet Protocol Version 4 (IPv4). But the available IPv4 numbers are dwindling, and a more complex and number-rich version, IPv6, had just been instituted as I was writing this book. In IPv4, each computer on a network is assigned an IP address, a set of four numbers separated by dots, such as 192.168.34.1. Each of the four numbers in an IP address can have a value of between 0 and 255.

Hackers use (or rather, misuse) IP addresses in two general ways. First, they try to locate as many static and legitimate IP addresses as possible. A computer's IP address is static when it does not change from session to session. It is legitimate when it can be traced to a real computer that is connected to the Internet, as opposed to a "private" IP address that can only be used on an internal network such as that operated by a corporation or other organization. Hackers sometimes try to locate as many IP addresses as possible; they then attempt to break into each of the computers associated with each address in order to launch a coordinated attack against another Web site.

Problems with "always on" connections

Every computer that is connected to the Internet has an IP address. But some IP addresses are temporary or dynamic, while others are constant or static. If you dial in to a Web server and connect to the Internet using a modem, your IP address is temporary. It is assigned to you by your Internet Service Provider (ISP), and it only lasts for the length of the phone call. When you disconnect, the address is assigned to another customer of the ISP. When you want to reconnect, you get a new, temporary IP address that is assigned to you from the ISP's pool of available addresses.

IP addresses of computers that are connected to the Internet are one of the things that hackers try to determine in order to break in to computers. But because of their transitory nature, temporary IP addresses are not only difficult to detect, but they are useless to hackers.

The problem comes when you upgrade to an Internet connection that is always on — as long as the computer is on or your cable modem or

DSL router is on (all of these devices can be switched off when you do not need to go online, for greater security). Rather than dialing in to a server with your modem, you are connected all the time thanks to a cable modem or Digital Subscriber Line (DSL) connection. When you connect to the Internet using one of these two kinds of systems, you get high-speed access. But you also get an IP address that seldom, if ever, changes.

Most ISPs that provide cable modem and DSL access offer their subscribers temporary IP addresses. But if the user is online for days or even weeks at a time, that temporary address remains the same during that time. A few users (such as me) pay extra to have static IP addresses, which never change. Obviously, they are even easier for hackers to find and exploit. It's great to have a direct connection to the Internet, but keep in mind that such a connection makes it even more important that you install and configure Norton Internet Security to provide the protection you need.

The second way in which hackers misuse IP addresses is by “spoofing” them. A spoofed IP address is one that has been deliberately falsified in order to conceal the identity of the person operating the computer — in other words, the hacker himself, who does not wish to be traced so as to continue probing and breaking into remote computer systems.

Back doors

As I mention earlier in the section “Port scans,” computers have a variety of both physical and virtual openings through which information can pass. The “front doors,” or the approved openings, are the plugs that you use to connect peripheral devices such as hard drives, or the ports that are assigned to let certain software programs communicate.

But computers have “back doors” as well. A back door is a hidden opening, often unknown to the end-user, through which hackers can infiltrate remote systems. A back door may be a port that is left open. But it can also be a password stolen or misused by an employee, or a way of accessing a network from a remote computer. It can also be an opening that is created by a computer program the user downloads. Unknown to the user, the program’s author has planted code in the program that establishes communication with the author through the Internet.

Some back doors are caused by flaws in system software or other applications. Microsoft Windows is occasionally the culprit. In April 2004, hackers believed to be from Brazil, Germany, and the Netherlands attempted to take advantage of a security flaw in a particular version of Windows in order to gain back-door access to major financial institutions in Australia. The security flaw was repaired by a patch issued by Microsoft, but all the banks’ servers may not have installed it. However, the global security monitoring service, Internet Security Systems (www.iss.net), issued alerts to the banks, and the attacks were thwarted. The lesson: Always install security patches issued by Microsoft or other software vendors as they become available.

Trojan horses

After hackers discover the presence of a “back door” on a remote system, they can send software through that back door into the system. Often, the software appears to be harmless. But inside, it has a potentially harmful payload. Such software is called a Trojan horse. Perhaps the worst kind of Trojan horse is one that comes disguised as a program designed to get rid of viruses or other malicious software. Instead of performing anti-virus functions, the program injects viruses into the system.

In early 2004, a security company called Intego announced that it had discovered what was believed to be the first Trojan horse designed to attack Macintosh computers. The program — which was described as harmless — came inside an MP3 file that could be downloaded from the Internet. Although this Trojan horse was harmless, the company said it pointed the way for other, more harmful programs that might be planted in the future.

Social engineering: Ha, fooled ya!

The term *social engineering*, invented by hackers, is a complicated-sounding term for fooling a person into giving out sensitive information that a hacker can then use to gain access to a system, use someone else's credit card account, and so on. Even companies that have teams of security professionals in place, as well as firewalls and other intrusion detection systems, can have their work undone by such methods.

The most famous hacker to date, Kevin Mitnick, was an expert at social engineering. He gave a speech to a group of hackers in 2000 where he boasted that he was able to “obtain any number, listed or unlisted,” as well as network access passwords and other information. You can read a report of the talk at <http://zdnet.com.com/2100-11-522261.html>. Being aware of social engineering attempts is one of the best ways to improve computer security. If someone sends an e-mail message that induces you to give out your credit card or bank account information, they will bypass all the safeguards provided by Norton Internet Security and any other security devices you have installed on your computer.

Viruses in downloaded software

Sometimes, it seems like you can find, download, and enjoy just about anything online. Whether you're looking for a piece of music, a trial version of a software program, an installer file that helps you install a larger program, or something else, be very careful and make sure you have Norton AntiVirus running before you click the Download button or link.

The file sharing sites that enable users around the world to share and download music and other files often give users more than they bargain for. In order to use sites such as KaZaA, Gnutella, or Morpheus, you need to download software that enables you to connect to the sites, search for shared files, and download. Over the years, such software has been known to have the capability of keeping tabs on what you do. These programs aren't exactly viruses, but they fall under a different category of software known as

spyware. The manufacturers of spyware pay a small fee to the file sharing companies to distribute the utilities. The utilities, which are often installed and run without the user's knowledge, can cause ads to pop up automatically on the user's machine and keep track of the Web sites the user visits so that ads can be tailored to his or her personal preferences. Here are a few examples of software "extras" that you don't ask for, but might get anyway:

- ✔ **cydoor.** Early versions of this program installed themselves in a part of Windows systems called the Registry, and were configured to start up automatically whenever your system was rebooted (whether you knew the program was there or not). The program downloads ads onto your computer. You can install the application, but you don't always have a choice about whether it's installed in the first place.
- ✔ **SaveNow.** A program that takes up processing resources, collects information on what Web sites you visit, and that automatically launches pop-up ads.
- ✔ **b3d.** A program distributed by a company called Brilliant Digital. At one time, this software turned your computer into a part of the company's worldwide network, giving Brilliant the ability to use your system for itself and its clients.

The last program mentioned on the list is no longer bundled with KaZaA. But because it used to be part of the program, would you really trust these people now?



You can read a review of KaZaA that mentions these bundled files and others at www.dooyoo.co.uk/computers/applications/kazaa.

Infected files

People can do an ever-increasing amount of work on computers and also on the Internet. People who write or edit for a living, as I do, know that entire books can be written and edited online. In the days when floppy disks used to be exchanged on a regular basis, viruses could (and did) spread from one person's computer to another. They can be spread when infected files are downloaded, opened, or copied.

The Internet has dramatically reduced the instance of floppy disk infection, but individual files can still be infected by macros and other harmful substances. A *macro* virus is a type of virus that infects a specific type of file. Commonly, Microsoft Word has been infected by macros, as has Microsoft Excel. Macro viruses aren't as prevalent as they once were. A major macro virus outbreak accompanied the release of the Windows 95 operating system

in 1995; another occurred in the year 2000. But viruses you download from file sharing networks or from CDs you receive from untrustworthy people can contain infected files as well. The moral: Keep Norton AntiVirus installed, don't open any file you don't recognize, and only download files from trusted sources.

Visiting Symantec Security Response

Symantec Security Response has a variety of resources besides the virus scanner that you should check on a regular basis. It's an especially good idea to visit the site if you manage the network for a small business; you can notify co-workers of any serious virus attacks and download any removal tools, for one thing. Here are some other reasons why you would want to visit the site:

- ✔ **Find out about updates.** The home page displays the most recent set of virus definitions included with Live Update, the component included with Norton Internet Security that automatically updates the program. A definition is a set of characteristics that identifies a virus or other intrusion; a firewall or anti-virus program uses the definitions to recognize security threats and handle them appropriately.
- ✔ **Learn about the latest security advisories.** Some threats can be handled by Norton Internet Security alone, but some (such as those that affect Microsoft Windows) require you to install patches to prevent intrusions.
- ✔ **Download an analyzer.** An analysis tool called DeepSight prepares reports of any intrusion attempts or virus attacks you have faced. It's designed to work with Norton Internet Security and is available for free. (Find out more in Chapter 4.)
- ✔ **Get background information.** The links presented under the heading "reference area" on the Symantec Security Response home page provide you with a wealth of general data about computer security.

If you use Norton Internet Security in a business environment and you need to inform your colleagues about security issues, the resources listed earlier can help you prepare well-researched reports and make sensible recommendations based on current security conditions.

Adopting Effective Privacy Strategies

If you use Norton Internet Security and do nothing else to protect your computer, you haven't really created a secure environment for yourself, your family, or your office. You also need to adopt some sensible strategies when

you sign up for online services or communicate via e-mail or instant messaging. It's a matter of changing the way you approach the Internet. If you are aware of privacy dangers and you adopt the approaches mentioned in the sections that follow, you'll help NIS protect your computer that much more effectively — because there will be fewer intrusions to fend off.

Don't believe everything you read

Some people will do anything to get your attention on the Internet. When they approach you online, they can't always use images or sounds to reach you. Instead, they try to entice you and tempt you using a variety of possible strategies:

- ✔ **They try to generate fear.** You might receive e-mail or Web-based messages such as, "There has been a security breach and your account has been compromised. You need to verify your personal information right away."
- ✔ **They arouse curiosity.** You connect to a Web page, and you see a warning informing you about a new search utility that you can install. Or, a dialog box appears, asking if you want to make the current page your browser's start page.
- ✔ **They offer you something too good to be true.** You see a copy of an expensive and complex program on a file sharing site, absolutely free. When you download the compressed file that supposedly contains the program, you get shortcuts that are automatically added to your Start menu, and that point to "adult" Web sites.

Be suspicious of everything you see online, only subscribe for services you really need, and never offer to sign up, subscribe, download, or install something for nothing. As they used to say at the University of Chicago, "There ain't no such thing as a free lunch." That applies to free downloads, too.

Recognize suspicious e-mail warning signs

It doesn't take long before you'll be able to recognize e-mail scams that can cause you harm. Bad spelling and grammar are an obvious , as are outlandish claims. I, personally, have received e-mail messages in recent weeks that said the following:

- ✔ "something is fool"
- ✔ "Would you like to become a successful real estate investor just like Donald Trump?"

- ✓ “Need to lose weight?”
- ✓ “This is the best way to control spam.”
- ✓ “Did you ask me for that?”

Almost all of these messages had an attachment just waiting for me to click on it. I didn't, of course, knowing that it probably contained a virus or other malicious program. Norton Internet Security not only has the capability of blocking much spam, but also for detecting suspicious e-mail attachments the moment they reach your inbox: You get an alert about a possible virus before you get to open it. But you still need to recognize e-mail spams just in case a new one manages to get past Norton Internet Security and into your computer.

Give out as little as possible

The Internet is a remarkably open place. It's a perfect medium for chatting, making online friends, sharing information, and learning about current events. But be selective about what you share and who you share it with.

One of the best ways to give out information that enables marketers to “attack” you with unwanted e-mail messages is by filling out forms. When you sign up for something, you typically provide your name, address, phone number, and e-mail address (if not more). Do you know what the online service you register with is going to do with that information?

One of the best ways to protect your privacy is to give out as little as possible. Do you have to provide a business with your real address and phone number? Why do they *need* such information, if they are only planning to contact you by e-mail? Don't fill out any fields on forms that are not required; when you do provide an e-mail address, make it an address that you have reserved for such registrations. That way, your “registration only” e-mail address will get all the special offers, confirmations, notices, and other messages you didn't ask for when you signed up. Your primary e-mail address will stay relatively free of spam if you just don't use it to sign up for anything, and if you give it out only to personal acquaintances you trust.



A sense of “minimalism” applies to running computer programs as well as filling out registration forms. Throw out or disable applications you don't use or don't need so they cannot be misused. Sometimes, system software runs programs that you don't need and that represent a security risk. Some versions of Microsoft Windows automatically started up Internet Information Server, a built-in Web server, which became a well-known vulnerable spot that hackers could breach.

Managing Your Passwords

One of the best things you can do, when you are preparing to install Norton Internet Security, is to tighten up your existing passwords and adopt a more secure policy toward any passwords you plan to set in the future. As you already know, a password is a set of characters you enter on your keyboard and submit to an application, a Web page, or a Web site server in order to go online, gather your e-mail, or use a software program or online service. When you send the password to the program or server, it is checked against a database of approved passwords. If a match is made, you gain access.

Norton Internet Security does not protect your passwords. It doesn't keep unscrupulous individuals from guessing them or stealing them, which can open up your whole computer to intrusion. Poor password security (or lack of passwords) can undo everything NIS tries to protect, so passwords are examined in some detail in the sections that follow.

Picking a good password

The most effective passwords are ones that are created randomly, by a software program that generates them for you, and that have a one-time use. After that single use, they are discarded. Such passwords are virtually impossible to crack, but they are also very impractical. You want to be able to quickly enter your own password (one that you can easily remember) whenever you go online, place a bid on eBay, or view the status of your checking account. You don't want to wait for a program to devise the password for you.

The best passwords are at least six to eight characters long. They use both numerals and alphabetic characters. A good password looks like this:

```
w3JjU@!39Gxv$
```

This would be a very hard password to crack, even for someone using a special software program. But could you possibly remember such a password? It can be helpful to use a recognizable slogan or phrase to create a password that sticks in your mind. Think about a slogan or phrase you can recall easily, such as You Ain't Nothin But a Hound Dog. The initials can be used to create a password:

```
YANBAHD
```

To make this password even more secure, add the date the song was a big hit, 1956:

```
YANBAHD56
```

For *really* good security, mix the upper and lower case, like this:

```
yAnBaHd56
```

The result is a highly secure password. Because anyone who uses the Internet needs more than one password, you can create a set of passwords that follows the same formula — in this case, the titles of Elvis Presley songs, such as ILYRSG, WTARM, and WMRAYN.

Encrypting your passwords

Coming up with a password that proves difficult for “cracking” software to uncover is only half the battle. The other half is storing your passwords in a secure place. You can’t be expected to memorize all of your passwords. I, personally, think I have at least 25 combinations of usernames and passwords. It’s also insecure to use the same password for every service you use — if someone obtains one password, they can gain access to all of those accounts.

Encryption provides a foolproof way to store your passwords. Encryption is the process of manipulating information so that it cannot be read by unauthorized individuals. Information is manipulated by means of a mathematical formula. Only authorized individuals who have the formula can decrypt the information in order to read it. On the Internet, some Web sites can encrypt sensitive information that passes between a browser and a server. Such encryption needs to be highly secure, and is accomplished by means of complex formulas called algorithms. The algorithms process large prime numbers to create long sets of alphanumeric characters called keys. The keys are then used to encrypt information and ensure that the individuals who possess the keys are who they say they are.

One way in which you can use encryption is to encrypt your passwords and store them using a specially designed software program. Several programs are available to help you conceal your passwords; two examples are described below.

Norton password protection

Symantec markets a password encryption tool with the Norton brand, but it’s a product that’s separate from Norton Internet Security. Norton Password Manager protects much of the data that Internet users give out when they fill

out forms. It has the capability of creating and storing multiple user profiles, so all of the people who use your computer can store their passwords there. Each user creates a profile that contains his or her address, phone number, and other contact information (see Figure 1-3). Password Manager enters the information for you automatically whenever you fill out a form. It also enters passwords automatically when applications prompt you for them.

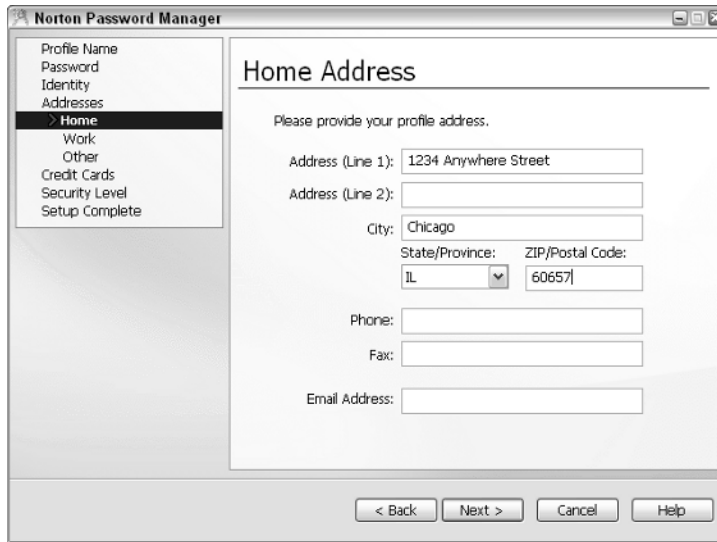
The screenshot shows the 'Norton Password Manager' window with the 'Home Address' form. The left sidebar contains a menu with options: Profile Name, Password, Identity, Addresses, Home (selected), Work, Other, Credit Cards, Security Level, and Setup Complete. The main form area is titled 'Home Address' and contains the following fields: 'Address (Line 1):' with the value '1234 Anywhere Street', 'Address (Line 2):' (empty), 'City:' with the value 'Chicago', 'State/Province:' with a dropdown menu showing 'IL', 'ZIP/Postal Code:' with the value '60657', 'Phone:', 'Fax:', and 'Email Address:'. At the bottom of the window are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

Figure 1-3: Norton Password Manager takes the work out of filling out forms and remembering passwords.

The trick, of course, is that you need to create a password in order to create a secure user profile. When you have the profile in place, you can store all of your credit card and bank account numbers, as well as passwords. The program then fills out forms for you automatically using your securely stored information. But you need to remember one password — your account password — in order to get access to your passwords. (Luckily, Password Manager lets you record a “hint” so you can remember this password more easily.) After you enter your personal information and credit card data, you can begin to store passwords as you visit Web sites and are prompted to enter them. The program’s interface (see Figure 1-4) closely resembles that of Norton Internet Security, as you’ll see in Chapter 2.



You don’t necessarily need to install a software program in order to securely store your passwords. You can also store them online using a service that protects your sensitive information. Obviously, you place a great deal of trust in such services. Consider PasswordSafe (www.passwordsafe.com) or one of the password safety services listed by an organization you really can trust, the Electronic Privacy Information Center, at www.epic.org/privacy/tools.html.

Password Officer

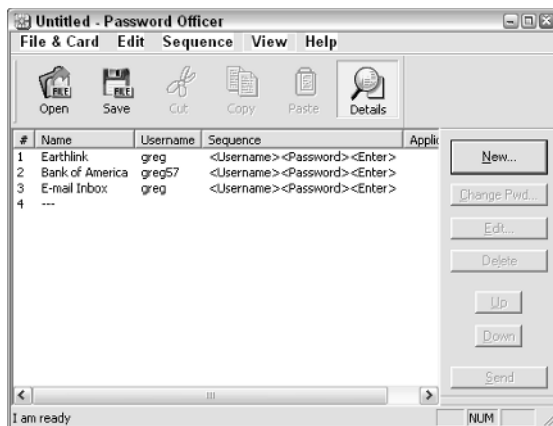
This program by Compelson Laboratories (www.compelson.com) comes in four different versions. You can't beat the price of Password Officer Lite: It lets you store ten passwords or other items for free. A Standard version lets you store 40 items and costs \$29; the DeLuxe version has unlimited storage capacity and costs \$59.

Figure 1-4: Norton Password Manager complements the features provided by Norton Internet Security.



The program not only stores passwords but also creates them for you. You assign each password a number or other code or a short account name that is easy to remember (see Figure 1-5). You only need to enter the code or name when you want to enter a password; Password Officer enters the actual password for you automatically.

Figure 1-5: Password Officer not only stores encrypted passwords but generates them for you.





Leaving passwords in place after you have memorized them is tempting. But you'll achieve an even greater level of security if you make an effort to change your passwords every few weeks or months. That way, if someone has cracked a password without your knowledge, the access they gain will last only until you change the password.



If you're looking for just the right password management application, read PC Magazine's review of password managers at www.pcmag.com/article2/0,1759,1587793,00.asp. (Password Officer is not included, however.)

