

Chapter 1

Understanding Virus Risks

.....

In This Chapter

- ▶ Figuring out whether you're at risk
 - ▶ Making good security decisions
-

There's an old saying: "Just because you're not paranoid doesn't mean that everyone isn't out to get you." This saying is proven by the people who write computer viruses — they *are* out to get you! And, in fact, a little paranoia may go a long way in protecting your computer.

In this chapter, I provide you with the factors that may increase your personal level of useful paranoia — in other words, the factors that can influence you to lower your personal risk level. Why? Because, get this, some people are more apt to catch computer viruses than others, and it's largely based upon some basic factors such as the version of Windows they're using, as well as their Internet and e-mail habits. In the computer world as well as in the biological world, good hygiene goes a long way in preventing infection in the first place — and prevention is far easier to deal with than curing an infection after it happens.

Assessing the Threat to Your Computer

Three primary factors contribute to your risk of catching viruses:

- ✓ The version of the Windows operating system you are using
- ✓ Whether you have installed security patches on your computer
- ✓ How many people use the computer

But also important are your Internet browsing habits:

- ✓ Do you visit many different Web sites?
- ✓ Do you visit sites that try to mess with your computer's settings (and how would you know — and prevent — that)?
- ✓ Do you have a tendency to open e-mail attachments from people you don't know?
- ✓ Do you visit Web sites cited in e-mail messages from strangers?

All these factors have a direct bearing on whether you are prone to catching viruses.

Finally, the manner in which your computer is connected to the Internet determines your susceptibility to viruses. If you have a high-speed, “always-on” Internet connection, then virus writers are actively trying to find you (or already have!). Dial-up connections are *somewhat* less risky — but not risk-free.

Which operating system are you using?

Microsoft's earlier versions of Windows had very little in the way of security — they conformed to Microsoft's earlier (and flawed) premise that everyone in corporations and everyone

on the Internet is nice and can be trusted and that no one will do anything bad. Microsoft, by the way, has been humbled by the experience and, as a result, the newer versions of Windows are far more secure than their predecessors.

Windows 95 and Windows 98

Collectively known as Windows 9x, these earlier versions of Windows lack the basic security components found in modern operating systems. Their primary fault is that they don't separate the function of the operating system from the person who uses it. You, the computer's user, have complete control over every aspect of the computer. Even back in the '90s that wasn't too safe; if you catch a virus, *the virus has the same range of control over your computer as you do.*

Microsoft no longer supports Windows 95. This means that, if any security vulnerability is discovered in Windows 95, Microsoft will not issue bulletins, advice, or security patches to fix it. Not an enviable position for any user to be in.

In 2003, Microsoft announced that it would soon end support for Windows 98. But when thousands of corporate and individual computer users stormed the Microsoft castle in Redmond, Washington, armed with torches, spears, axes, and old dot-matrix printers, Microsoft relented and postponed the Windows 98 "end of life."

But for users of Windows 98, the message is clear: Your days of support from Microsoft are growing short.

Windows ME

Officially called Windows Millennium Edition or Windows ME (and playfully referred to in some circles as the Windows Miserable Edition), this is just Windows 98 with some additional features thrown in and some stability improvements. The stability improvements come at the price of higher hardware requirements, however, and Windows ME suffers from the same basic security issues as its predecessors, namely that viruses can run roughshod throughout the unprotected operating system.

Windows 2000

At long last, Microsoft had taken the kernel (insides) of Windows NT and grafted on the Windows 98 *user interface*

(the stuff that you see on-screen when you use it), and after exhausting the world's supply of duct tape and baling wire, made it work.

Windows 2000 is a very decent operating system. It contains most of the security features that corporate customers and consumers had been requesting for a long time. Primary is the notion of “logging on” to the computer. In Windows 2000 and newer versions of Windows, if you can't log on to the computer, you can't use it. Contrast that to Windows 9x — if you can make the computer run, you can use it and do anything you want to it.

Windows XP

Windows XP contains many refinements over Windows 2000 and is even more secure. For the most part, Windows XP is an improved version of Windows 2000 and includes additional features and functions.

I've heard some say that Windows XP is just Windows 2000 with the soft, friendly interface. If you haven't seen Windows XP, it's like Windows 2000 with brighter colors and smooth, rounded corners.

Do you install security patches?

Microsoft regularly releases *security patches* — fixes to their software — that close security holes that could lead to virus infections. Many of these patches are deemed “critical,” and a good number of them have been exploited by those chip-on-their-shoulder Internet thugs who have nothing better to do than to spread misery to as many people as possible.

Microsoft has provided a number of ways that you can use to find out about and install security patches, including Windows Update, Automatic Update, and e-mail notifications of new patches.

If you *do* install the critical patches that Microsoft releases, then you're in far better shape than if you have no security patches at all. Having no security patches is almost as bad as having no antivirus software: You're up the creek with a sitting duck.

I don't want you to feel bad if you're among (what I suspect is) the majority of computer users — those who have never installed security patches. Had I chosen a different career path without much chance to get familiar with computers, the thought of installing security patches would seem about as intimidating as working on my home's electrical wiring or working on a late-model automobile with all its complex wiring and safety systems. But that's what this book is for: to help get you past the reluctance.

How many people use the computer?

Are you the only person who uses your computer? Or are several colleagues, family members, or (gasp!) total strangers using your computer, like so many people sharing a germ-infested bathroom water cup?

The greater the number of people using a computer, the greater the chances are that something bad will happen. How do I know this? When several people share a complex machine like a PC, the inconsistencies in the ways that the people use the computer, and the accumulation of every user's bad habits and mistakes, can make the computer's condition deteriorate over time.

How is your computer connected to the Internet?

While there are many ways to connect to the Internet, I'm concerned with just one factor: Is your computer "always on and connected" through any sort of a *broadband* (high-speed) connection like DSL, a cable modem, ISDN, or satellite? Or do you use a dial-up (phone-line) connection to connect your computer to the Internet, get your e-mail, do a little surfing, and then disconnect?

It boils down to this: Is your computer *always on* and *always connected* to the Internet? If so, then your computer is far more likely to be targeted by Internet worms. Some hackers like to scan for — and find — new always-on computers.

They're looking for recruits — to see whether they can add your system to their legion of slave computers.



Let me explain this high-speed, always-on thing a little more. If your computer is connected to the Internet using a high-speed connection, then your computer is *statistically* more likely to be found by a scan than it would be if it were connected, say, only one or two hours per day. Statistically speaking, an always-on computer is ten times more likely to be scanned, because it's connected ten times as many hours per day. But more than that, if your computer is always on and always connected, then hackers would consider your computer more dependable. And because the connection is higher speed than dial-up, they can get more performance out of your computer for their own evil purposes.

Do you have a firewall?

A firewall, as I explain more fully in Chapter 10, is something that is designed to block the probing scans that are often associated with viruses, worms, and Trojan horses. Those people who have installed either a software firewall or a hardware firewall have far better protection than people who have neither.

A *software firewall* is a program that runs on your computer, invisibly (in the background), much like an antivirus program. The software firewall program carefully watches all communication coming into your computer and leaving your computer. Each network message — or *packet* — is examined to ascertain its type, origin, and destination. These properties are then compared to a list of rules to determine whether each packet should be allowed to pass through or not. Should the message be allowed to pass, the firewall lets it move along towards its destination. But should the message be blocked, then the firewall will not permit it to pass — and it will fail to reach its destination, like a postal letter that is intercepted in transit and simply thrown away.

A *hardware firewall* is an electronic appliance that is installed on a network. Its internal function is essentially similar to the software firewall, except that its protection is more centralized: All the computers on the network are protected by the hardware firewall, so none of the bad traffic on the Internet is permitted to reach any of the computers on the network.

The legion of zombies

Many of the viruses, worms, and Trojan horses that have been released in recent years have a single, diabolical purpose — to identify and “take over” those so-called always-on and always-connected computers that are typically connected to the Internet using high-speed DSL, cable modem, ISDN, or satellite connections.

A recent study estimates that fully *one-third* of all such computers have *backdoors* (programs that allow hackers to bypass all security) installed on them and are used for a variety of purposes — generally for transmitting spam (unwanted junk) e-mail or for participating in massive distributed denial of service (DDoS) attacks.

A *distributed denial of service* (DDoS) attack is one where a hacker, after enlisting hundreds or thousands of computers with his backdoor program, sends a command to “his” (your) computer, instructing it (and many, many others) to begin flooding some particular Web site with as many network messages as possible. The victim’s Web site would then be receiving millions of network messages from hundreds or thousands of computers located all over the world and be nearly powerless to stop it (because of the vast number of sources of the attack). As a result, the victim’s Web site would, for all

practical purposes, be “off the air” for as long as the attack continued.

This is no pipe dream or theoretical missive. Such attacks are commonplace. Major corporations, organizations, and governments, such as Microsoft, SCO, Yahoo!, E-Trade, the U.S. Whitehouse, and some countries’ government or news sites, have been victims of DDoS attacks lasting hours or days. And unless that corporation is both clever and resourceful, the corporation’s Web site is essentially unreachable for all legitimate use until the attack ceases.

Home users — even those who are IT professionals by day — would likely have no reason to suspect that their home PCs have been taken over. Generally speaking, hackers have designed their backdoors to minimize the likelihood of being detected. They use a measured, limited portion of your computer’s resources so you can continue to use your computer for whatever you do with it. At the same time, however, your computer would also be used to relay and transmit spam to hundreds or thousands of other unsuspecting people (and many of *those* spam messages may contain their own viruses, worms, or Trojan horses to enlist even more unsuspecting and poorly-protected computers). Your computer could be the modern version of the zombies in *Night of the Living Dead*.

A firewall is like a security guard at the entrance of an office building. He (or she) scrutinizes each person coming and going. He may want to look at each person's identification by examining their employee badge or other credential. If the person coming or going is carrying anything, he may ask questions about it. If the person is a guest, the guard may request that the user sign their name into a visitor's log.

The guard has a list of rules that he uses to determine whether each person coming and going will be permitted to pass through. Occasionally he will need to turn someone away, for one reason or another. He will detail each such denial so his boss can later view who was denied access and why.

Occasionally, the guard will need to call his boss and ask if a visitor is permitted to pass through (in a firewall software program, this takes the form of a pop-up window that asks if a particular program should be permitted to communicate or not).

High-risk activities

The types of activities performed on your PC also contribute to your risk, whether high or low. Each of these activities is related to how social you permit your computer to be. Do you often take it out in public where it can exchange information with other computers? In the analogy between biological viruses and computer viruses, a high degree of *socialization* (mingling with others) increases risk. The following sections look at some examples.

Wireless "Hot Spots"

Hoping to attract well-to-do customers, many public establishments — such as coffee houses, restaurants, and other businesses — have installed so-called Internet *hot spots*. These hot spots are Internet connections that a customer can use to connect to the Internet with a laptop computer, provided it's equipped with a wireless networking (also called Wi-Fi or 802.11) capability. Some establishments charge a fee for the use of their hot spots; others permit use free of charge.

People who own laptops equipped with those Wi-Fi connections can visit any of the hundreds of thousands (or perhaps millions) of Wi-Fi-equipped establishments and access the Internet to retrieve e-mail, visit Web sites, or whatever they do

on the Internet. At a coffeehouse, for instance, you would purchase your tall double-shot vanilla low-fat latte and then sit down at one of the tables, turn on your laptop, and catch up on e-mail while quaffing your favorite coffee drink.

But here's the problem: These hot-spot connections have many of the same risks that are associated with always-on high-speed connections. Hackers and worms frequently scan the wireless networks in these establishments, hoping to find new victims — like, for instance, your computer. Computers lacking adequate antivirus protection fall victim to the worm and become one of those zombie computers, awaiting the commands from their fiendish master.

Downloading and file sharing

If you or someone with access to your computer is doing a lot of file and program downloading and file sharing with others, chances are that sooner or later one of the files you download will be infected with a virus.

Because many viruses travel from computer to computer by hiding inside of software program files, it makes sense that the more program files you bring into your system, the more likely it will be that one of them will have a virus. Also, program files that have been copied from other computers (rather than coming directly from the manufacturer) have a *much* greater chance of being infected with a virus.

Instant messaging

If you are an Instant Messaging (IM) user, you are increasing your chances of catching a virus (or, of course a worm, Trojan, or other ill fate). As the popularity of IM rises, so too does this get the attention of virus writers looking for new ways to get viruses from one computer to another. Already, there have been a number of worms that have propagated themselves using IM. Every day, minute by minute, you can be sure that there will have been more such incidents.

Add-on programs

If you are the type who can't resist an online or computer store bargain, sooner or later something you pick up will have a little extra feature. While it doesn't happen often, viruses have been known to sneak onto the *gold* (or final) version of a software manufacturer's CD-ROM or online download area.

How many viruses are there?

Tens of thousands of viruses, worms, and Trojan horses have been developed and released onto the Internet over the past two decades. On the day that I am writing this section, my own PC's antivirus program shows over 66,000 known viruses in its list.

In the first half of 2003 alone, 3,855 new viruses were introduced. That is over 21 new viruses each and every day.

Nearly all new viruses are targeted at Microsoft products, including Windows, Outlook, and Office.

And remember — virus writers like to get their viruses to propagate in large numbers. That means, some spend considerable time trying to get their wares into programs that will be mass-marketed or mass-distributed.

Sharing your e-mail address with too many other people and organizations

Persons who have a habit of signing up for things on the Internet are far more likely to end up on one or more spammers' lists. Or if you are the type of person whose e-mail address is "in circulation" — meaning your e-mail address appears online in Web sites, chat rooms, mailing lists, newsgroups, and so forth — then the chances improve that your e-mail address will be picked up and wind up in the hands of one or more mass marketers. As soon as this happens, one or more of the spammers who like to send large volumes (we're talking *millions*) of virus-laden e-mail messages will take advantage of the target you've given them.

This is not unlike giving out your phone number to lots of different people and organizations, only to discover that you are beginning to receive far more unwanted phone calls than before. So it is with e-mail. It's the fastest possible way to infest your once-pristine inbox with more unwanted mail than legitimate mail.

In my case, about *three-fourths* of all the e-mail I receive is spam. My e-mail address appears in my online column in

ComputerWorld. Of course, the address I use there is different from any I use anywhere else — and it isn't hard to see why: Soon after I started writing my column, I began to receive additional spam, much of it sent to that unique address. This occurs because some spammers have *spider* programs that run all over the Web in search of e-mail addresses to harvest from Web sites.

Deciding How Much Security Is Enough

Without getting too scientific about it, the best way to think about “how much security is enough” is to compare the value of the possession you are trying to protect against the level of effort you're willing to expend to protect it.

Let me illustrate with a simple example. Would you protect a \$1,000 automobile with a \$2,000 alarm system? Not likely, because it isn't proportional.

Like shoes and bathing suits, one size does not fit all people and all needs. And so it is with computers. Depending on what you do with your computer, you will need to spend a particular level of effort in order to protect the information on your computer and the ability to continue performing whatever activities you use it for.

For example, a casual user sends and receives e-mail and surfs the Internet. But someone else uses their computer to make their living: Perhaps they use their computer to build Web sites, do financial accounting for small businesses, or write *For Dummies* books. The latter user has a lot more to lose if something goes wrong with his or her computer, than does the casual user, who is merely inconvenienced.

Take a look at three somewhat arbitrary levels of security in Table 1-1. Each one also represents a level of value, and I include examples of how often particular security activities should take place.

Table 1-1		Levels of Security	
<i>Typical Uses</i>	<i>Low</i>	<i>Medium</i>	<i>High</i>
	Casual e-mail, computer games, Web-surfing	Family or business correspondence, online bill payment	Small business accounting, writer of <i>For Dummies</i> books
Virus scans	Monthly	Weekly	Daily
Virus updates	Weekly	Daily	Hourly
Risk tolerance	High	Medium	Low
Backups	Infrequent	Weekly	Daily

You can see in these examples that the higher-value systems deserve more elaborate protection. If you think about it, a high-value system is helping its owner to derive income or some other economic value, or pursue some other form of value that the user feels personally invested in. Given the risks associated with online computing, it makes sense to protect systems associated with economic (or other) value more than systems that were little more than hobbyist-level systems.