CHAPTER 1

Understanding Computer Viruses

You've heard about them. You've read the news reports about the number of incidents reported, and the amount of damage they inflict. Maybe you've even experienced one firsthand. And if you haven't, count yourself fortunate.

Computer viruses are real—and they're costly.

Springing up seemingly from nowhere, spreading like wildfire, computer viruses attack computer systems large and small, damaging files and rendering computers and networks unusable. They proliferate through e-mail, Internet file downloads, and shared diskettes. And they don't play favorites; your home computer is just as likely as a Fortune 500 company's network to experience an infection.

This first section of the book is about protecting your computer from these destructive virus programs. Read this chapter to learn more about the background of computer viruses; then proceed to the following chapters to learn how to avoid and recover from specific types of virus attacks.

The Dangers of Computer Viruses

Not a month goes by without another big-time virus scare.

Tens of millions of computers are infected by computer viruses every year. In 2001, 2.3 million computers were infected by the SirCam virus, and another million computers were hit by CodeRed. Even worse, the LoveLetter virus hit an estimated 45 million computers—on a single day in 2000.

ICSA Labs (`www.icsalabs.com`), a leading provider of security research, intelligence, and certification, found that the rate of virus infection in North America in 2001 was 113 infections per 1000 computers—meaning that more than 10% of all computers they surveyed had been hit by a virus. And this rate is increasing; ICSA says that the likelihood of contracting a computer virus has doubled for each of the past five years.

Viruses hit the corporate world especially hard; a single infected computer can spread the virus among the entire corporate network. McAfee.com (`www.mcafee.com`), a company specializing in virus protection, estimates that two-third of U.S. companies are attacked by viruses each year. A third of those companies reported that viruses knocked out their servers for an average of 5.8 hours per infection, and 46% of the companies required more than 19 days to completely recover from the virus incident.

These incidents come with a heavy cost. The research firm Computer Economics (`www.computereconomics.com`) estimates that companies spent $10.7 billion to recover from virus attacks in 2001. Technology magazine *The Industry Standard* (`www.thestandard.com`) puts the cost much higher, at upwards of $266 billion. Whatever the real number, it's clear that computer viruses are costly to all concerned—in terms of both money and the time required to clean up after them.

Just look at the costs inflicted by individual viruses. For example, Computer Economics estimates that the Nimda virus alone cost companies $590 million in cleanup costs; CodeRed and LoveLetter were even more costly, running up costs of $2.6 billion apiece.

To an individual company, these costs can be staggering. ICSA Labs estimates that virus cleanup costs large companies anywhere from $100,000 to $1 million each per year.

That's real money.

Unfortunately, this problem doesn't look like it's going to go away. In fact, the problem just keeps getting worse. To date, more than 53,000 different viruses have been identified and catalogued—with another half-dozen or so appearing *every day*.

Just what is it about computer viruses that makes them so deadly—and so easily spread?

How Computer Viruses Work

As you'll see in the next section, the term *virus* was applied to this type of software very early in its history. It's an apt metaphor, because a computer virus is, in many ways, similar to the biological viruses that attack human bodies.

A biological virus isn't truly a living, independent entity; as biologists will tell you, a virus is nothing more than a fragment of DNA sheathed in a protective jacket. It reproduces by injecting its DNA into a host cell. The DNA then uses the host cell's normal mechanisms to reproduce itself.

A computer virus is like a biological virus in that it also isn't an independent entity; it must piggyback on a host (another program or document) in order to propagate.

Many viruses are hidden in the code of legitimate software programs—programs that have been "infected," that is. These viruses are called *file infector viruses*, and when the host program is launched, the code for the virus is also executed, and the virus loads itself into your computer's memory. From there, the virus code searches for other programs on your system that it can infect; if it finds one, it adds its code to the new program, which, now infected, can be used to infect other computers.

This entire process is shown in Figure 1.1.

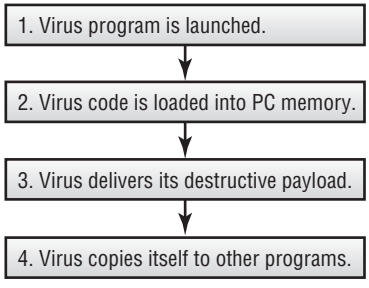

Figure 1.1 *How a virus infects your computer*

If all a virus did was copy itself to additional programs and computers, there would be little harm done, save for having all our programs get slightly larger (thanks to the virus code). Unfortunately, most viruses not only replicate themselves, they also perform other operations—many of which are wholly destructive. A virus might, for example, delete certain files on your computer. It might overwrite the boot sector of your hard disk, making the disk inaccessible. It might write messages on your screen, or cause your system to emit rude noises. It might also hijack your e-mail program and use the program to send itself to all your friends and colleagues, thus replicating itself to a large number of PCs.

Viruses that replicate themselves via e-mail or over a computer network cause the subsidiary problem of increasing the amount of Internet and network traffic. These fast-replicating viruses—called *worms*—can completely overload a company network, shutting down servers and forcing tens of thousands of users offline. While no individual machines might be damaged, this type of communications disruption can be quite costly.

As you might suspect, most viruses are designed to deliver their payload when they're first executed. However, some viruses won't attack until specifically prompted, typically on a predetermined date or day of the week. They stay on your system, hidden from sight like a sleeper agent in a spy novel, until they're awoken on a specific date; then they go about the work they were programmed to do.

In short, viruses are nasty little bits of computer code, designed to inflict as much damage as possible, and to spread to as many computers as possible—a particularly vicious combination.

The History of Computer Viruses

Where, exactly, do computer viruses come from? To answer that question, it's helpful to examine the history of computer viruses.

Technically, the concept of a computer virus was first imagined in 1949, well before computers became commonplace. In that year, computer pioneer John von Neumann wrote a paper titled "Theory and Organization of Complicated Automata." In this paper, von Neumann postulated that a computer program could be self-replicating—and thus predicted today's self-replicating virus programs.

The theories of von Neumann came to life in the 1950s, at Bell Labs. Programmers there developed a game called "Core Wars," where two players would unleash software "organisms" into the mainframe computer, and watch as the competing programs would vie for control of the machine—just as viruses do today.

In the real world, computer viruses came to the fore in the early 1980s, coincident with the rise of the very first personal computers. These early viruses were typically spread by users sharing programs and documents on floppy disks; a shared floppy was the perfect medium for spreading virus files.

The first virus "in the wild," as they say, infected Apple II floppy disk in 1981. The virus went by the name of Elk Cloner, and didn't do any real damage; all it did was display a short rhyme onscreen:

```
It will get on all your disks

It will infiltrate your chips

Yes it's Cloner!


It will stick to you like glue

It will modify ram too

Send in the Cloner!
```

At the time, Elk Cloner wasn't identified as a virus, because the phrase "computer virus" had yet to be coined. That happened in 1983, when programmer Len Adleman designed and demonstrated the first experimental virus on a VAX 11/750 computer. From Adleman's lab to the real world was but a short step.

In 1986, the Brain virus became the first documented file infector virus for MS-DOS computers. That same year, the first PC-based Trojan horse was released, disguised as the then-popular shareware program PC Write.

From there, things only went downhill, with the popularity of computer bulletin board services (BBSs) helping to spread viruses beyond what was previously physically possible. BBSs were the online precursors to the Internet; users could use their low-speed modems to dial into public and private BBSs, both to exchange messages and to download files. As any Monday-morning quarterback could predict, there were viruses hiding among the standard utilities and applications that users downloaded, thus facilitating the spread of those viruses.

To make things worse, in 1990 the first BBS specifically for virus writers was created. This virus exchange BBS, housed on a computer in Bulgaria, provided a means for virus writers to exchange virus code and learn new tricks.

Computer viruses hit the big time in 1992, when the Michelangelo virus hit. Michelangelo was one of the first viruses to spread worldwide, and garnered much media attention. Fortunately, its bark was worse than its bite, and little actual damage occurred.

NOTE *Michelangelo was more of a virus scare than a virus threat. In the days building up to Michelangelo's threatened March 6 delivery date, news stories worldwide projected that millions of computers would have their hard disks destroyed. In reality, fewer than 20,000 computers were hit, but—thanks to all the publicity—the world was forever made aware of the perils posed by computer viruses.*

The year 1996 saw the first virus designed specifically for Windows 95 and the first macro viruses for Word and Excel files. That year also saw the first virus for the Linux operating system.

By 1999, viruses had become almost mainstream. The Melissa virus, released that year, was a combination macro virus and worm that spread itself by e-mailing contacts in a user's Outlook or Outlook Express Address Book. Melissa did untold amounts of damage to computers and company networks around the world, and was followed (in 2000) by the LoveLetter worm (also known as the "Love Bug"), which shut down tens of thousands of corporate e-mail systems. Since then, viruses have continued to proliferate and mutate, with viruses being developed for personal digital assistants (PDAs), file-swapping networks, instant messaging systems, and more.

And the chaos continues.

Different Types of Viruses

Technically, a computer virus is a piece of software that surreptitiously attaches itself to other programs and then does something unexpected. There are other types of programs—such as Trojan horses and worms—that do similar damage but don't embed themselves within other program code. These programs aren't technically viruses, but they pose the same danger to computer systems everywhere. For that reason, all these programs—virus and non-virus, alike—are typically lumped together and referred to, in common parlance, as viruses. (Or, as some experts prefer, *malware*—for "malicious software.") The following chapters will examine all these different types of malicious programs, since the best defense against one is a defense against all.

That's not to say that all malicious programs work the same way, or pack the same potential punch. They don't. So it helps to know a little bit about each type of virus, to help better protect against them.

> **NOTE** *Some viruses—called* hybrid viruses*—include aspects of more than one virus type. An example would be a worm that can infect program files, such as the Hybris virus. This sometimes makes it difficult to precisely classify a virus—and, in fact, many viruses fall into more than one category.*

File Infector Viruses

The most "traditional" form of computer virus is the file infector virus, which hides within the code of another program. The infected program can be a business application, a utility, or even a game—just as long as it's an executable program, typically with an `EXE`, `COM`, `SYS`, `BAT`, or `PIF` extension.

When an infected program is launched, the virus code copies itself into your computer's memory, typically before the program code is loaded. By loading itself into memory separately from the host program, the virus can continue to run in your system's memory, even after the host program is closed down.

Before the advent of the Internet and coincident creation of macro viruses, file infector viruses accounted for probably 85% of all virus infections. Today that number is much lower, because the other types of viruses are much easier to propagate.

NOTE *Learn more about file infector viruses in Chapter 3, "Boot Sector and File Infector Viruses."*

Boot Sector Viruses

Boot sector viruses reside in the part of the disk that is read into memory and executed when your computer first boots up. (On a floppy disk, that's the *boot sector;* on a hard disk, the equivalent area is called the *Master Boot Record.*) Once loaded, the virus can then infect any other disk used by the computer; a disk-based boot sector virus can also infect a PC's hard disk.

Most boot sector viruses were spread by floppy disk, especially in the days before hard disks were common. Since removable disks are less widely used today, boot sector viruses have become much less prevalent than they were in the early 1990s.

TIP *Learn more about boot sector viruses in Chapter 3.*

Macro Viruses

Some computer viruses are created with the *macro* coding languages used with many of today's software applications. Macros are small programs that are created to do highly specific tasks within an application and are written in a pseudo-programming language designed to work with the application. The most common macro language, used in all Microsoft applications, is called Visual Basic for Applications (VBA). VBA code can be added to a Word document to create custom menus and perform automatic operations; unfortunately, VBA code can also be used to modify files and send unwanted e-mail messages, which is where the virus writers come in.

What makes macro viruses potentially more dangerous than file infector or boot sector viruses is that macros—and thus macro viruses—can be attached to document files. Older virus types had to be embedded in executable programs, which made them relatively easy to find and stop. But when any Word or Excel document you open could contain a macro virus, the world is suddenly a much more dangerous place.

The widespread, relatively nonchalant sharing of data files has contributed to the huge rise in macro virus attacks. Even users who are extra-vigilant about the programs they download often don't think twice about opening a Word or Excel document they receive from another user. Because data files are shared so freely, macro viruses are able to spread rapidly from one machine to another—and run, automatically, whenever the infected document is opened.

NOTE *Learn more about macro viruses in Chapter 4, "Macro Viruses."*

Script Viruses

Script viruses are based on common scripting languages, which are macro-like pseudo-programming languages typically used on Web sites and in some computer applications. These viruses are written into JavaScript, ActiveX, and Java applets, which often run automatically when you visit a Web page or open a Word or Excel application. With the increasing use of the Web, these script viruses are becoming more common—and more deadly.

NOTE *Learn more about these ActiveX, JavaScript, and Java viruses in Chapter 5, "Script Viruses."*

Trojan Horses

A *Trojan horse* is a program that claims to do one thing but then does something totally different. A typical Trojan horse has a filename that makes you think it's a harmless type of file; it looks innocuous enough to be safe to open. But when you run the file, it's actually a virus program that proceeds to inflict its damage on your system. It delivers its payload through deception, just like the fabled Trojan horse of yore.

Trojan horses are becoming more common, primarily through the spread of Internet-based e-mail. These e-mail Trojans spread as innocent-looking attachments to e-mail messages; when you click to open the attachment, you launch the virus.

NOTE *Learn more about Trojan horses in Chapter 6, "Trojan Horses and Worms."*

Worms

A *worm* is a program that scans a company's network, or the Internet, for another computer that has a specific security hole. It copies itself to the new machine (through the security hole), and

then starts replicating itself there. Worms replicate themselves very quickly; a network infected with a worm can be brought to its knees within a matter of hours.

Worms don't even have to be delivered via conventional programs; so-called "fileless" worms are recent additions to the virus scene. While in operation, these programs exist only in system memory, making them harder to identify than conventional file-hosted worms. These worms—such as the CodeRed and CodeBlue viruses—could cause considerable havoc in the future.

NOTE *Learn more about worms in Chapter 6.*

E-Mail Viruses

An *e-mail virus* is a program that is distributed as an attachment to an e-mail message. These viruses are typically separate programs (Trojan horses, mainly) that do their damage when they're manually executed by you, the user. These viruses masquerade as pictures, Word files, and other common attachments, but are really EXE, VBS, PIF, and other types of executable files in disguise. Many e-mail viruses hijack your e-mail program and send themselves out to all the contacts in your address book.

Because of the proliferation of the Internet, e-mail is the fastest-growing medium for virus delivery today. According to Kaspersky Lab, the research arm of the company that produces Kaspersky Anti-Virus software, e-mail viruses accounted for 90% of all virus attacks in 2001.

NOTE *Learn more about e-mail viruses in Chapter 7, "E-Mail, Chat, and Instant Messaging Viruses."*

Chat and Instant Messaging Viruses

Many computer users like to chat online, either in public chat rooms or in private instant messaging (IM) conversations. Most chat and IM programs let you send files across to other users, and it's that capability that has contributed to the spread of so-called "instant" viruses.

Just as many users are in the habit of automatically opening all attachments to their incoming e-mail messages, many users are also accustomed to accepting any files sent to them when they're chatting. Unfortunately, a significant percentage of files sent via chat or IM are virus files, often Trojan horses masquerading as photographs or helpful utilities. Downloading and then opening one of these files begins the infection process.

NOTE *Learn more about these "instant" viruses in Chapter 7.*

Today's Top Viruses

With so many different types of viruses out there, what are the most widespread computer viruses today?

Unfortunately, that's a bit of a trick question. That's because most viruses have a defined and relatively short life cycle; they appear on the scene with a bang, doing considerable damage, but then—as protective methods are employed—just as quickly disappear from the radar scope. So the top viruses as I'm writing this chapter will be much different from the top viruses when you're reading it a few months from now.

(Figure 1.2 illustrates the typical virus life cycle, from creation to eradication.)

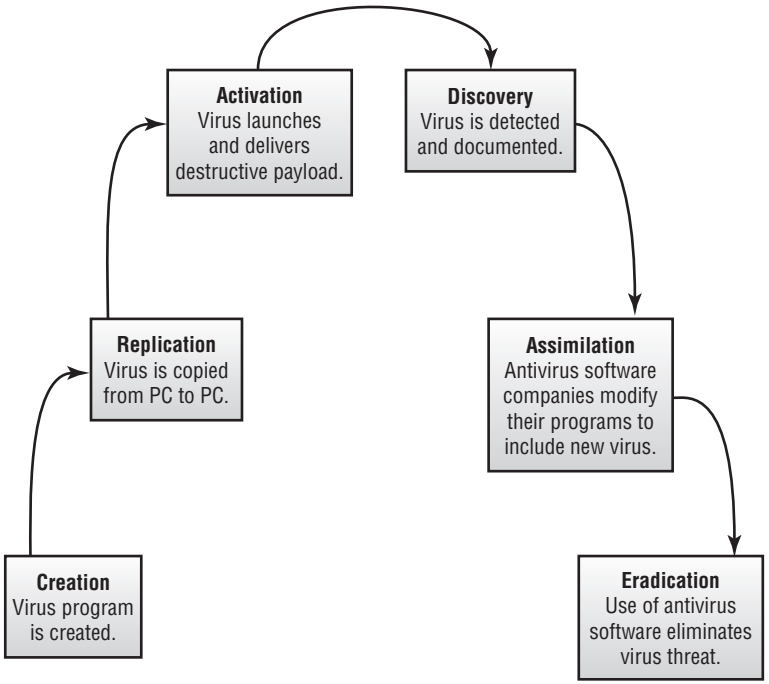

Figure 1.2 *The life cycle of a computer virus*

You can see this phenomenon for yourself by comparing two different virus "Top Ten Lists." Both lists were compiled by Kaspersky Lab. Table 1.1 details the ten most widespread viruses for the last quarter of 2001, along with the percentage of the total number of infections that each virus represents:

Table 1.1 *Top Ten Viruses for Q4 2001*

Ranking	Virus	Percentage of Occurrence
1	Badtrans	37.0%
2	SirCam	15.4%
3	Hybris	6.2%
4	Aliz	3.0%
5	Nimda	2.5%
6	Magistr	2.2%
7	GIP	1.8%
8	Happytime	0.5%
9	Klez	0.3%
10	Seeker	0.3%

The second list, in Table 1.2, presents the situation two months later, for the month of February 2002:

Table 1.2 *Top Ten Viruses for February 2002*

Ranking	Virus	Percentage of Occurrence
1	Klez	61.5%
2	Badtrans	28.5%
3	SirCam	1.5%
4	Hybris	1.4%
5	Aliz	1.2%
6	Magistr	0.7%
7	CodeRed	0.6%
8	Thus	0.4%
9	Petik	0.4%
10	Death	0.3%

NOTE *View more current virus lists from Kaspersky Lab at* `www.viruslist.com`.

As you can see, the big virus in September–December was Badtrans (accounting for 37% of infections), and it was still pretty big in February (28.5%). But the really big virus in February was Klez (61.5%), which accounted for just 0.3% of occurrences just two months earlier. It came out of nowhere to be a major presence—but by the time you read this book, it probably won't be around at all.

The other trend you can see in these charts is that when a virus hits, it really hits. Witness the Klez worm accounting for almost two-thirds of all virus infections in February 2002. This shows just how fast and how far a virus can spread. In fact, most major virus attacks reach their peak within a single week, or less. These viruses use the Internet to propagate across multiple computers, as fast as e-mail messages can be delivered.

It's scary how fast these viruses can spread—and how much damage they can do.

Why Viruses Exist

Computer viruses, unlike biological viruses, don't spring up out of nowhere—they're created. By people.

And the people—programmers and developers, typically—who create computer viruses know what they're doing. These code writers deliberately create programs that they know will wreak havoc on huge numbers of computer users.

The question is *why*?

It takes some degree of technical skill to create a virus. To that end, creating a computer virus is no different than creating any other computer application. Any computer programmer or developer with a minimal amount of skill can create a virus—all it takes is knowledge of a programming language, such as C, Visual Basic, or Java, or a macro language, such as VBA.

NOTE *In reality, you can create a virus even if you have very little technical knowledge, by using a "build your own virus" program—of which there are several available, via the Internet underground.*

So, by definition, a virus writer is a person with a certain amount of technical expertise. But instead of using that expertise productively, virus writers use it to generate indiscriminate mayhem among other computer users.

This havoc-wreaking is, in almost all instances, deliberate. Virus writers *intend* to be destructive. They get some sort of kick out of causing as much damage as possible, from the relative anonymity of their computer keyboards.

In addition, some developers create viruses to prove their technical prowess. Among certain developers, writing a "successful" virus provides a kind of bragging right, and demonstrates, in some warped fashion, that the writer is especially skilled.

Unfortunately, the one attribute that virus writers apparently lack is ethical sense. Virus programs can be enormously destructive, and it takes a peculiar lack of ethics to deliberately perpetrate such destruction on such a wide scale.

In the end, a virus writer is no better than a common vandal. Except for the technical expertise required, the difference between throwing a rock through a window and destroying PC files via a virus is minimal. Some people find pleasure in destruction, and in our high-tech age, such pleasure can come from writing destructive virus code.

What You Can Do About Computer Viruses

There's very little you can do, on a personal level, to discourage those high-tech vandals who create virus programs. There are plenty of laws already on the books that can be used to prosecute these criminals, and such criminal investigations—and prosecutions—have become more common in recent years. However, as with most criminal activity, the presence of laws doesn't always mean there are fewer criminals; the truth is, there's a new batch of virus writers coming online every day.

All of which means that you can't rely on anyone else to protect you from these virus-writing criminals. Ultimately, you have to protect yourself.

The next 11 chapters go into more detail about the specific types of viruses, and they offer detailed instructions about protecting yourself from those viruses. In general, however, there are some simple steps you can take to reduce your chances of becoming a virus-related statistic.

Reducing Your Chances of Infection

To make yourself less of a target for virus infection, take the following steps:

Restrict your file downloading to known or secure sources. The surest way to catch a virus is to download an unknown file from an unknown site; try not to put yourself at risk like this unless you absolutely have to.

Don't open any e-mail attachments you weren't expecting. The majority of viruses today arrive in your mailbox as attachments to e-mail messages; resist the temptation to open or view every file attachment you receive.

Use an up-to-date anti-virus program or service. Antivirus programs work; they scan the files on your computer (as well as new files you download, and e-mail messages you receive) and check for any previously identified viruses. They're a good first line of defense, as long as you keep the programs up-to-date with information about the very latest viruses—and most antivirus programs make it easy to download updates.

Enable macro virus protection in all your applications. Most current Microsoft applications include special features that keep the program from running unknown macros—and thus prevent your system from being infected by macro viruses.

Create backup copies of all your important data. If worse comes to worst and your entire system is infected, you may need to revert to noninfected versions of your most critical files. You can't do this unless you plan ahead and back up your important data.

NOTE *Learn more about protecting your system from virus attacks in Chapter 11, "Preventing Virus Attacks."*

Diagnosing a Virus Infection

How do you know if your computer has been infected with a virus? In short, if it starts acting funny—doing anything it didn't do before—then a probable cause is some sort of computer virus. Here are some symptoms to watch for:

- Programs quit working or freeze up.
- Documents become inaccessible.
- Computer freezes up or won't start properly.
- The CAPS LOCK key quits working—or works intermittently.
- Files increase in size.
- Frequent error messages appear onscreen.
- Strange messages or pictures appear onscreen.
- Your PC emits strange sounds.
- Friends and colleagues inform you that they've received strange e-mails from you, that you don't remember sending.

NOTE *Learn more about diagnosing virus attacks in Chapter 2, "How to Catch a Virus."*

Recovering from a Virus Attack

If you're unfortunate enough to be the victim of a virus attack, your options narrow. You have to find the infected files on your computer, and then either disinfect them (by removing the virus code) or delete them—hopefully before the virus has done any permanent damage to your system.

You don't, however, have to give up and throw your computer away. Almost all viruses can be recovered from—some quite easily. All you need is a little information, and the right tools.

The right tools include one of the major antivirus programs discussed in Chapter 9, "Anti-Virus Software and Services." These programs—such as Norton AntiVirus and McAfee VirusScan—identify infected files and then either disinfect or delete them, as appropriate.

Quite often, running an antivirus program is all you need to do to recover from a virus infection. However, if a virus has deleted or corrupted any document or program files on your PC, you'll probably have to restore those files from backup copies—or reinstall any damaged programs from their original CD-ROMs. In a worst-case scenario, where your operating system files have been affected, you may need to reinstall your entire operating system—or even, in some instances, reformat your hard disk and rebuild your entire system from scratch.

> **NOTE** *Learn more about recovering from a virus attack in Chapter 12, "Dealing with a Virus Attack."*

Learning More About Computer Viruses

Sometimes the best defense is a good education. To that end, there are several Internet-based resources you can use to learn more about computer viruses—how they work, and how to protect against them. Many of these sites also provide lists of the most menacing viruses, as well as alerts for newly created viruses.

Here are some of the best Web sites to visit:

- Computer Associates Virus Information Center (`www3.ca.com/virus/`)
- Computer Security Resource Center Virus Information (`csrc.ncsl.nist.gov/virus/`)
- F-Secure Security Information Center (`www.datafellows.com/virus-info/`)
- IBM Antivirus Research Project (`www.research.ibm.com/antivirus/`)
- McAfee AVERT (`www.mcafeeb2b.com/naicommon/avert/`)
- Sophos Virus Analyses (`www.sophos.com/virusinfo/analyses/`)
- Symantec Security Response (`www.symantec.com`)

- Trend Micro Virus Information Center (`www.antivirus.com/vinfo/`)
- Virus Bulletin (`www.virusbtn.com`)
- Viruslist.com (`www.viruslist.com`)
- The WildList Organization International (`www.wildlist.org`)

Summing Up

Computer viruses are malicious computer programs, designed to spread rapidly and deliver various types of destructive payloads to infected computers. Viruses have been around almost as long as computers themselves, and they account for untold billions of dollars of damage every year. While there are many different types of viruses, the best protection against them is to exhibit extreme caution when downloading files from the Internet and opening e-mail attachments—and to religiously avail yourself of one of the many antivirus software programs currently on the market.

Read on to learn more about specific types of computer viruses—and, in the next chapter, how to determine if you've been the victim of a virus attack.