

# Chapter 1

## The Spyware Menace

Addison-Wesley

---

Imagine what you would do if you turned on your computer one day and saw the following message pop up on your screen:

“Hi! I’m about to install a piece of software that will track the websites you go to and send that information to online retailers who want to send you lots of spam. While I’m at it, the software I’m about to install will send you about a dozen pop-up windows every time you try to open your web browser and will make your computer run as slow as a snail. If I’m in a particularly bad mood, then I’ll alter some files on your hard drive so that your machine won’t start up properly anymore.

Oh yes, one more thing: I’ll also collect your credit card information every time you check out at an online store and send your credit card numbers and personal information back to my nefarious maker.

If you’d like me to install this software, please click **Yes** so that I can start. If for some reason you’d rather I didn’t install this software, go ahead and click **No**, and I won’t bother you again.”

Now, if you saw a message like this, you'd click "No," right? Of course you would: if a piece of software as malicious as this one came right out and told you everything it was planning to do, there's no way you'd install it on your computer willingly. But what do you do if this piece of software *wasn't* polite enough to give you this kind of warning? What if this software installed itself automatically (and without your permission) just because you browsed to a particular website or downloaded a game that you like to play? I bet you'd call that annoying at best and downright dangerous at worst.

Unfortunately, this kind of software already exists on the Internet. It's called *spyware*, and it can install itself on your computer without you even being aware of it. You don't remember installing it, and that's probably because you actually *didn't*—it installed in the background while you were doing something else on the Internet. All you know is that you've got all these pop-up ads every time you turn on your PC, your computer is running slower or is just acting "weird," and your browser opens up to this strange web page that you don't remember visiting. It almost feels like it isn't your computer anymore, and in some ways it's not. Spyware has become fairly widespread, now that so many people have high-speed Internet access from their homes. Because your cable modem or DSL connection is always connected, it means that you're always "on the Internet," even if you're not actually browsing websites or checking your email. Spyware can use this always-on connection to display pop-up ads on your screen just about at will, and it can often do even worse things.

Luckily, there are a number of steps that you can take to protect yourself from this threat, even if your computer has already caught a bad case of spyware. From free tools that you can install to monitor for spyware and remove existing problems to simple tips and guidelines to make Internet browsing a safer experience, there are steps that you can take to minimize your exposure to spyware. In this book, I'll talk about some guidelines that you can follow to protect yourself, and I'll look at some free tools that you can use to clean up the clutter that spyware causes on your computer.

A few words on language before we get started: I'll use the words "PC," "personal computer," and "computer" fairly interchangeably throughout this book. I'm referring to the personal computer that you have sitting in your bedroom, your kid's room, or your home office. If you have a problem with a PC at work, I suggest that you talk to your company's IT people before installing any of the spyware removal tools that I'll be talking about. I say this because many companies have specific policies in place about what kinds of software you can install on your office PC, and they (hopefully) have their own procedures in place for dealing with spyware.

You'll also hear me talk about "spyware," "viruses," and "malicious software," or "malware" for short. I use the term "malicious software" to describe any kind of software that (1) you didn't install, and (2) tries to do something *bad* to your computer. Spyware is malicious software, and computer viruses also fit the bill. Spyware and computer viruses aren't quite the same thing, though, which we'll talk more about later in the book. I'm also going to assume that you're running some version of Microsoft Windows, and that you've been using the Internet Explorer browser, which comes pre-installed on Windows machines.

I'm also not going to be an alarmist and tell you that the Internet is this horrible place that's full of nothing but spyware, viruses, and spam. I *like* the Internet, and I like computers—I wouldn't be writing this if I didn't. Without the Internet, I'd have a much harder time researching the things I write about and use in my life as a computer consultant. The Internet is a great resource for anyone, just so long as you approach it with a certain amount of common sense. I try to think of the Internet as if it were a major city like Manhattan, London, or Berlin. That is to say, the majority of the people who live there are basically decent folks who are just going about their business and want to be left alone. The bad and even criminal element is there, for sure, but as long as you take a few precautions and don't needlessly expose yourself to risks, you can enjoy a stay on the Internet just as much as a trip to New York to see a Broadway show.

So, let's get started with a look at what spyware is and how you can protect yourself from it.

## I. What Is Spyware, and How Does It Get Installed on My Computer?

So, what exactly is spyware? And how can you recognize when it's been installed on your PC? Generally speaking, spyware refers to software that's been installed on your computer without your consent and that does things like collect your personal information without you being aware of it, change how your computer or web browser is configured, or bombard you with online advertisements. If a piece of spyware changes how your computer is configured, it will often lead to your computer becoming very slow or freezing, or even crashing with the dreaded "Blue Screen of Death." Spyware programs are notorious for being difficult to remove on your own, so even if you find an offending program and *uninstall* it, sometimes it will come right back whenever you reboot your computer.

The next obvious question is: how did these programs get installed on my computer to begin with? There are two common ways that you can find yourself infected with spyware. The first is that spyware can "hide" inside of other programs,

even ones that you download from websites that might be otherwise trustworthy. Here's a good example: you download a game from one of your favorite websites. After you download the game and click on "CoolGameSetup.exe," the game installs just like you wanted. But you also end up with additional software installed that you *didn't* want: a tiny program that tracks the websites you visit gets installed in the background, and you weren't even aware of it. Spyware programs will often "piggyback" in this way on top of games, MP3 players, and other software utilities—the manufacturer of the software will typically allow this spyware to be installed as a part of their product to drive more business to their website, for example.

A slightly less common (but much more dangerous) way for spyware to spread is through flaws in Microsoft Windows or your web browser. Even though Microsoft has been working for years to get all of the security "bugs" out of its products, it's still a really big task that isn't even close to completion. And every now and then, some hacker will find a way that he or she can install something on your PC just by using a software programming trick. This is especially dangerous because the hacker will be able to install software on your computer without even having physical access to it; all the hacker needs is for your computer to be connected to the Internet. This might be the most disturbing aspect of spyware because, in essence, this software has been installed on your computer without your permission, and you *didn't do anything at all*.

No matter how it gets installed on your computer, spyware can take on many forms that range from annoying to dangerous. Some of the more common spyware behaviors you'll see are listed here:

## Adware

Adware is a term for spyware that opens up advertisements within Internet browser windows, called "pop-up ads" or simply "pop-ups" because your web browser opens (or "pops up") a new window on your screen containing an advertisement or an entirely new web page. You run into pop-up ads all over the Internet, even from legitimate websites belonging to your favorite sports teams and online retailers; they're the Internet equivalent of the postcard advertisements that get inserted into print magazines. So, it's important to understand that every time you see a pop-up advertisement, it doesn't necessarily mean that you've been hit with adware. If you go to the website of your favorite book seller and you see a pop-up ad offering you free shipping if you spend \$75 on their site, chances are good that

there's nothing wrong with your computer. You're just seeing a legitimate advertisement from the website that you're visiting.

You may also subscribe to an online service that lets you receive email or watch music videos for free, but you "pay" for this service by having pop-up ads appear before you can check your mail or watch the video. Most legitimate sites will spell this out for you loud and clear when you sign up for their service, so you can decide if it's worth putting up with a few pop-up ads to be able to use their site for free. Any piece of software that you download or web service that you use should come with an *End User License Agreement*, or *EULA* for short. This should explain exactly what the installer is doing and whether it's installing any additional software pieces (like spyware) along with it. Sometimes the makers of a piece of software will actually *tell you* that they're installing adware on your PC, but they'll stick the notice all the way at the end of the EULA in the hopes that you'll miss it.

If you've ever installed a piece of software on your PC, you've seen a EULA...or at least the first few lines of one. The EULA is the text that's listed on the screen that appears whenever you install a new piece of software, where you need to select "Yes, I agree to the terms of this software" and then click **Next** before you can continue the installation. Almost nobody reads the EULA; we just skip right past it and keep going. Less-than-scrupulous websites are counting on this fact so that they can install spyware on your machine and then say, "Well, we *told* you we were going to install it. It's not our fault you didn't read the EULA." There are even some software companies that are bringing *lawsuits* against some anti-spyware software companies, claiming that their products should not be considered spyware since the terms of service are spelled out right in the EULA.

If you're serious about stopping spyware on your home computer, it's worth taking the extra minute to read the EULA on each piece of software that you've downloaded, just to make sure that nothing is piggybacking on top of the thing that you're installing. If a piece of software doesn't have a EULA, you should leave that website immediately and find one of their competitors who cares a bit more about your security and privacy.

So, how do you know if something is amiss? How do you know that the pop-up ads you're seeing are not legitimate pop-ups from "normal" websites, but rather ones that indicate that something more insidious is going on? A good indication is

that all of a sudden you find that you're drowning in pop-up ads, even when you're not surfing the web:

- You're working on a word processor document or a spreadsheet program and Internet advertisements start popping up out of nowhere.
- You receive pop-up ads while you're browsing the web that have nothing to do with the site you're visiting. These can often contain adult content or be objectionable in nature.
- Advertisements pop up as soon as you turn on your computer.

If you're seeing any of these behaviors, chances are pretty good that you've got some type of adware installed on your system that's causing this to happen. And it's at this point that pop-up ads can go from "irritating" to "unsafe": unscrupulous website designers can include other types of malicious software in a web page so that what started as a simple pop-up ad can then install *another* piece of spyware onto your system.

Even beyond generating pop-up ads, spyware can create other, more serious issues with your home PC and your personal information, which we'll discuss next.

## Hijackers

You open up your web browser, expecting to see [www.yahoo.com](http://www.yahoo.com), [www.cnn.com](http://www.cnn.com), or whatever you've set your home page to be. Instead, you're sent to a site you've never seen before, usually one that fires 10 or 15 pop-up ads at you. You change your homepage back to where you want it to be, but the next time you open your browser, you're back at that annoying page again. Or maybe there's a new toolbar on your browser that you don't remember installing, and you can't figure out how to get rid of it. This is a form of spyware called *hijacking*. Like pop-up ads, this is usually more obnoxious than harmful, but you're still running the risk of getting one of those pop-up windows that has some of that nasty software embedded in it.

## Keystroke Loggers

Maybe up until now, you've been reading my description of adware and hijackers, and you aren't quite sold on the extent to which spyware can threaten your privacy. And in some respects, this is a perfectly fair assessment: some forms of spyware only consist of annoying (but otherwise benign) pop-up ads that are trying to entice you to purchase a new product or website membership. But in many cases,

the risks caused by spyware are much greater than simply forcing you to swat away a few pop-up ads: some forms of spyware will keep a record of every website you visit and *every single thing* you type on your keyboard and then transmit that information to a website or another web server that belongs to the hacker.

So, you open up your web browser, close the three or four pop-up ads that appear whenever you connect to the Internet, and log onto your online banking site. Now, you think you're secure at this point because the URL begins with "https://" , signifying that it's a *secure* site. You're further assured of your security because you can see the little padlock in the lower-right corner of your browser, which also indicates that you're using a website that is securing and encrypting any information that you send to it. (If you don't know how to look for these, we'll be discussing web browser security in a later section.) But even a secure web connection isn't going to help you if a hacker can grab your username and password *as you're typing them in* and then can log onto your bank's website pretending to be you. Just think about all the things that you type at your keyboard when you're on the Internet. This seedy individual could snatch up:

- Your credit card number as you're typing it in to buy a CD from Amazon
- Personal information like your home address and telephone number, or even your Social Security number
- Usernames, passwords, and account numbers to online banking or brokerage sites

This kind of threat is often how identity theft happens: just as you're careful about shredding paper documents that contain your personal information, you need to protect your computer from spyware to be just as careful about your online data. Some keystroke loggers will even record everything you type into a text file and then email it to a hacker at a later time. This means that you don't even have to be connected to the Internet for keystroke loggers to work. Keystroke loggers are particularly insidious because they're sometimes marketed as legitimate programs. Maybe you downloaded a piece of software to help keep track of your child's online activity, but the maker of the "nanny" program turns out to be just as bad as the people you were trying to protect yourself from.

This is not to say that the makers of all such "nanny" software programs are out to steal your credit card numbers: there are a number of perfectly reputable options in this area. It's all a matter of being careful about where you're downloading software from, which we'll be talking about later as well.

## II. Is Spyware a Virus?

At this point, you might still be thinking that your computer is sufficiently protected against spyware infections and that you don't have anything to worry about. After all, you bought the newest anti-virus software from your computer store and paid the fee they charged you to receive automatic updates for the next year. So, you should be safe from everything, right?

Unfortunately that's not quite the case. Like I said earlier in this section, although viruses and spyware both fall under the heading of "malicious software," they're not quite the same thing. How are they different? In technical terms, a virus is a small piece of computer *code*—a miniature computer program, in other words—that attempts to spread from one computer to another through email attachments or over the Internet. Viruses range from annoying to destructive in nature: the miniature computer program can do anything from just clogging up your Inbox with unwanted emails all the way to modifying or deleting important files on your hard drive.

Spyware, on the other hand, is only "spread" by someone installing a piece of software that has spyware piggy-backing on top of it, or by browsing to a website that installs it automatically. So the largest difference between spyware and viruses is that, for the most part, spyware does not attempt to spread itself to other computers in the same way that a virus does.

But now we should move past the technical distinctions and talk about the more important question: "Why do I *care* that viruses and spyware are different?" And the answer to that question is quite simple, and a little frightening:

**Most (if not all) anti-virus software is *not* able to protect you against spyware.**

Anti-virus software does a great job at finding and removing viruses, especially if you keep your anti-virus definitions up-to-date. But anti-virus software by itself will do next to nothing to detect or prevent spyware infections. This is because anti-virus software scans for the particular piece of code that makes up a virus and uses that *signature* to prevent the virus from causing any damage to your computer. But for the most part, anti-virus software doesn't detect spyware because spyware doesn't have the same sort of easily-identifiable signature as a virus. As time has gone on, some newer versions of virus scanners have begun to incorporate spyware scanning capabilities. But not everyone's doing it, and the ones that are doing it still have quite a way to go. I can't tell you the number of

times I've run a virus scan on somebody's home PC and had it come back clean, only to run a spyware detection tool and find dozens or hundreds of spyware applications installed on their computer. In order to fully protect your PC from the malicious software that exists on the Internet, you need to have protection in place against both viruses *and* spyware. I say this because I don't want to give you the impression that anti-virus software is unimportant: it's absolutely critical.

