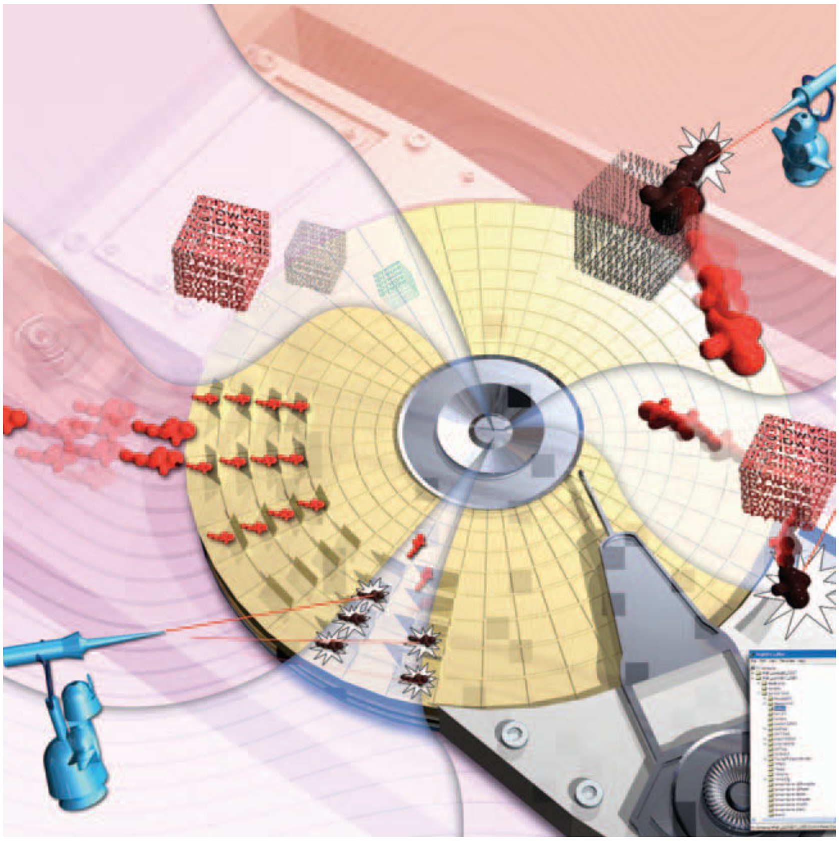
CHAPTER 3

How Spyware and Anti-Spyware Work



THESE days, the biggest danger you face when you go onto the Internet might be spyware—a type of malicious software that can invade your privacy and wreak havoc on your PC. Spyware is a relatively new phenomenon; it does not have a long history as do viruses, Trojans, and worms.

Spyware is an umbrella name for many types of malicious programs, but these kinds of programs have several things in common. First, all of them, one way or another, spy on your behavior. They may watch which web pages you visit and report that information to a server or person, or they might track your web searches. They may even allow people to record every keystroke you make or open a back door into your computer so hackers can later take control of your PC when they want.

The second thing they have in common is that they install either without your knowledge or by tricking you. One common way they get on your PC is when you install a piece of software, such as file-sharing software. When you install that software, spyware often comes along for a ride and installs itself without your knowledge or misleads you about what the program actually does.

Although some spyware is created for purely malicious reasons, other kinds are created as part of money-making schemes. One kind of spyware swarms your PC with dozens of pop-up ads, some of which you'll most likely click to close. But every time you click, the spyware purveyor makes money because he has a business arrangement with a merchant or website to drive traffic to it.

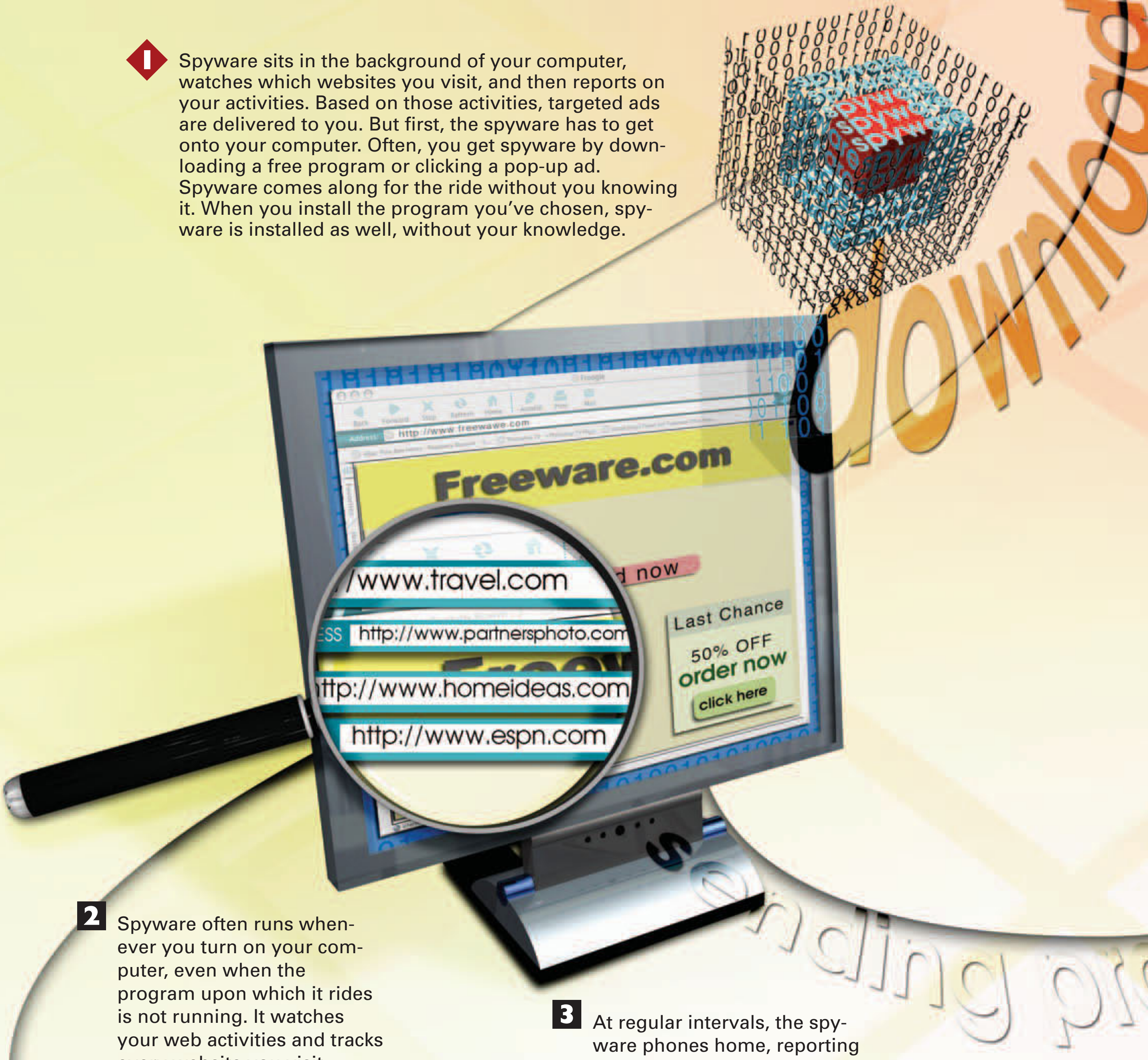
There is a fine line between spyware and what is called *adware*. They work similarly, but with adware, you download a piece of software that you can use for free, such as a weather program. In return, the adware watches your surfing habits and sends that information to a server, which then delivers ads to you based on your behavior. The ads are displayed only inside the weather program and don't appear when you don't use it. Spyware, by way of contrast, watches you all the time and displays ads whenever you surf the Web or are connected to the Internet.

Spyware can do more than just spy on you. It can do damage to your computer as well. Some spyware inundates your computer with blizzards of pop-up ads—in some instances so many that it takes away all your system resources and your PC grinds to a halt. This makes your computer unusable.

Because there is money to be made from surfing, spyware isn't going away any time soon. But as you'll see in this chapter, anti-spyware can combat it, so there are ways to keep yourself safe and protect your privacy.

How Spyware Invades Your PC

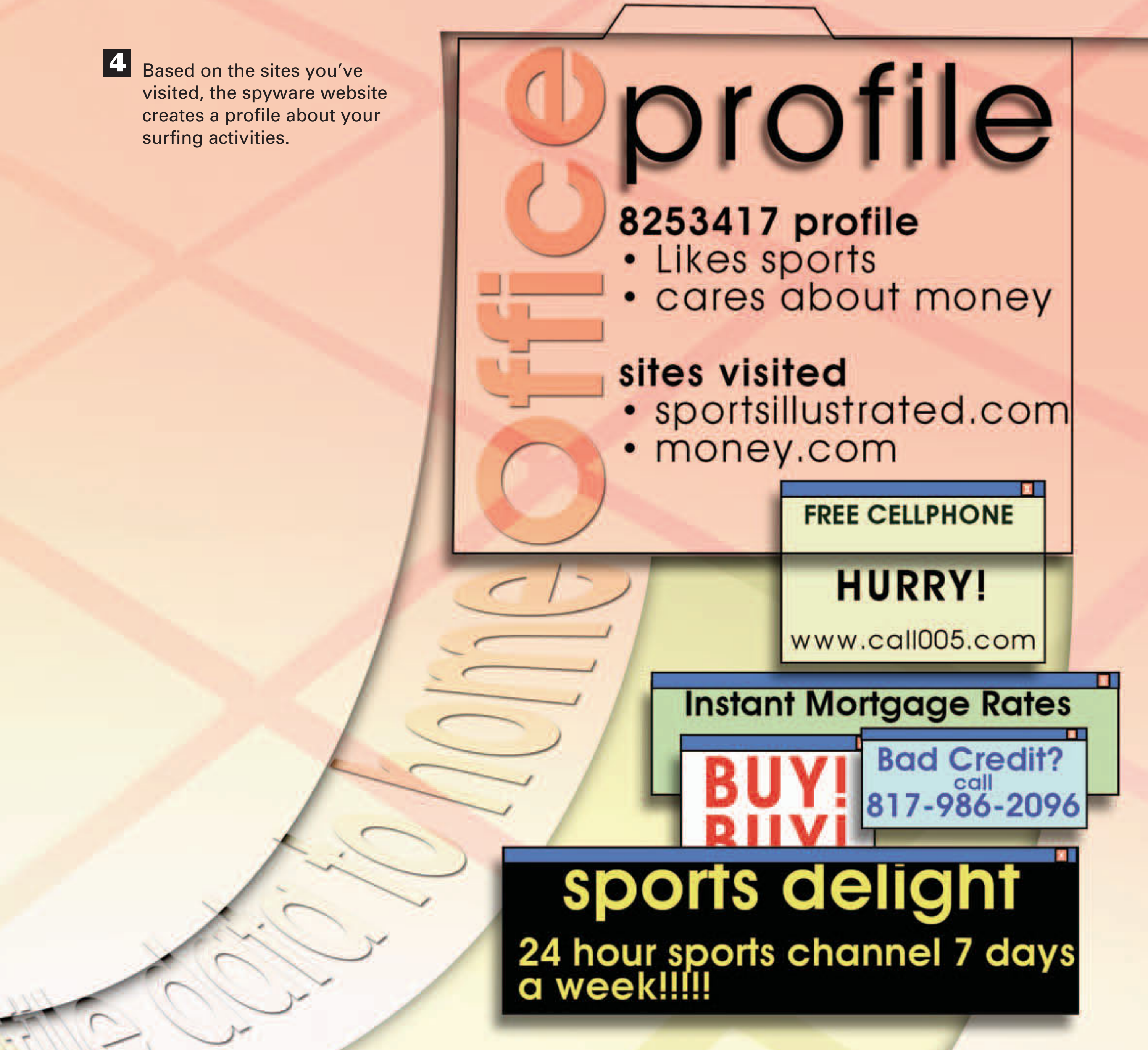
1 Spyware sits in the background of your computer, watches which websites you visit, and then reports on your activities. Based on those activities, targeted ads are delivered to you. But first, the spyware has to get onto your computer. Often, you get spyware by downloading a free program or clicking a pop-up ad. Spyware comes along for the ride without you knowing it. When you install the program you've chosen, spyware is installed as well, without your knowledge.



2 Spyware often runs whenever you turn on your computer, even when the program upon which it rides is not running. It watches your web activities and tracks every website you visit.

3 At regular intervals, the spyware phones home, reporting to the spyware website which sites you've visited.

4 Based on the sites you've visited, the spyware website creates a profile about your surfing activities.



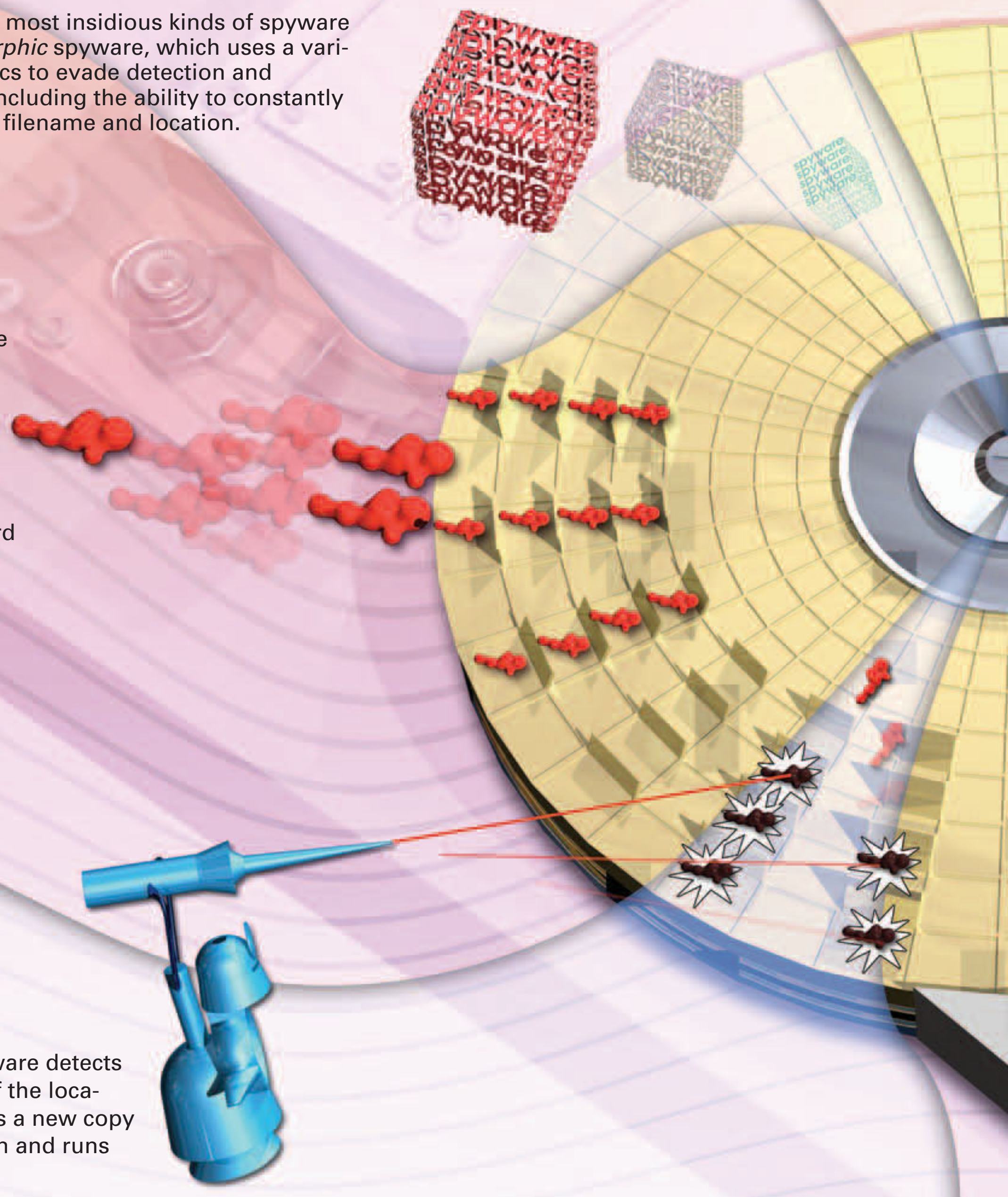
5 Based on that profile, the website delivers targeted ads to you. The ads appear whenever you run the program on which the spyware piggybacked onto your system. When you delete the program on which the spyware piggybacked onto your system, the spyware typically does not get deleted. It keeps watching your surfing activities and reporting on them, although it can't deliver ads based on that information because the program on which it was piggybacked has been deleted. To delete the spyware, you need a special spyware detector and killer, such as Ad-Aware from www.lavasoft.com.

How Spyware Morphs Itself to Escape Detection

1 One of the most insidious kinds of spyware is *polymorphic* spyware, which uses a variety of tactics to evade detection and removal, including the ability to constantly change its filename and location.

2 Cool Web Search and About: Blank are two home page–hijacking pieces of shareware that morph and use other techniques to evade detection and deletion. Programs like these can install themselves to multiple locations on a hard disk.

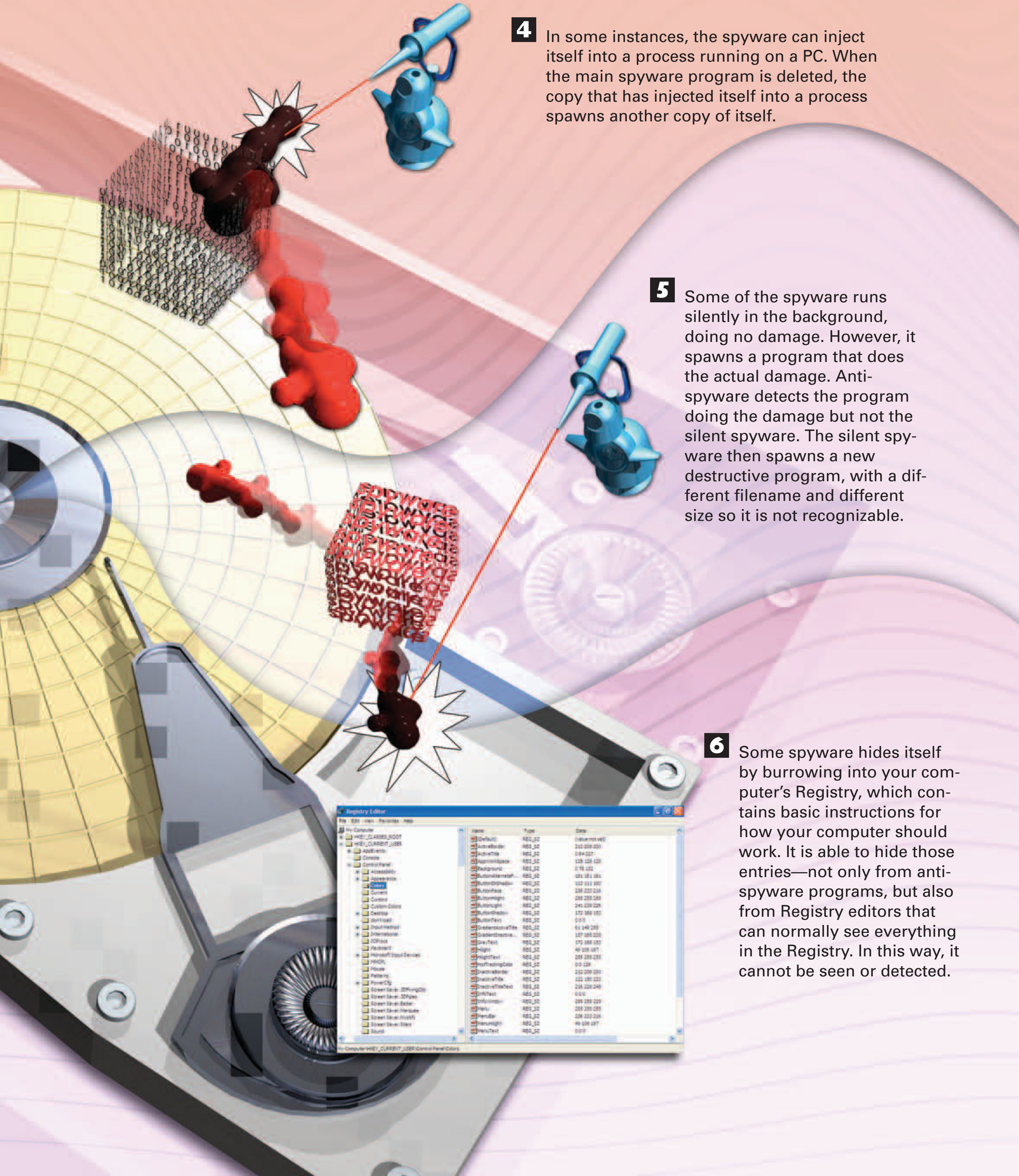
3 When a piece of anti-spyware detects and kills the files in one of the locations, the spyware spawns a new copy of itself at another location and runs from there.



4 In some instances, the spyware can inject itself into a process running on a PC. When the main spyware program is deleted, the copy that has injected itself into a process spawns another copy of itself.

5 Some of the spyware runs silently in the background, doing no damage. However, it spawns a program that does the actual damage. Anti-spyware detects the program doing the damage but not the silent spyware. The silent spyware then spawns a new destructive program, with a different filename and different size so it is not recognizable.

6 Some spyware hides itself by burrowing into your computer's Registry, which contains basic instructions for how your computer should work. It is able to hide those entries—not only from anti-spyware programs, but also from Registry editors that can normally see everything in the Registry. In this way, it cannot be seen or detected.

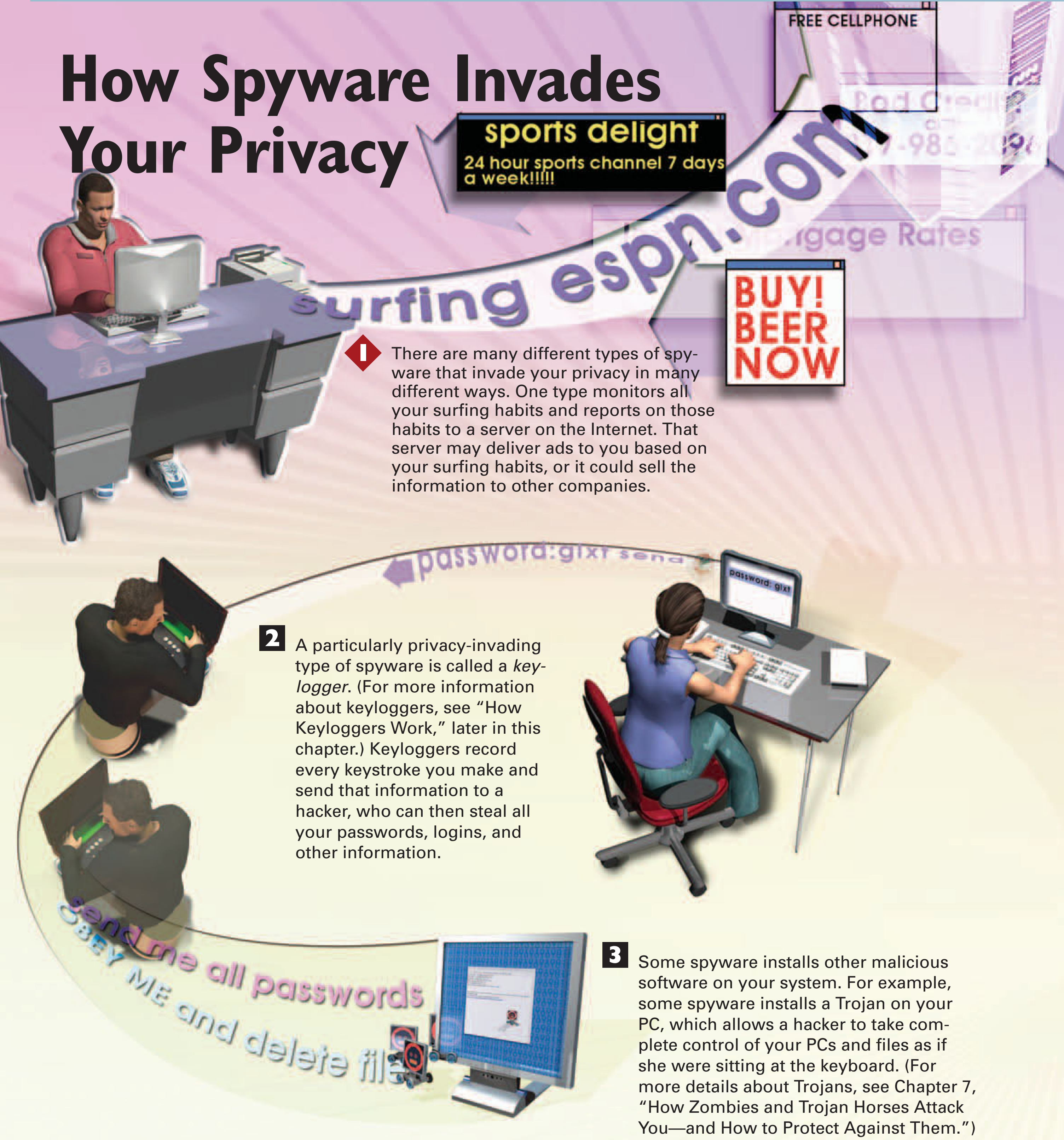


My Computer
- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
  - AppEvents
  - Console
  - Control Panel
    - Accessibility
    - Appearance
    - Colors
    - Current
    - Cursors
    - Custom Colors
    - Desktop
    - don't load
    - Input Method
    - International
    - IOProcs
    - Keyboard
    - Microsoft Input Devices
    - MMCPL
    - Mouse
    - Patterns
    - PowerCfg
    - Screen Saver.3DFlyingObj
    - Screen Saver.3DPipes
    - Screen Saver.Bezier
    - Screen Saver.Marquee
    - Screen Saver.Mystify
    - Screen Saver.Stars
    - Sound

Name	Type	Data
(Default)	REG_SZ	(value not set)
ActiveBorder	REG_SZ	212 208 200
ActiveTitle	REG_SZ	0 84 227
AppWorkspace	REG_SZ	128 128 128
Background	REG_SZ	0 78 152
ButtonAlternateF...	REG_SZ	181 181 181
ButtonDkShadow	REG_SZ	113 111 100
ButtonFace	REG_SZ	236 233 216
ButtonHilight	REG_SZ	255 255 255
ButtonLight	REG_SZ	241 239 226
ButtonShadow	REG_SZ	172 168 153
ButtonText	REG_SZ	0 0 0
GradientActiveTitle	REG_SZ	61 149 255
GradientInactive...	REG_SZ	157 185 235
GrayText	REG_SZ	172 168 153
Hilight	REG_SZ	49 106 197
HilightText	REG_SZ	255 255 255
HotTrackingColor	REG_SZ	0 0 128
InactiveBorder	REG_SZ	212 208 200
InactiveTitle	REG_SZ	122 150 223
InactiveTitleText	REG_SZ	216 228 248
InfoText	REG_SZ	0 0 0
InfoWindow	REG_SZ	255 255 225
Menu	REG_SZ	255 255 255
MenuBar	REG_SZ	236 233 216
MenuHilight	REG_SZ	49 106 197
MenuText	REG_SZ	0 0 0

My Computer\HKEY_CURRENT_USER\Control Panel\Colors

How Spyware Invades Your Privacy



1 There are many different types of spyware that invade your privacy in many different ways. One type monitors all your surfing habits and reports on those habits to a server on the Internet. That server may deliver ads to you based on your surfing habits, or it could sell the information to other companies.

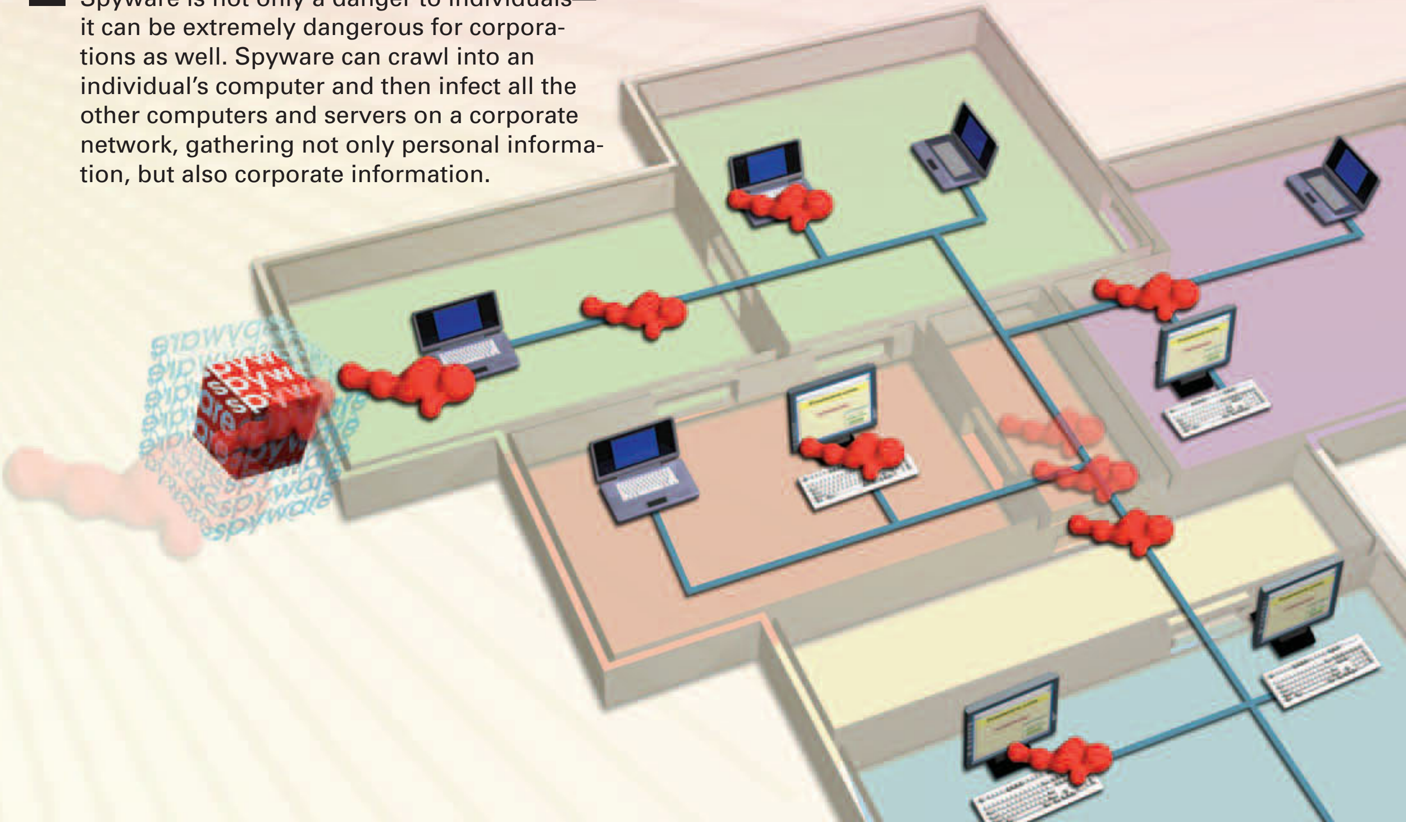
2 A particularly privacy-invading type of spyware is called a *keylogger*. (For more information about keyloggers, see "How Keyloggers Work," later in this chapter.) Keyloggers record every keystroke you make and send that information to a hacker, who can then steal all your passwords, logins, and other information.

3 Some spyware installs other malicious software on your system. For example, some spyware installs a Trojan on your PC, which allows a hacker to take complete control of your PCs and files as if she were sitting at the keyboard. (For more details about Trojans, see Chapter 7, "How Zombies and Trojan Horses Attack You—and How to Protect Against Them.")

4 Some spyware monitors your Internet searching activity and reports that activity to servers, which can then keep track of your interests and deliver ads to you based on them or create profiles of you and sell that information to other companies.

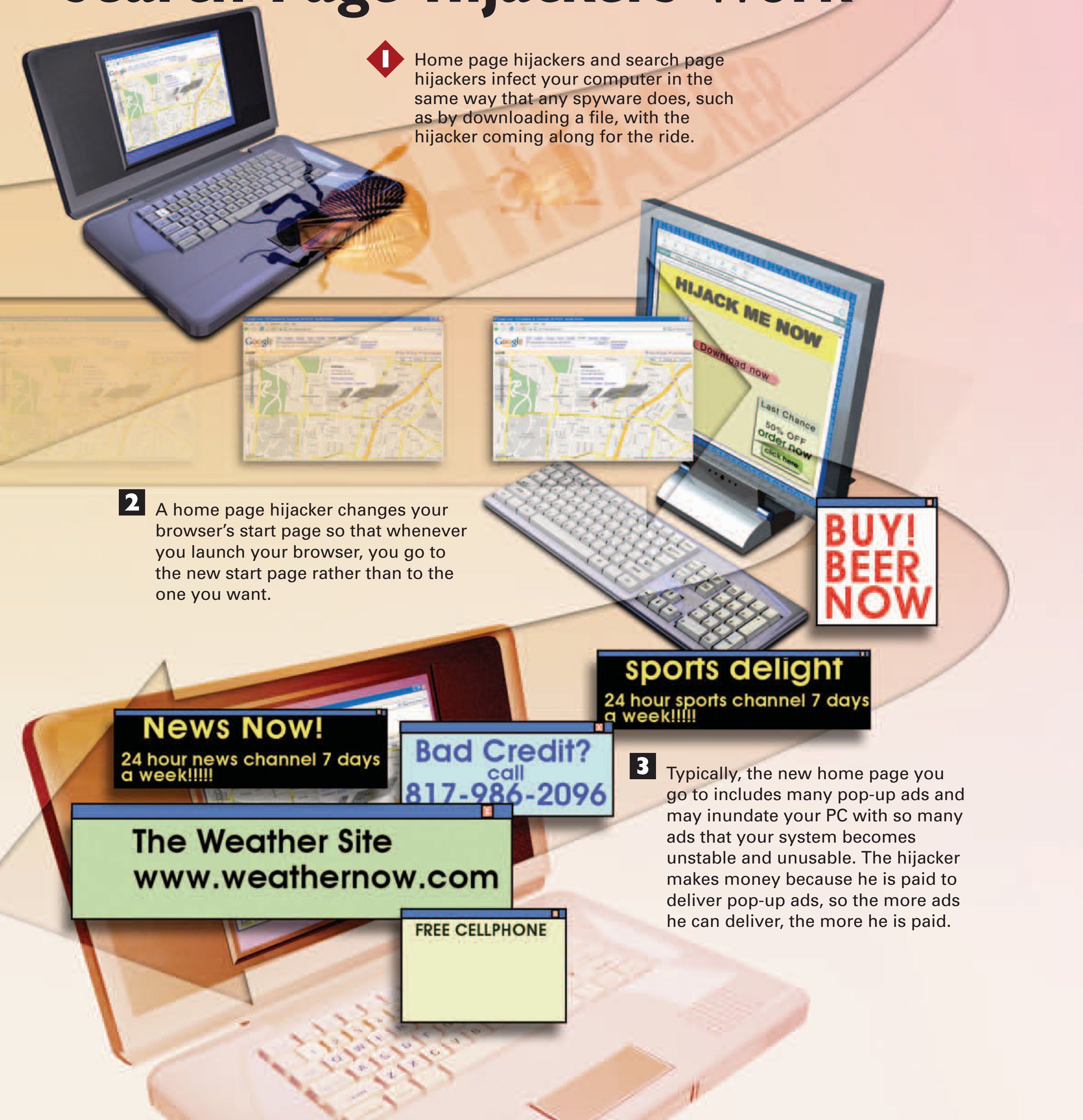
News Now!
24 hour news channel 7 days a week!!!!!
FREE CELLPHONE
Bad Credit? call 817-986-2096
search for news
The Weather Site
www.we
Top News network

5 Spyware is not only a danger to individuals—it can be extremely dangerous for corporations as well. Spyware can crawl into an individual's computer and then infect all the other computers and servers on a corporate network, gathering not only personal information, but also corporate information.



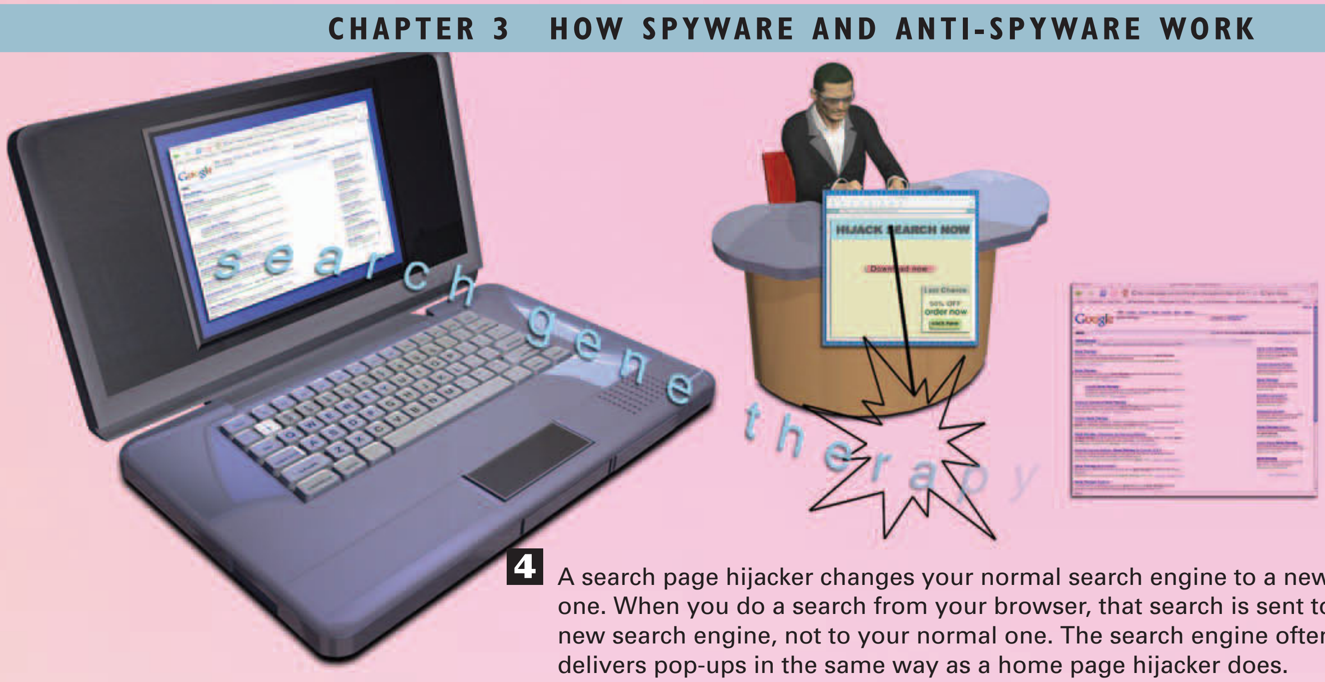
How Home Page and Search Page Hijackers Work

1 Home page hijackers and search page hijackers infect your computer in the same way that any spyware does, such as by downloading a file, with the hijacker coming along for the ride.



2 A home page hijacker changes your browser's start page so that whenever you launch your browser, you go to the new start page rather than to the one you want.

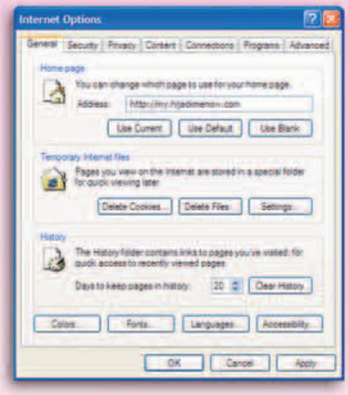
3 Typically, the new home page you go to includes many pop-up ads and may inundate your PC with so many ads that your system becomes unstable and unusable. The hijacker makes money because he is paid to deliver pop-up ads, so the more ads he can deliver, the more he is paid.



4 A search page hijacker changes your normal search engine to a new one. When you do a search from your browser, that search is sent to the new search engine, not to your normal one. The search engine often delivers pop-ups in the same way as a home page hijacker does.

Some home page hijackers intercept every search you perform. For example, if you visit Google and do a search there, the hijacker sends the search to the new search engine, not Google, and then inundates you with pop-ups.

5 Some home page hijackers and search page hijackers are very difficult to eradicate. When you change your browser settings to go back to your normal search and home page, they might change them back again. They can do this by putting themselves in your startup folder and starting up every time you turn on your PC.



Home page

You can change which page to use for your home page.

Address: http://my.hijackmenow.com

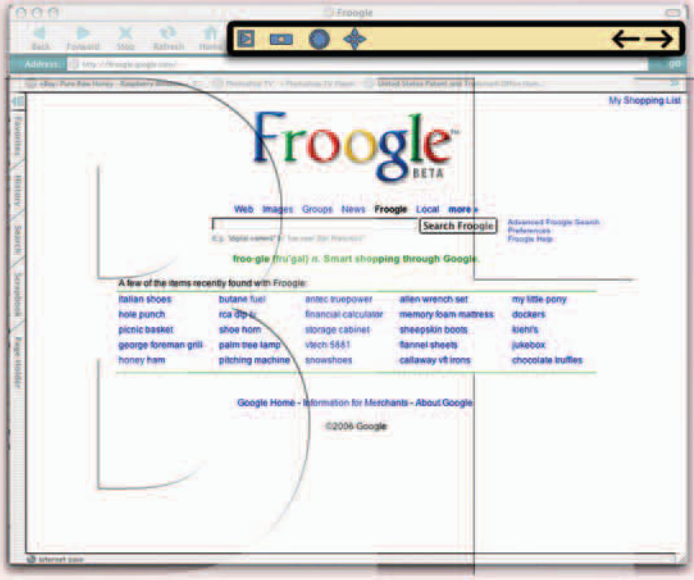
Temporary Internet files

Pages you view on the Internet are stored in a special folder for quick viewing later.

History

The History folder contains links to pages you've visited, for quick access to recently viewed pages.

Days to keep pages in history: 20



froo·gle (fru'gal) *n.* Smart shopping through Google.

A few of the items recently found with Froogle:

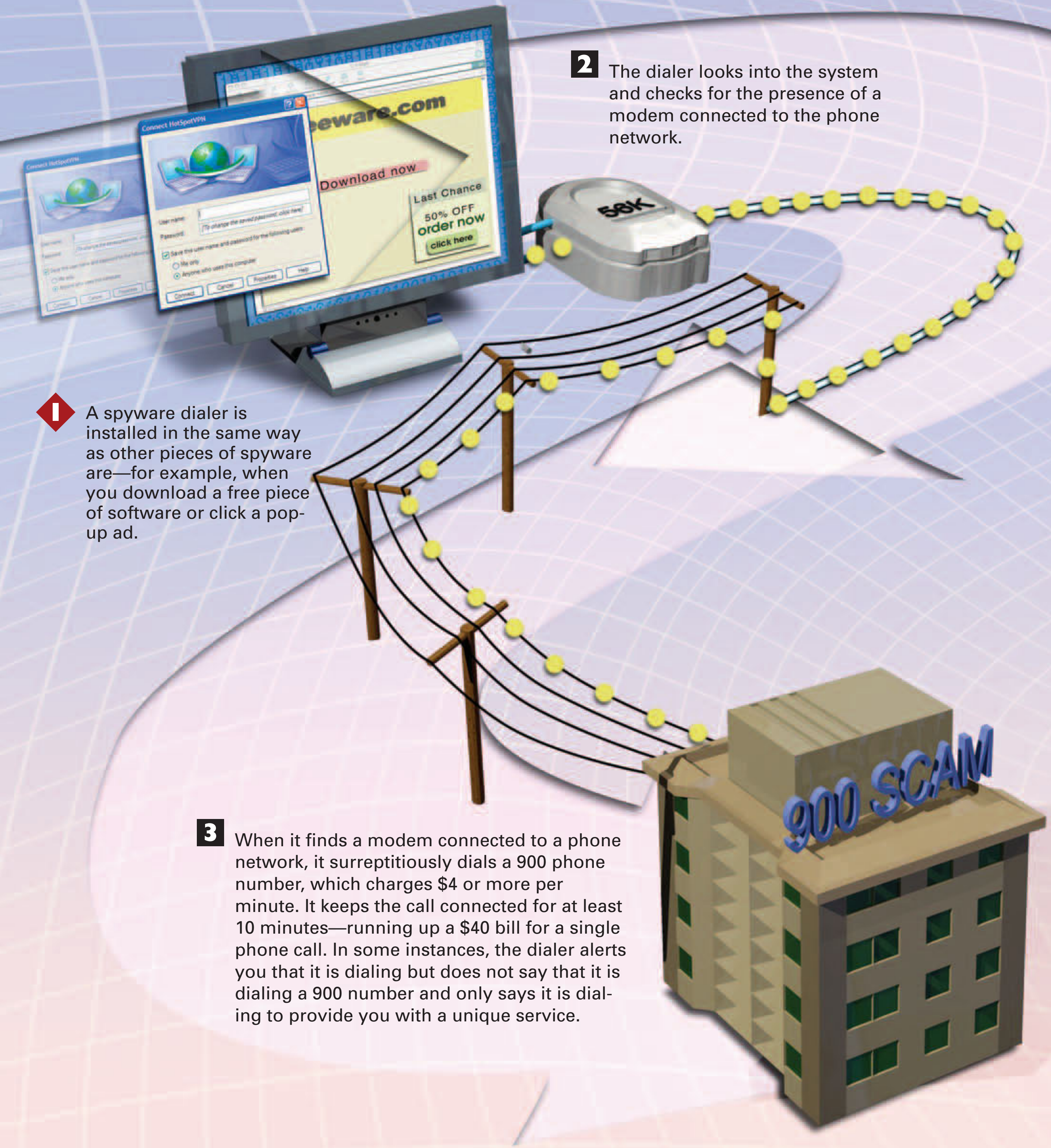
italian shoes	butane fuel	antec truepower	allen wrench set	my little pony
hole punch	rca dlp tv	financial calculator	memory foam mattress	dockers
picnic basket	shoe horn	storage cabinet	sheepskin boots	kiehl's
george foreman grill	palm tree lamp	vtech 5881	flannel sheets	jukebox
honey ham	pitching machine	snowshoes	callaway x4 irons	chocolate truffles

Google Home - Information for Merchants - About Google

©2006 Google

6 Some home page hijackers and search page hijackers disguise themselves as browser add-ins (called browser helper objects [BHOs]) or toolbars. So you think that the toolbar is performing a useful function, but in fact, it is hijacking your home page and search page.

How Dialers Work

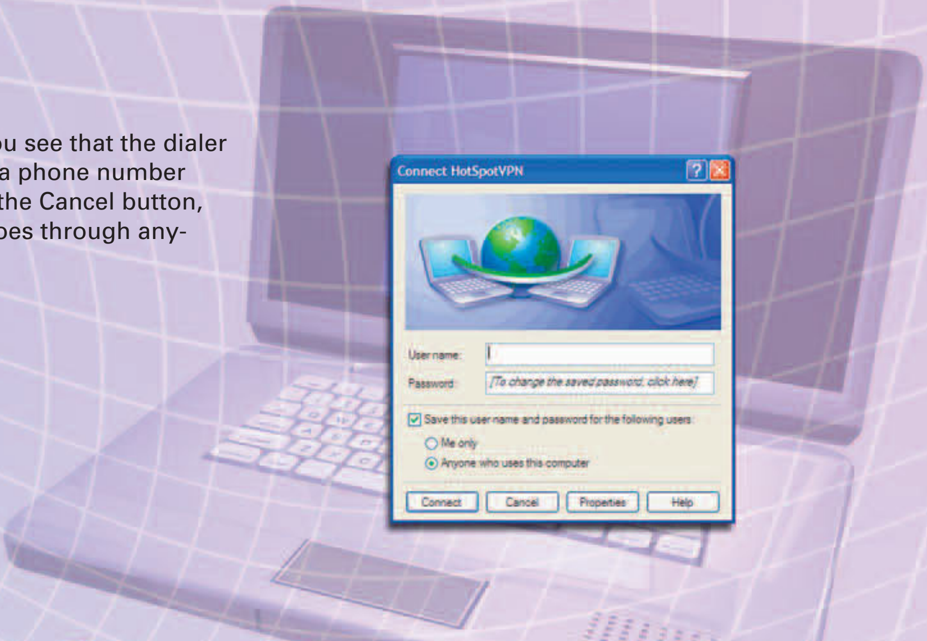


1 A spyware dialer is installed in the same way as other pieces of spyware are—for example, when you download a free piece of software or click a pop-up ad.

2 The dialer looks into the system and checks for the presence of a modem connected to the phone network.

3 When it finds a modem connected to a phone network, it surreptitiously dials a 900 phone number, which charges $4 or more per minute. It keeps the call connected for at least 10 minutes—running up a $40 bill for a single phone call. In some instances, the dialer alerts you that it is dialing but does not say that it is dialing a 900 number and only says it is dialing to provide you with a unique service.

4 Even if you see that the dialer is calling a phone number and click the Cancel button, the call goes through anyway.

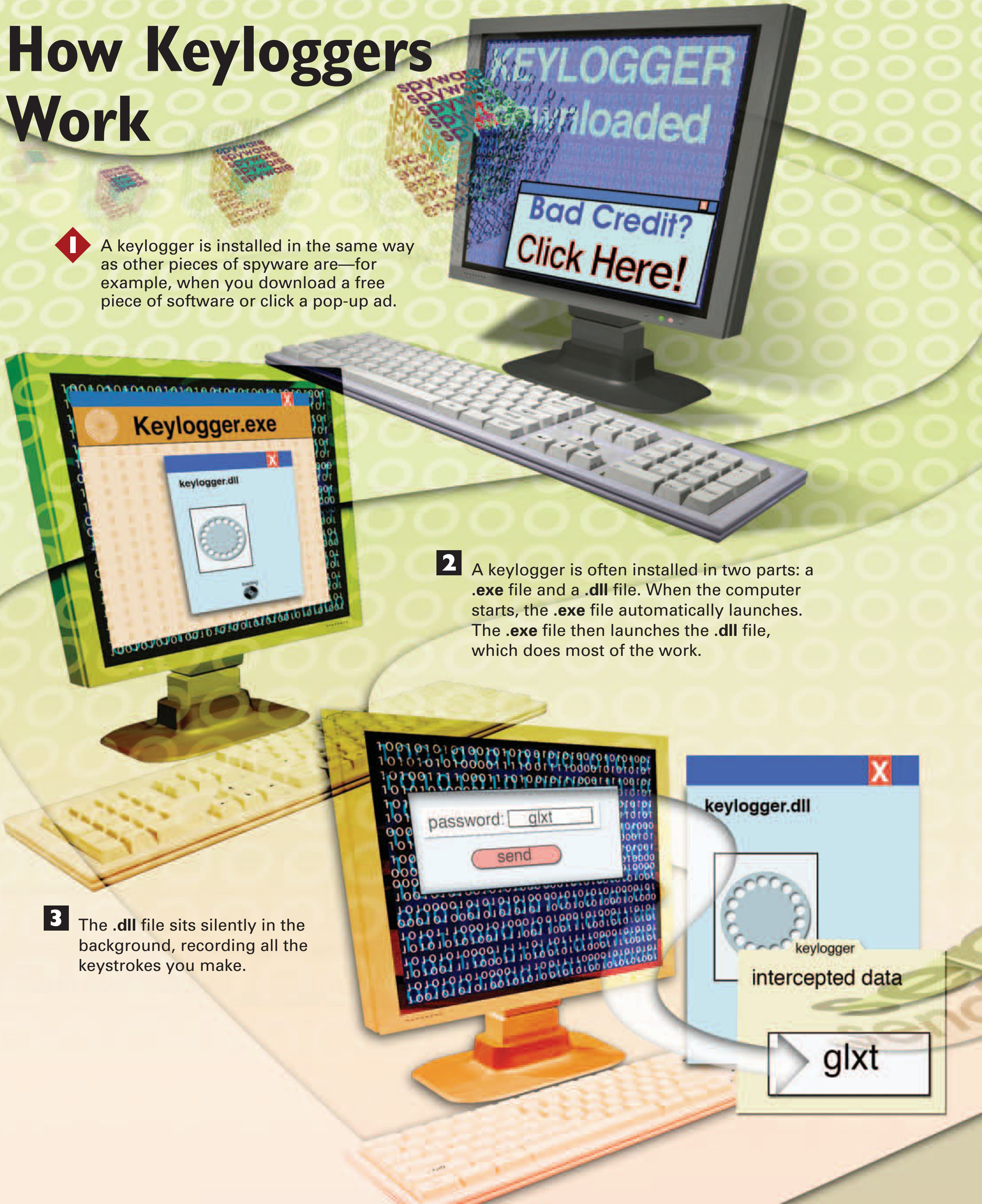

Connect HotSpotVPN
User name:
Password:
[To change the saved password, click here]
☑ Save this user name and password for the following users:
○ Me only
● Anyone who uses this computer
Connect
Cancel
Properties
Help

5 You then receive a telecommunications bill for the cost of the dialing and have to fight against the bill to try to prove that you didn't make the payment.

Connect HotSpotVPN
User name
Password
[To change the saved password, click here]
☑ Save this user name and password for the following users
○ Me only
● Anyone who uses this computer
Connect
Cancel
Properties
modem

6 Because people are increasingly connecting to the Internet via DSL or cable modem lines via Ethernet cables, dialers are not as common as they used to be. A dialer cannot make calls via Ethernet cables over a DSL or cable modem connection.

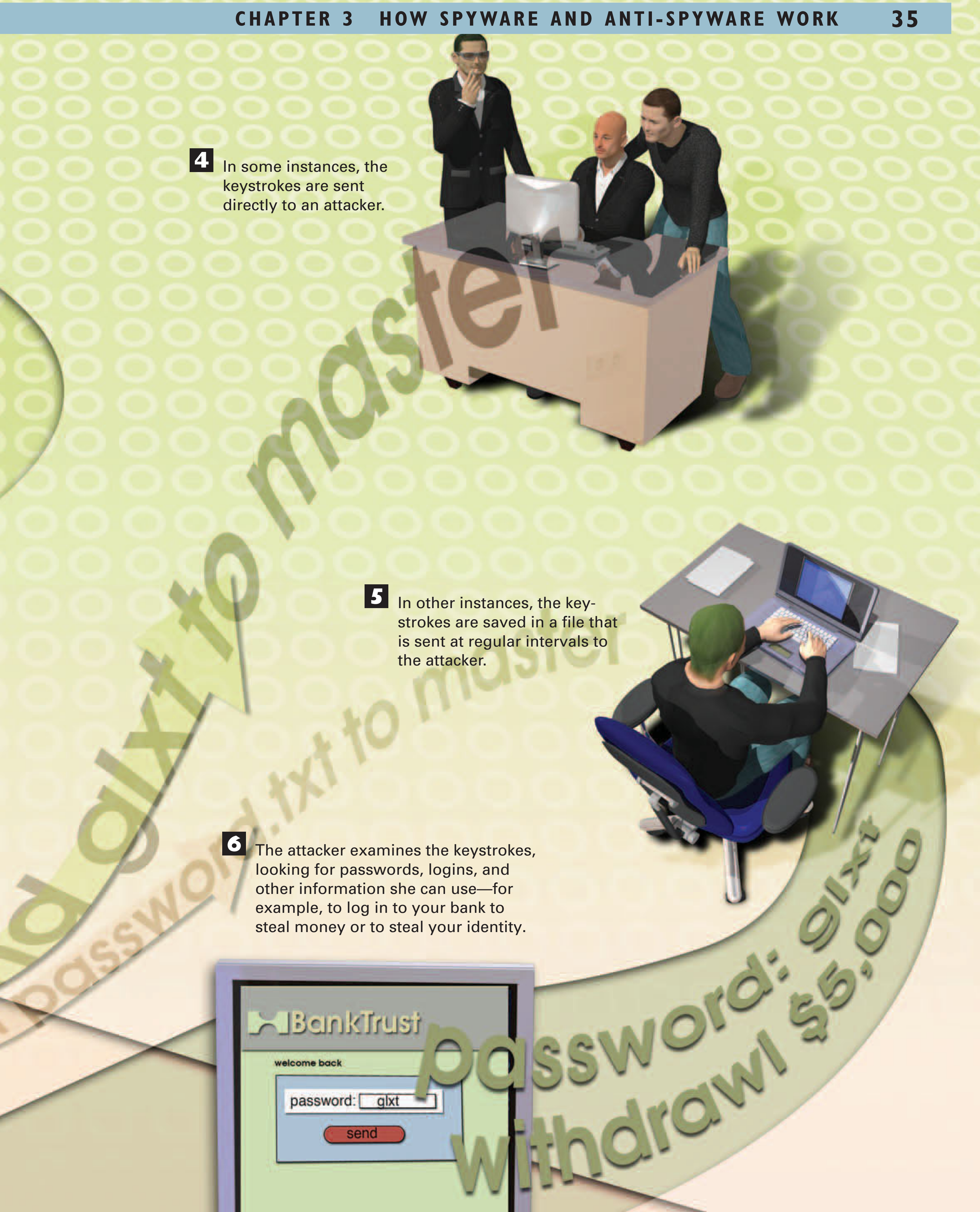
How Keyloggers Work



1 A keylogger is installed in the same way as other pieces of spyware are—for example, when you download a free piece of software or click a pop-up ad.

2 A keylogger is often installed in two parts: a **.exe** file and a **.dll** file. When the computer starts, the **.exe** file automatically launches. The **.exe** file then launches the **.dll** file, which does most of the work.

3 The **.dll** file sits silently in the background, recording all the keystrokes you make.



4 In some instances, the keystrokes are sent directly to an attacker.

5 In other instances, the keystrokes are saved in a file that is sent at regular intervals to the attacker.

6 The attacker examines the keystrokes, looking for passwords, logins, and other information she can use—for example, to log in to your bank to steal money or to steal your identity.

How Rootkits Work

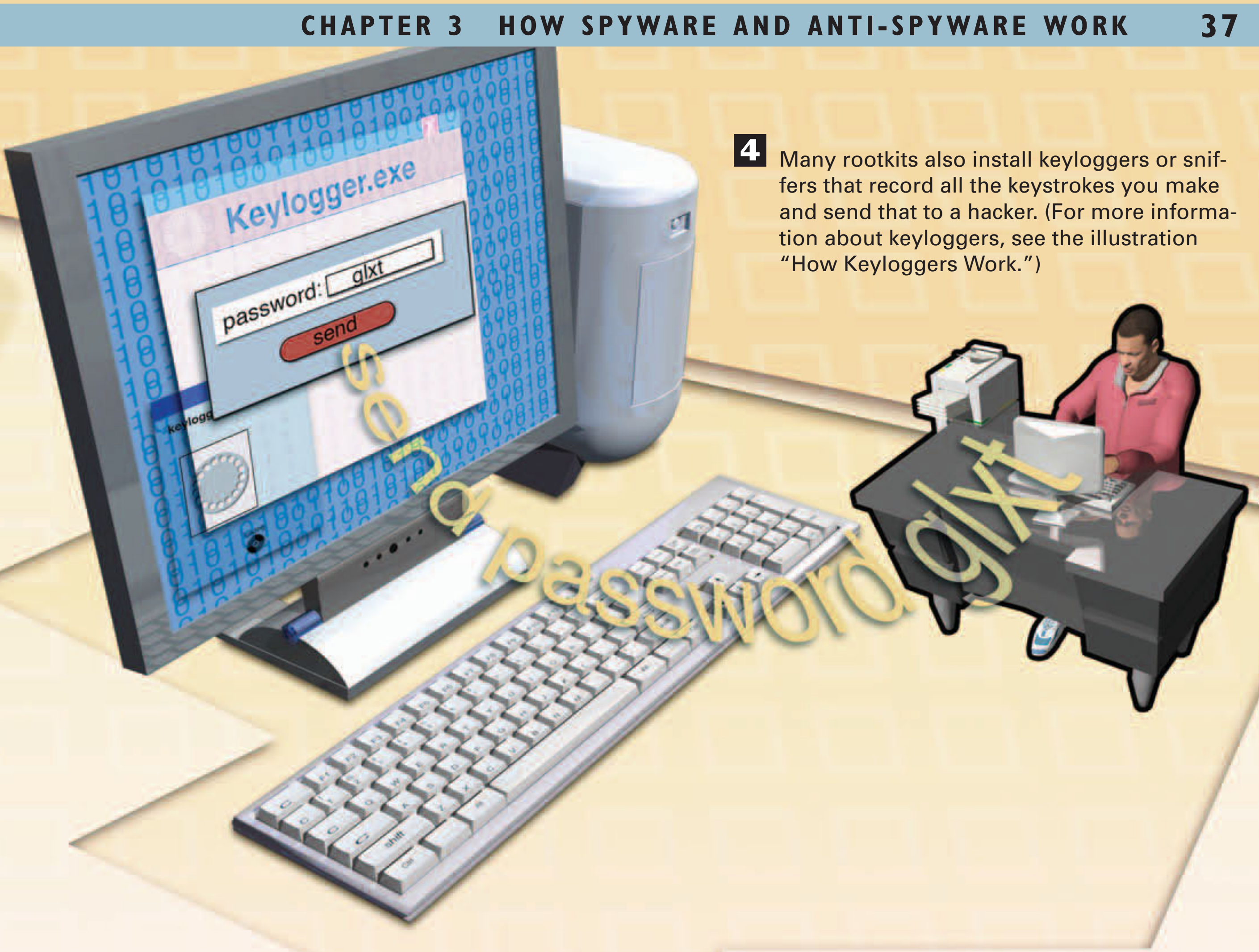
1 A rootkit allows an intruder to gain access to someone's PC whenever he wants, without being detected. It is made up of a series of files and tools. It can be installed on a system in a number of ways, sometimes in the same way that shareware is installed. In the most notorious instance of a rootkit, Sony surreptitiously installed rootkits on tens of thousands or more computers by shipping it as part of software that installed on people's PCs when they put a Sony music CD into their PC's drive.

2 A rootkit can replace important components of an operating system with new software. The new software disguises itself as the original files, including the same file size, creation date, and so on, making it extremely difficult to detect.

kernel.exe
1/10/2006
537,111 bytes
kernel.exe
1/10/2006
537,111 bytes

3 A rootkit installs a backdoor *daemon*, or automatic program. This backdoor opens a hole in the system, allowing the rootkit creator to crawl in and take control of the PC whenever he wants.

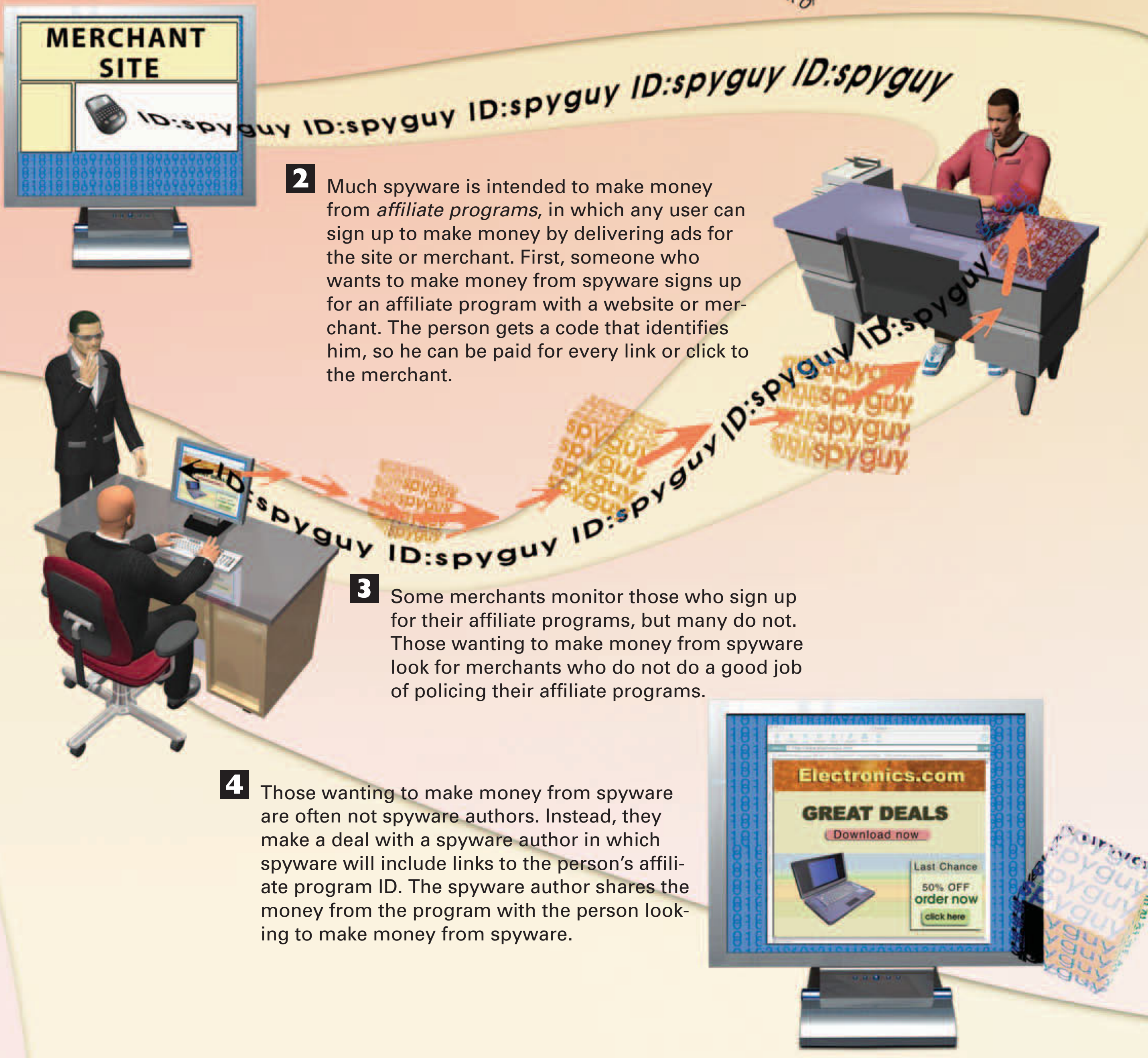
4 Many rootkits also install keyloggers or sniffers that record all the keystrokes you make and send that to a hacker. (For more information about keyloggers, see the illustration "How Keyloggers Work.")



5 A rootkit can modify a computer's system log that tracks all the activity on a PC. The system log normally includes all activity, including malicious activity, so the rootkit modifies the log to hide all traces of itself.

Following the Spyware Money Trail

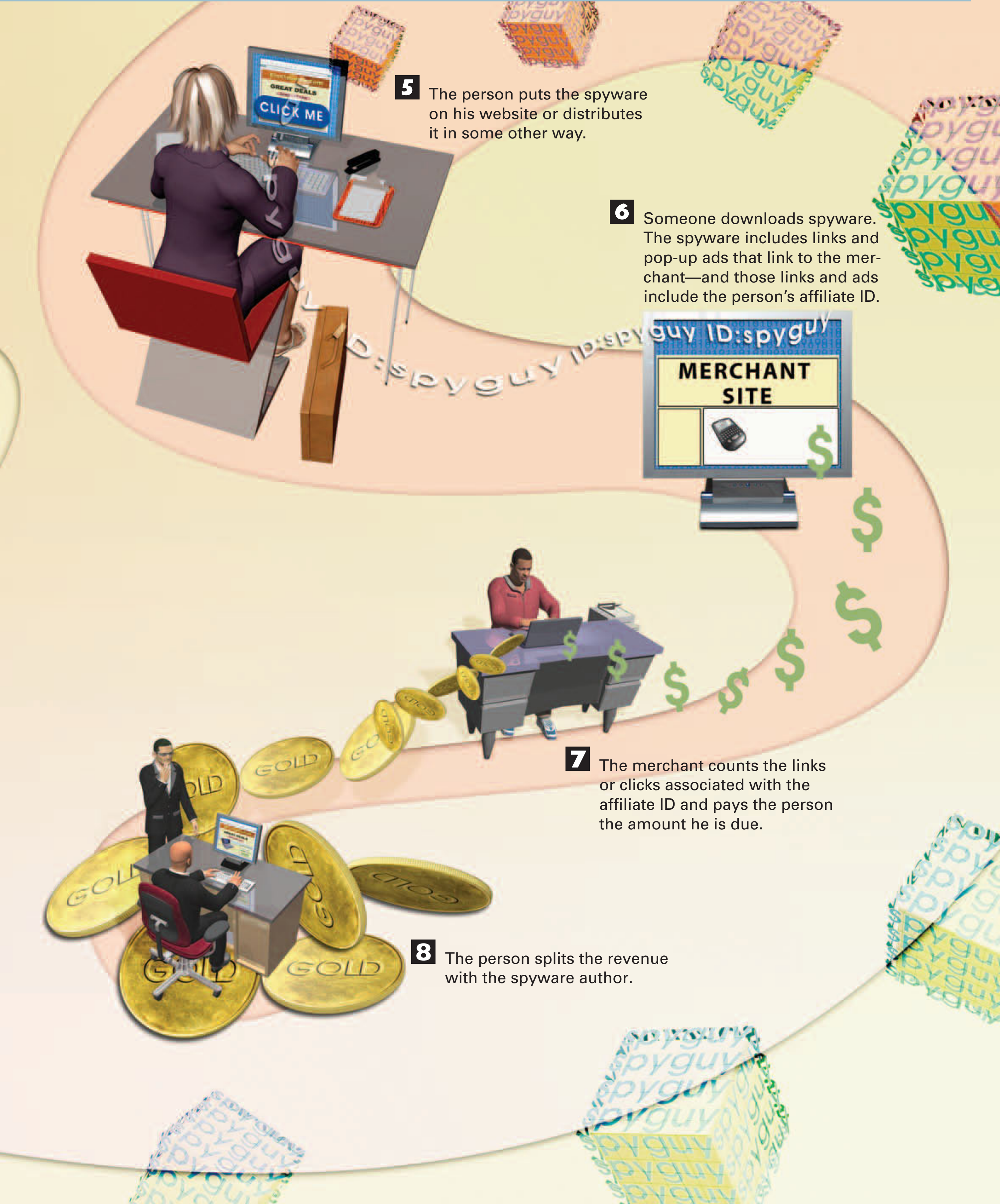
1 Many types of spyware make money for spyware creators or users in many different ways. This illustration shows how a lot of spyware has a money trail that includes reputable, well-known websites and merchants.



2 Much spyware is intended to make money from *affiliate programs*, in which any user can sign up to make money by delivering ads for the site or merchant. First, someone who wants to make money from spyware signs up for an affiliate program with a website or merchant. The person gets a code that identifies him, so he can be paid for every link or click to the merchant.

3 Some merchants monitor those who sign up for their affiliate programs, but many do not. Those wanting to make money from spyware look for merchants who do not do a good job of policing their affiliate programs.

4 Those wanting to make money from spyware are often not spyware authors. Instead, they make a deal with a spyware author in which spyware will include links to the person's affiliate program ID. The spyware author shares the money from the program with the person looking to make money from spyware.



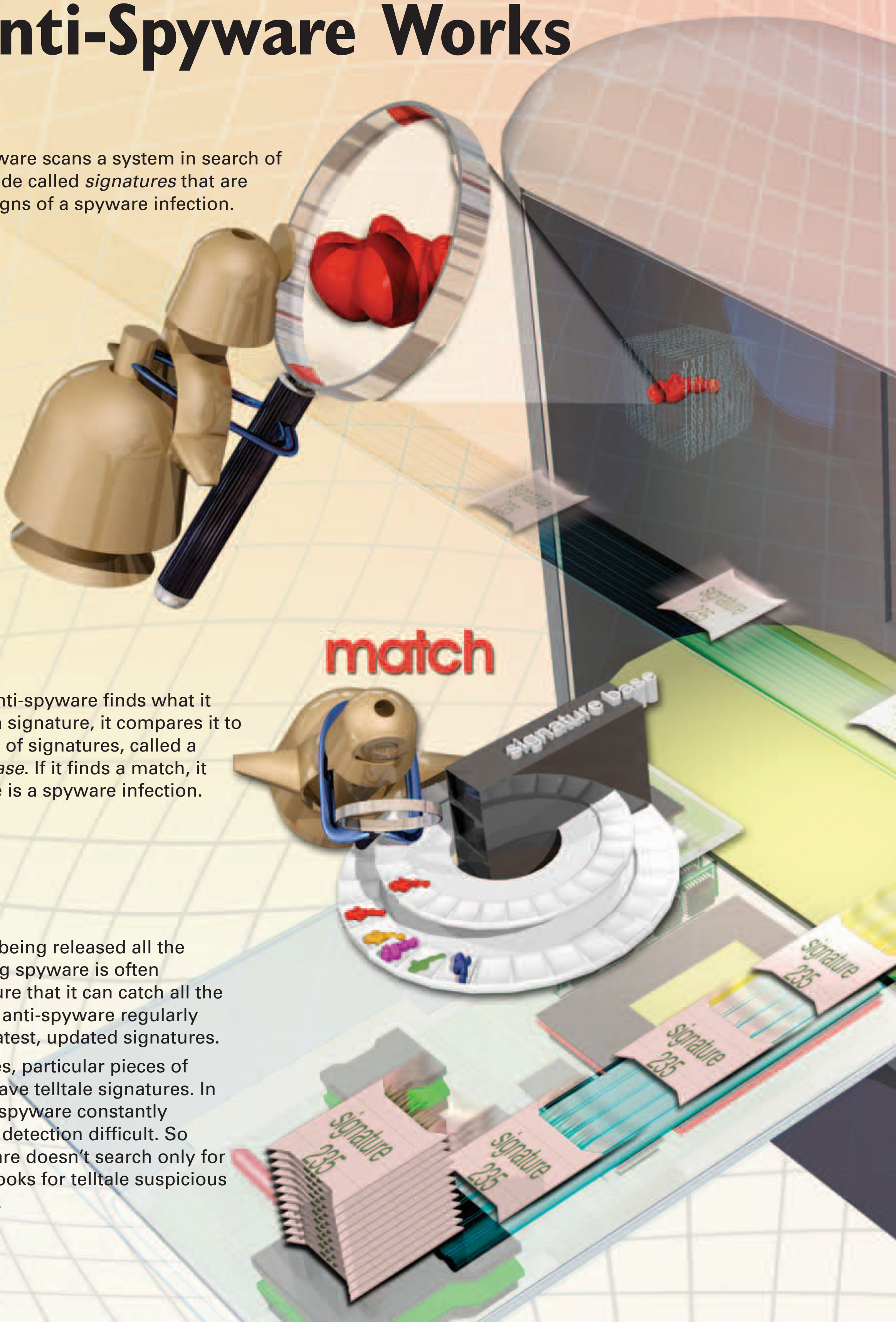
5 The person puts the spyware on his website or distributes it in some other way.

6 Someone downloads spyware. The spyware includes links and pop-up ads that link to the merchant—and those links and ads include the person's affiliate ID.

7 The merchant counts the links or clicks associated with the affiliate ID and pays the person the amount he is due.

8 The person splits the revenue with the spyware author.

How Anti-Spyware Works

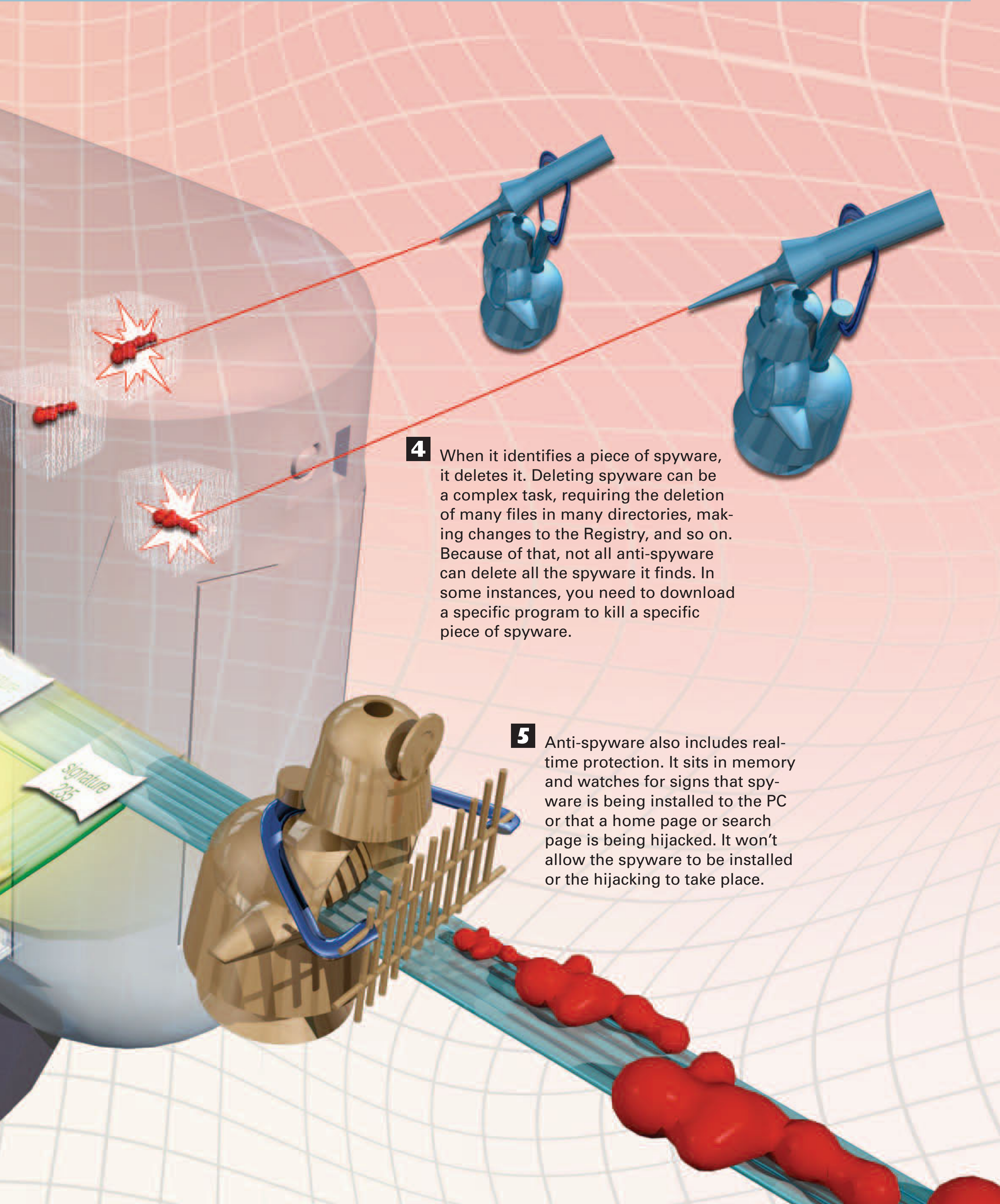


1 Anti-spyware scans a system in search of bits of code called *signatures* that are telltale signs of a spyware infection.

2 When the anti-spyware finds what it believes is a signature, it compares it to its database of signatures, called a *signature base*. If it finds a match, it knows there is a spyware infection.

3 New spyware is being released all the time, and existing spyware is often updated. To ensure that it can catch all the latest infections, anti-spyware regularly downloads the latest, updated signatures.

In some instances, particular pieces of spyware don't leave telltale signatures. In other instances, spyware constantly morphs, making detection difficult. So some anti-spyware doesn't search only for signatures, but looks for telltale suspicious behavior as well.



4 When it identifies a piece of spyware, it deletes it. Deleting spyware can be a complex task, requiring the deletion of many files in many directories, making changes to the Registry, and so on. Because of that, not all anti-spyware can delete all the spyware it finds. In some instances, you need to download a specific program to kill a specific piece of spyware.

5 Anti-spyware also includes real-time protection. It sits in memory and watches for signs that spyware is being installed to the PC or that a home page or search page is being hijacked. It won't allow the spyware to be installed or the hijacking to take place.