Chapter 1

Unwelcome Intruders Seeking Entry

To some extent, it's reasonable to view the Internet as "the ultimate jungle" of lore and story: deep, dark, and full of dangerous denizens. For PC users, this means that any activities involving a trip into the wild — that is, onto the Internet — carries with it the risks of infection, compromise, or attack that prudent visitors to real jungles usually take steps to avoid. Much of this book talks about what's involved in being prudent, how to limit or eliminate chances of compromise, and what kinds of Internet attacks or other hazards are best avoided whenever possible.

It's a Jungle Out There!

These days, anybody who goes online has a chance to experience the wild frontier. This doesn't require leaving home, or even walking any further than to wherever you keep your computer. But once you turn it on, fire up a Web browser or e-mail program, and start digging into the unbelievable variety that the Internet has to offer, you're also exposing your computer to an assortment of hazards that can vary all the way from merely annoying to potentially catastrophic in terms of what such hazards can do to your machine. All kinds of risks and exposures lurk in waiting for the unwarned or unwary, and require only that you visit a certain Web page or open a certain e-mail attachment to inflict themselves upon you — or at least, upon your computer and its contents.

Caution

Any time something unknown or uncertain comes your way, whether a Web site asks if you want to change your default home page setting, pick a new search engine, or add a toolbar to your browser, or you're asked in your e-mail to open an unexpected e-mail attachment, the safe thing to do is "Just Say No!" — that is, you should refuse such proffered changes and avoid opening any e-mail attachments you're not explicitly expecting. Unfortunately, not all threats are kind enough to ask permission before attempting to get familiar with your PC, but if you have the chance to say no, you probably should.

No one can deny that all kinds of unwanted and potentially dangerous threats are out there. The news media routinely report new hazards as they're discovered, and the rates of discovery are going nowhere but up. Whereas it was unheard of for more than 50 or 60 threats to be reported weekly worldwide in the mid to late 1990s, in 2004, the total number of such reports meets or exceeds those numbers on some days. Why is this happening? As the Internet becomes more pervasive, more people use it, and it creates more opportunities for those who may not have your best interests at heart to seek ways to learn more about you, influence or manage your behavior, or simply to mess with your computer (and probably with your sense of security and well-being, too).

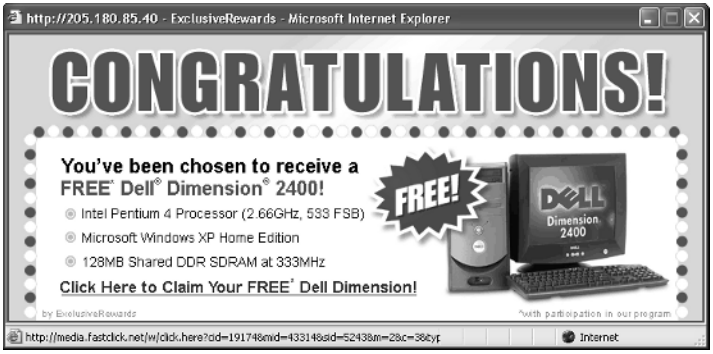
The motivations that drive individuals — and even some companies — to try to find covert or unannounced ways to introduce all kinds of software or tracking tools onto your computer are many and varied. Information is worth money to some, whether it be in the form of reselling information about you to others or using that information to sell things to you directly. This helps explain why visiting so many Web sites results in the deposit of all kinds of small, passive data-collection tools, called *cookies* (more about them later), that record information about your activities on the Web, ready to report them to a server the next time you visit a site that knows how to ask for and read that cookie.

Cross-Reference

Not all cookies are inherently evil. Though some collect information about you that you might not want or need them to know, more benign cookies keep track of site-specific activities, or gather information about you that may actually be helpful the next time you visit a site. As you learn in Chapter 3, cookies don't pose the same kinds of threats that other unwanted deposits on your computer do. Later, in Chapters 6 and 7, you learn more about the tools you can use to fend off cookies. But if you notice that your ability to navigate or be recognized on some Web site suffers because its cookie is turned off, you may want to consider turning such a cookie back on (lots more on this later).

Access to consumers is also worth money, along the lines of "another warm body." Because advertisers pay to show you advertisements on the Web, just as they do on radio or TV, this may help you to understand why visiting certain free Web sites produces a seemingly endless series of small windows designed to inform you, educate you, or perhaps just to catch your eye — but ultimately, also designed to sell you something. Many Web sites generate the funding they need to keep operating by selling advertising to all comers, then inserting banners or separate advertising windows — known as pop-ups or pop-up ads — that they show to visitors who pass through their sites. You can see an example of this kind of thing in Figure 1-1.

You may even notice that some Web sites bring strange "invisible" Web pages to your desktop. Figure 1-2 shows the toolbar icon for what's sometimes called a "one-pixel" Web page — that is, a page frame so small you can't see it. Normally, such pages exist only as a way to bring other (unwanted) stuff to your desktop. Usually, they can't be restored, resized, or maximized by right-clicking their toolbar icons. If you try to move the window, you'll see your cursor dragging and dropping nothing visible!



http://205.180.85.40 - ExclusiveRewards - Microsoft Internet Explorer

CONGRATULATIONS!

You've been chosen to receive a FREE* Dell® Dimension® 2400!

- Intel Pentium 4 Processor (2.66GHz, 533 FSB)
- Microsoft Windows XP Home Edition
- 128MB Shared DDR SDRAM at 333MHz

Click Here to Claim Your FREE* Dell Dimension!

by ExclusiveRewards

*with participation in our program

http://media.fastclick.net/w/click.here?cid=19174&mid=43314&sid=5243&m=2&c=3&typ

Figure 1-1: Pop-ups jump to the top of your screen, forcing you to close them to keep working on what's underneath. Some are more objectionable than others; all interfere with your desktop.

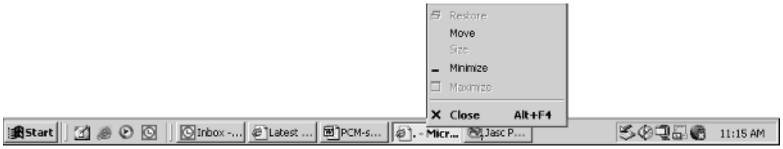


Figure 1-2: A one-pixel Web page shows up on your toolbar (it shows up as a document named period "."), but you can't force it to appear on your desktop. It's there only to open the way for unwanted intrusions or advertisements.

Tip

Because the pop-up menu shown in Figure 1-2 includes a Close control, you can indeed close this unwanted item manually. But it's better to block such items from making a home on your desktop completely — I describe exactly how to do that in Chapter 6.

Some Web sites even try to change the way your Web browser works to turn it to their advantage. If you've ever wondered why your home page has been switched from your favorite starting point on the Internet (perhaps Yahoo! or Google, if you're like many casual Internet users) to some other home page, it might be because you agreed to this change in a dialog box without really realizing the consequences of such an agreement. Some Web sites are reputed to make such changes without even asking, in a sort of home page hijack maneuver.

Other Web sites are still more aggressive with visitors. They don't try to change your home page; instead, they'll request permission to install a toolbar in your Web browser. Besides changing your home page assignment, this also results in the appearance of additional buttons in the control areas of a browser window. Behind the scenes, it may even change your favorites or bookmarks to preferentially drive you toward sites of their choosing, switch your preferred search engine to their preferred search engine, and all kinds of other things that can be a real pain to figure out, let alone fix. Here again, some Web sites don't even bother to ask your permission: If your computer isn't ready to repel such advances, they'll simply make whatever changes they want and let you deal with the consequences however you can.

As an innocuous example is the Yahoo! toolbar, which you can choose to install at www.yahoo.com if you wnat to see what something like this adds to your browser. In Internet Explorer, toolbars normally appear at the top of the window, just above the Web page display and below the page address. The Yahoo! toolbar, however, is by no means an unwanted item. It's well-behaved about asking install permission but it can give you an idea of what such a browser change might look like.

One of this book's primary goals is to help you recognize these kinds of potential intrusions on your computer, leaving aside for the moment whether or not they pose any real dangers to your computer or your privacy. I also want to explain how such things work, what kinds of traces they leave behind, and how you can clean up after them if you must. Better still, I explain various ways to avoid such unwanted influences and activities on your computer in the hopes that you'll use them in preventive fashion. As you'll see elsewhere in this book (or as you may have or will learn through direct experience some day), it's a lot easier to avoid such trouble than to catch it and have to clean up the aftermath!

In general, however, if unexpected changes occur on your PC, there's a chance that unwanted software may be involved. It's smart to keep your eyes on this kind of thing and to take what steps you can to head them off before they make themselves at home on your computer. In the sections that make up the rest of this chapter, you'll have a chance to see more examples of these things, to understand what they are and how they work, and to appreciate what kinds of symptoms you might notice if one or more of these things take up residence on or try to make their way onto your machine.

Cross-Reference

The rest of this chapter tackles the more benign forms of unwanted software — namely spyware, adware (pop-ups), and spam (unwanted e-mail). Chapter 2 is where I get into the stuff that can sometimes do bad things to your computer, including what's sometimes called *malware* (a contraction of "malicious software"), such as viruses, worms, Trojans, and other members of that unsavory software genre.

Understanding Spyware

To start any discussion of spyware, it's essential to understand what the term means. As the name implies, *spyware* is anything that takes up residence on a computer, usually uninvited, that can report on the activities and preferences of the computer's users, or disclose information about data stored on a computer. In other words, it spies on what the computer is used for and possibly for what it contains, to report on its findings to outsiders when an opportunity presents itself.

Whatis.com provides a slightly more detailed definition of spyware that's interesting to peruse and ponder next:

> Spyware is any technology that aids in gathering information about a person or organization without their knowledge. On the Internet (where it is sometimes called a spybot or tracking software), spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties. Spyware can get in a computer as a software virus or as the result of installing a new program. Data collecting programs that are installed with the user's knowledge are not considered to be spyware if the user fully understands what data is being collected and with whom it is being shared. However, spyware is often installed without the user's consent, as a drive-by download, or as the result of clicking some option in a deceptive pop-up window.
>
> The cookie is a well-known mechanism for storing information about an Internet user on their own computer. However, the existence of cookies and their use is generally not concealed from users, who can also disallow access to cookie information. Nevertheless, to the extent that a Web site stores information about you in a cookie that you don't know about, the cookie mechanism could be considered a form of spyware.

There's enough material in this lengthy quote from Whatis.com to justify a little follow-up commentary. The term *drive-by download* describes the circumstance in which visiting a Web page causes software to be downloaded and installed on user machines without informing users that this has happened, or without obtaining their prior consent. Please recall also that cookies are passive, mostly textual records that Web sites read and write to help track user history, preferences, and activity. They are covered in more detail in Chapters 7 and 11 of this book.

On the Web

In general, you'll find `www.whatis.com` **a great place to learn about all kinds of computing terminology. Spyware is defined at** `http://searchcrm.techtarget.com/sDefinition/0,,sid11_gci214518,00.html`.

Taking my definition and the Whatis.com definition together, the key points about spyware are as follows:

- Information is gathered without obtaining the user's consent
- It may be relayed to third parties without the user's knowledge
- It may sometimes change the behavior, look, or feel of a PC without either the user's knowledge or consent

The Whatis.com definition mentions viruses as a potential source of spyware; although true, this is a far less common cause than simply visiting certain Web sites that target the unwary or the unprepared. Cookies do indeed deserve mention in this context, because they remain the most widespread and prevalent tool for gathering information about users. But because cookies are easy to turn off or block, they're also relatively easy to deal with. Anti-spyware programs do a great job of this, but privacy controls in most Web browsers can also help you manage cookies quickly and easily. Generally speaking, cookies are not the biggest causes of trouble or concern when it comes to spyware.

In the end, perhaps the Federal Trade Commission's definition of spyware (which you can find at `www.ftc.gov/opa/2004/04/spywaretest.htm`) also bears repeating: Spyware is "software that aids in gathering information about a person or organization without their knowledge and which may send such information to another entity without the consumer's consent, or asserts control over a computer without the consumer's knowledge." The real issue is that something makes changes to your system or gathers and reports information about you without first securing your agreement and consent to do so.

What Qualifies as Spyware?

Microsoft offers some great clues as to what else qualifies as spyware on a Web page entitled "What you can do about spyware and other unwanted software" (see the next On the Web icon for the URL). It makes some valuable points about where spyware comes from and how it behaves, noting that spyware is often picked up when making free downloads (such as free games, tools, utilities, and so forth). It also points out that the information that spyware gathers ranges from fairly innocuous, such as all the Web sites a user visits on a PC, to potentially dangerous, such as account or usernames and the passwords that go with them. Spyware can come from all kinds of sources, such as music- or file-sharing sites, free games from untrusted providers, or tools and utilities from unknown or untrusted sources.

On the Web

Read Microsoft's "What you can do about spyware and other unwanted software" online at `http://www.microsoft.com/athome/security/spyware/spywarewhat.mspx`

Likewise, spyware often travels in company with other software used to display advertisements, also known as adware (the subject of the next section in this chapter, in fact). Sometimes, adware includes spyware components, in that it also tracks user activity, preferences, and behavior, as well as coordinating a ceaseless stream of unwanted pop-ups on your PC's desktop.

Another key concept in deciding whether software on your PC is good or bad hinges on the notion of deception. Deceptive software changes settings or defaults, adds (or removes) components from your PC, and generally manages your system without seeking permission or explaining consequences and outcomes in advance so you can decide whether or not to proceed. Deceptive software often creeps onto systems during the installation of other free software, as with the music, games, tools, or utilities mentioned earlier. It can also be disclosed in long, deliberately obtuse or boring license agreements, which many users agree to without reading deeply or completely (and in that case, some spyware vendors have even been bold enough to claim "informed consent" on the part of hoodwinked users). Sometimes, so-called *active content* is covertly loaded when you visit certain

Web pages (active content basically represents a software-based, program-like capability that gets covertly installed on your machine).

Sometimes, a Web page may ask your permission to add an innocuous-sounding widget to your computer, ostensibly to permit that page to perform some useful function or service. This is when my earlier advice to "Just say No" to unsolicited downloads is worth recalling—and heeding! Likewise, anything that asks you to extend your trust permanently is probably worth denying as well. That means you should avoid clicking the check box in a download that reads "Always trust content from XYZ Corp" unless you're pretty darn sure you really can trust all content from that source (I don't even give Microsoft or Symantec that privilege on my desktops, to be absolutely candid, because I want to be informed and to grant permission before anything shows up there).

Signs of Potential Spyware Infestation

Although other, more subtle signs exist that spyware (or other unwanted software) has invaded your system, the most common and discernible symptoms are as follows:

- **Something new or unexpected shows up**—Whether in your Web browser or on your desktop, it could be anything from a new home or search page, to a toolbar, to a piece of software. Be grateful it's something you can see!
- **An increase in ads, pop-ups, or advertising**—Sometimes, you'll be overwhelmed with ads and it's easy to recognize that something's amiss; at other times, volume may just go up a little, or you'll find that closing one ad provokes another to appear, ad infinitum.
- **Performance slows down noticeably**—If your system starts running sluggishly without a good cause (indexing files, compacting your drives, or other intensive tasks), it may just be that the overhead of recording your actions or delivering oodles of ads are dragging down performance. Worse yet, buggy spyware or adware can make a previously stable system susceptible to crashing.

Among the many potential and unwanted effects of spyware, a little research into news coverage of this topic will document numerous cases of bogged-down systems or Internet access, theft of personal identity or other information, system crashes or instability, and loss of key system files or documents. While some of these are scarier than others, none is welcome news!

Cross-Reference

If your PC starts acting up for no good reason, something may indeed be up to no good on your system. In Chapter 4, you learn more about how to detect and cure spyware, adware, and other infestations that explains how to test and possibly confirm your suspicions, and how to clean up if there's a need.

Even as I'm writing this chapter, the news is full of stories about spyware, adware, and so forth. Scanning relevant headlines, I found items like "One in three PCs hosts spyware or Trojans" and "PCs infested with 30 pieces of spyware" in the recent past. If anything, a review of historical trends in such reporting shows things are getting worse over time, not better.

Understanding Adware and Pop-Ups

If spyware's job is to covertly track and report on user activity or data, *adware's* job is to bring advertising to your desktop — ready, willing, and able to deal with it or not. I want to turn once again to Whatis.com for its take on this term:

> Adware is any software application in which advertising banners are displayed while the program is running. The authors of these applications include additional code that delivers the ads, which can be viewed through pop-up windows or through a bar that appears on a computer screen. The justification for adware is that it helps recover programming development cost and helps to hold down the cost for the user.
>
> Adware has been criticized for occasionally including code that tracks a user's personal information and passes it on to third parties, without the user's authorization or knowledge. This practice has been dubbed spyware and has prompted an outcry from computer security and privacy advocates, including the Electronic Privacy Information Center. (`http://searchsmallbizit.techtarget.com/sDefinition/0,,sid44_gci521293,00.html`)

Here again, you can see a profound tendency for adware and spyware to travel together, if they're not bundled into the same unwanted programs.

In the introduction to this chapter, I discussed the notion of a one-pixel Web page, which creates a running instance of a Web browser on your computer without showing you anything you can see on your desktop. In actuality, it's not that there's nothing there; rather, what's there is just so small you can't really see it. But what these one-pixel windows provide is a constant presence on your computer, thereby creating a launch pad for invoking ad after ad after ad.

Though not everybody objects to all advertisements per se, plenty of unsavory ads — often of an overtly and offensively sexual nature that nobody would want a minor child to see (and which most adults would gladly skip, too) — can pop up on an unprotected desktop. The trick is to avoid adware sites whenever possible, and to know how to escape when ads run amok and just won't stop popping up on your desktop. Only experience can teach the former (but my recommendations on anti-spyware and anti-adware tools will protect you to a large extent, should you choose to follow them).

Using Task Manager to Halt a Pop-up Invasion

If you ever find yourself in a situation in which ads are popping up faster than you can close browser windows with your mouse, here's a trick you can try in the form of a step-by-step example.

Note

For the examples throughout this book, I assume readers are using Microsoft Windows XP, with Service Pack 2 (SP2) or later installed on that machine. Some of the details in step-by-steps will differ if you're using a different version of Windows. It's also worth noting that even though Windows XP SP2 is by no means a perfect operating system, it appears to be the most secure version of Windows Microsoft has ever produced. If you're using an older version of Windows, especially something older than Windows 2000 or Windows Me, it's probably time to think long and hard about upgrading your operating system, and probably your hardware, too, because Windows XP's processing requirements (64MB RAM minimum, 128MB or more RAM recommended, 300 MHz Pentium/Celeron or AMD K6/Athlon/Duron processor or better, 1.5GB or more of free hard disk space, Super VGA [800x600] graphics display and adapter, and keyboard and

Microsoft-compatible mouse) are more than what most older systems include. See `www.microsoft.com/windowsxp/` for more details on Windows XP Home and Professional requirements.

If you click your way through these steps, or find a workable analog on your version of Windows, you can kill your Web browser and thereby bring a pop-up invasion to a screeching halt:

1. Right-click on any open area on your Windows taskbar (by default, it's at the bottom of your screen). This action produces a pop-up menu, as shown in Figure 1-3.

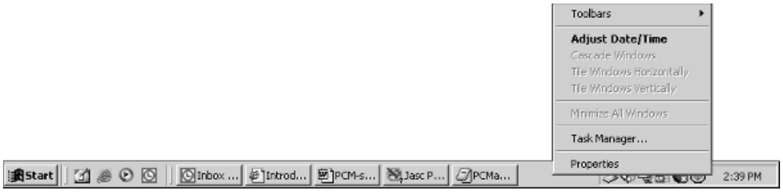


Figure 1-3: Right-clicking on the Windows taskbar produces a pop-up menu from which you can launch Task Manager.

2. On the pop-up menu, select the entry labeled Task Manager . . . .
3. When Windows Task Manager opens, click the Processes tab, if it's not already selected (Figure 1-4 shows Task Manager with the Processes tab selected).

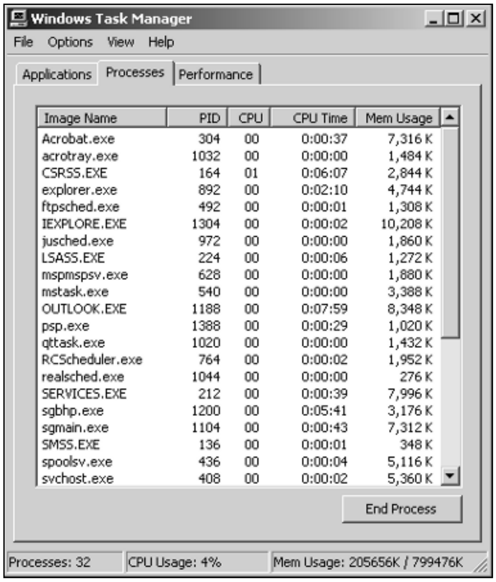


Image Name	PID	CPU	CPU Time	Mem Usage
Acrobat.exe	304	00	0:00:37	7,316 K
acrotray.exe	1032	00	0:00:00	1,484 K
CSRSS.EXE	164	01	0:06:07	2,844 K
explorer.exe	892	00	0:02:10	4,744 K
ftpsched.exe	492	00	0:00:01	1,308 K
IEXPLORE.EXE	1304	00	0:00:02	10,208 K
jusched.exe	972	00	0:00:00	1,860 K
LSASS.EXE	224	00	0:00:06	1,272 K
mspmspsv.exe	628	00	0:00:00	1,880 K
mstask.exe	540	00	0:00:00	3,388 K
OUTLOOK.EXE	1188	00	0:07:59	8,348 K
psp.exe	1388	00	0:00:29	1,020 K
qttask.exe	1020	00	0:00:00	1,432 K
RCScheduler.exe	764	00	0:00:02	1,952 K
realsched.exe	1044	00	0:00:00	276 K
SERVICES.EXE	212	00	0:00:39	7,996 K
sgbhp.exe	1200	00	0:05:41	3,176 K
sgmain.exe	1104	00	0:00:43	7,312 K
SMSS.EXE	136	00	0:00:01	348 K
spoolsv.exe	436	00	0:00:04	5,116 K
svchost.exe	408	00	0:00:02	5,360 K

Processes: 32 | CPU Usage: 4% | Mem Usage: 205656K / 799476K

Figure 1-4: The Task Manager display varies by which tab is selected; here, it's the Processes tab, which is the one you want.

4. In the Image Name list, select any line that reads `IEXPLORE.EXE` (or whatever the name for your Web browser's executable process happens to be — for example `mozilla.exe` for Mozilla, `opera.exe` for Opera, and `firefox.exe` for Firefox), and then click the End Process button.
5. Confirm that you do indeed want to end the process by clicking the Yes button on the subsequent screen.

Caution

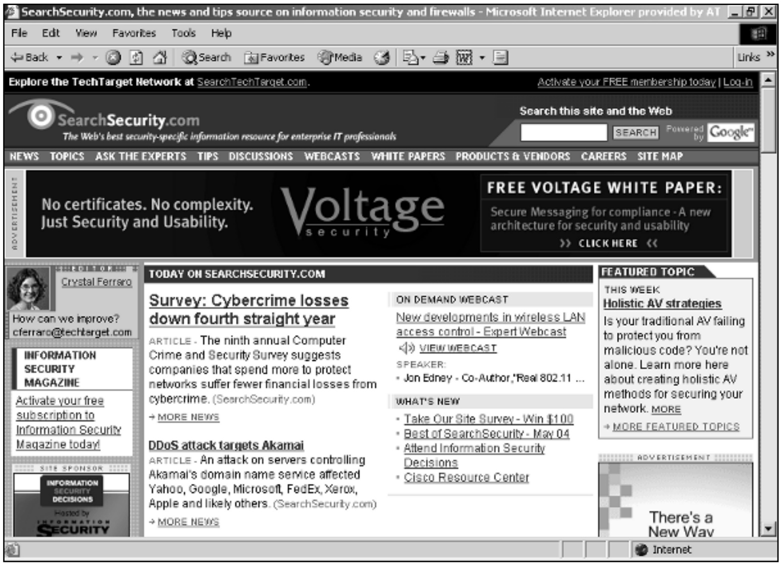
Clicking the End Process button as directed in the preceding step-by-step list shuts down the process that all open Web browser windows share. If you do this, you'll lose any work you may not yet have saved in whatever browser windows you opened yourself. But this is a sure way to stop an ad invasion, so it's worth knowing. It's strictly an emergency move, but may come in handy some day. Indeed, if it weren't the case that every pop-up that appears on your desktop also creates an application instance in the Task Manager Applications tab view, I would suggest you kill things there instead — but when that view is crammed full of a dozen or more instances of the same thing, with more popping up all the time, desperate moves like the one described here really do make sense.

Of Banners and Pop-Ups

Adware typically brings advertisements to users in one of two forms: banners and pop-ups. Of the two, banners are less objectionable in the way they appear in your Web browser, though their content may be just as unwanted as that in any pop-up.

Banners are advertisements that appear within the normal frame of a Web page. Web site operators sell ads for these spaces, which often occur at the top of most pages, or in areas along the right-hand or left-hand sides of a page, just like magazines sell print ads. As you can always flip the page in a magazine, so can you also scroll away from such ads on a Web site (though some top-of-page banners do use frames to remain in view even so). Figure 1-5 shows a banner on the top of a Web page on a well-behaved Web site: It's labeled on the left-hand side as an advertisement, and you can scroll away from it if you like. Notice the other banner on the lower right, of which you can see only the top edge.

Pop-ups appear in separate browser windows above the Web page you were looking at before they showed up. Normally, you must close the pop-up to return to that page and continue reading, scanning, or whatever else you might have been doing. One or two pop-ups can be annoying; a continuing stream of pop-ups can be overwhelming and infuriating. Figure 1-6 shows a pop-up on an otherwise favorite site where every acronym known to man can be expanded. Another type of ad, called a *pop-under*, appears underneath the open window, only to be discovered later when the covering window is closed. Also, one browser window can deliberately open another window when following a script or executing active content, so not all additional windows are pop-ups or unwanted (there's lots more detail on this subject in Chapter 6, which takes pop-ups as its entire focus).


SearchSecurity.com, the news and tips source on information security and firewalls - Microsoft Internet Explorer provided by AT
File Edit View Favorites Tools Help
Back Search Favorites Media
Links
Explore the TechTarget Network at SearchTechTarget.com.
Activate your FREE membership today | Log-in
SearchSecurity.com
The Web's best security-specific information resource for enterprise IT professionals
Search this site and the Web
SEARCH
Powered by Google
NEWS TOPICS ASK THE EXPERTS TIPS DISCUSSIONS WEBCASTS WHITE PAPERS PRODUCTS & VENDORS CAREERS SITE MAP
ADVERTISEMENT
No certificates. No complexity. Just Security and Usability.
Voltage security
FREE VOLTAGE WHITE PAPER:
Secure Messaging for compliance - A new architecture for security and usability
>> CLICK HERE <<
EDITOR
Crystal Ferraro
How can we improve?
cferraro@techtarget.com
INFORMATION SECURITY MAGAZINE
Activate your free subscription to Information Security Magazine today!
SITE SPONSOR
INFORMATION SECURITY DECISIONS
Hosted by INFORMATION SECURITY
ADVERTISEMENT
There's a New Way
Internet

TODAY ON SEARCHSECURITY.COM

Survey: Cybercrime losses down fourth straight year

ARTICLE - The ninth annual Computer Crime and Security Survey suggests companies that spend more to protect networks suffer fewer financial losses from cybercrime. (SearchSecurity.com)

→ MORE NEWS

DDoS attack targets Akamai

ARTICLE - An attack on servers controlling Akamai's domain name service affected Yahoo, Google, Microsoft, FedEx, Xerox, Apple and likely others. (SearchSecurity.com)

→ MORE NEWS

ON DEMAND WEBCAST

New developments in wireless LAN access control - Expert Webcast

VIEW WEBCAST

SPEAKER:

- Jon Edney - Co-Author,"Real 802.11 ...

WHAT'S NEW

- Take Our Site Survey - Win $100
- Best of SearchSecurity - May 04
- Attend Information Security Decisions
- Cisco Resource Center

FEATURED TOPIC

THIS WEEK

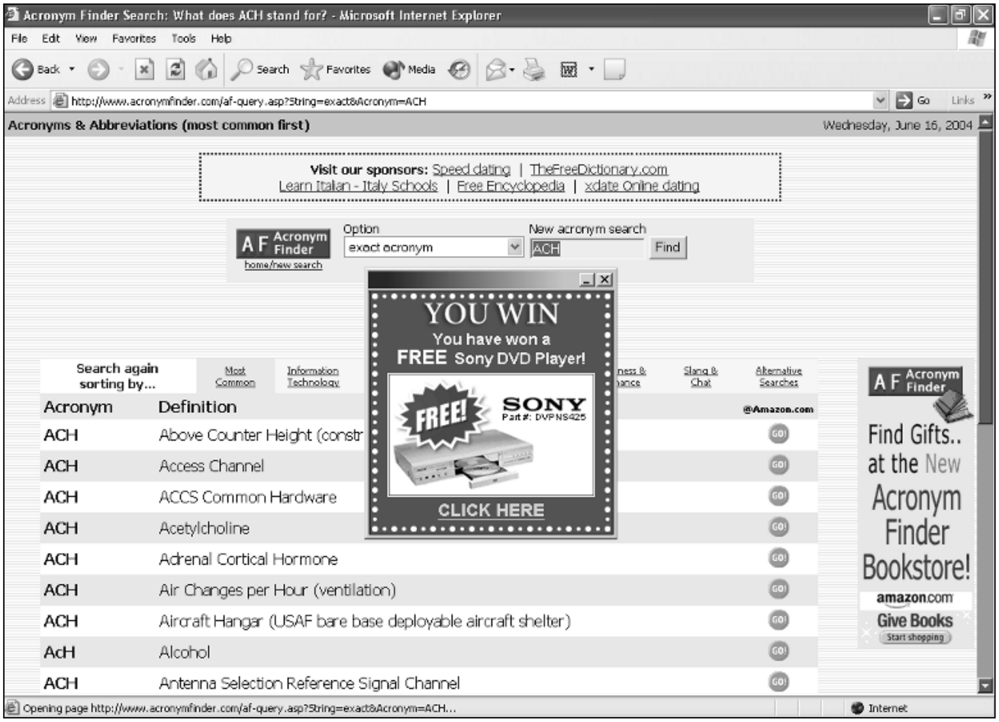
Holistic AV strategies

Is your traditional AV failing to protect you from malicious code? You're not alone. Learn more here about creating holistic AV methods for securing your network. MORE

→ MORE FEATURED TOPICS

Figure 1-5: Banners appear inside a normal Web page frame, and aren't usually as obnoxious as pop-ups.

Reprinted by permission of Tech Target, Inc.


Acronym Finder Search: What does ACH stand for? - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.acronymfinder.com/af-query.asp?String=exact&Acronym=ACH
Go Links
AF Acronym Finder
home/new search
Option
exact acronym
New acronym search
ACH
Find
YOU WIN
You have won a FREE Sony DVD Player!
FREE!
SONY Part #: DVPNS425
CLICK HERE
Search again sorting by...
Most Common
Information Technology
ness & ance
Slang & Chat
Alternative Searches
@Amazon.com
GO!
AF Acronym Finder
Find Gifts.. at the New Acronym Finder Bookstore!
amazon.com
Give Books
Start shopping
Opening page http://www.acronymfinder.com/af-query.asp?String=exact&Acronym=ACH...
Internet

Acronyms & Abbreviations (most common first)

Wednesday, June 16, 2004

Visit our sponsors: Speed dating | TheFreeDictionary.com
Learn Italian - Italy Schools | Free Encyclopedia | xdate Online dating

Acronym	Definition
ACH	Above Counter Height (constr
ACH	Access Channel
ACH	ACCS Common Hardware
ACH	Acetylcholine
ACH	Adrenal Cortical Hormone
ACH	Air Changes per Hour (ventilation)
ACH	Aircraft Hangar (USAF bare base deployable aircraft shelter)
AcH	Alcohol
ACH	Antenna Selection Reference Signal Channel

Figure 1-6: The pop-up ad in this figure says you've won a free DVD player! Wanna bet?

Good news for users of Windows XP who install SP2: Not only does the new and improved version of IE 6 include a pop-up blocker that works pretty well (see my discussion of its test results in Chapter 6 for more details), but it's also turned on by default. Thus, once you upgrade (or after you've upgraded) you won't have to put up with such distractions any more unless you actually want to see them.

Cross-Reference

Other kinds of pop-ups besides ads sometimes occur on PCs. These include instant messaging windows, Windows Messenger windows, and other kinds of pop-ups that Windows itself or other applications enable. You learn more about how to recognize and deal with these in Chapters 4 and 6.

Understanding Spam

The exact origins of the term *spam*, as commonly used to identify and denigrate unsolicited e-mail, are a matter of some debate. Most experts tend to mention the now-infamous Monty Python skit in which the word *spam* represents most of what's available on a restaurant menu, wherein the term's sheer repetition becomes thoroughly maddening long before the skit finally ends. Some of the same qualities still adhere to the e-mail variety of spam — in fact, many experts now believe that spam makes up more than 70 percent of all e-mail traffic on the Internet.

Here's the Whatis.com definition for spam:

> Spam is unsolicited e-mail on the Internet. From the sender's point-of-view, it's a form of bulk mail, often to a list obtained from a spambot or to a list obtained by companies that specialize in creating e-mail distribution lists. To the receiver, it usually seems like junk e-mail. It's roughly equivalent to unsolicited telephone marketing calls except that the user pays for part of the message because everyone shares the cost of maintaining the Internet. Spammers typically send a piece of e-mail to a distribution list in the millions, expecting that only a tiny number of readers will respond to their offer. Spam has become a major problem for all Internet users. (`http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci213031,00.html`)

To help clarify the Whatis.com definition, a *spambot* (a contraction of "spam robot") is a type of software robot that cruises the Web, reading all the pages it can find. As it does, it extracts all e-mail addresses it finds and writes them to a file. Periodically, the spambot's e-mail address file is harvested and used to add to bulk e-mail distribution lists (which often number in the millions of recipients, as the Whatis.com definition indicates).

However the bulk e-mails that send spam obtain their distribution lists, those recipients are almost always united in their distaste for e-mails of that type. But because some miniscule percentage of the population that such e-mail targets apparently bites at whatever's offered, lots of companies — many of them located outside the United States, Canada, and the European Union to get beyond reach of anti-spam laws now in effect in those parts of the world — continue to broadcast spam to the masses.

Spam is also something of a triple-whammy.

- First, by itself spam e-mail is unwanted and causes Internet congestion, consumes e-mail server resources, and generally ticks off a lot of people.
- Second, many forms of spam originate from running malware programs (more on this in Chapter 2) that send e-mail with infected attachments so they can reproduce and keep spreading.

Caution

This helps to explain one of the golden rules of e-mail security: *Never* open an attachment you don't expect to receive, even if it claims to be from a friend or family member.

Numerous clever e-mail-based infections harvest e-mail address books on the computers they infect, then mail themselves to everyone listed therein. To make matters more interesting, this kind of spam often claims to originate from a randomly selected harvested address. Thus, somebody you know (and trust) whose address also appears in a harvested address book can be identified as the sender of an infected e-mail message.

- Third, many e-mail servers with built-in attachment screening capabilities automatically send "warning messages" to senders identified in incoming messages when infection is detected or suspected. This is all well and good when such notification warns a sender about a real infection. But when incoming e-mail uses harvested addresses from innocent third parties, the original spam is doubled when a bogus infection report is sent to somebody who's probably not infected!

Given the astonishing volume and pervasive presence of spam, numerous short-term solutions are possible. Many companies or individuals now route their e-mail through special spam-screening services to clean out the worst of the spam before accepting incoming deliveries. Likewise, most modern e-mail software — including that used on e-mail servers to store and forward messages, and that used on e-mail clients so users can read mail on their desktops — includes all kinds of filters and blocks that can also hunt out and eliminate obvious spam before it shows up (or stays) in somebody's inbox.

The real problem with spam is human ingenuity. It's become a kind of cops-and-robbers game, in that as the good guys come up with more and better ways to identify and block spam from being delivered, the bad guys come up with more and better ways to circumvent identification and sneak into your inbox anyway. In fact, it's the unwanted, covert, and unsolicited nature of spam that permits me to lump it in with spyware and adware, because all of these items find ways to weasel onto computers despite reasonable attempts to keep them away.

Resources

For more discussion of the depth of the problem, you can turn to three good online articles:

Jacques, Robert. "One in three PCs hosts spyware or Trojans." vnunet.com, June 16, 2004, www.vnunet.com/news/1155923. A survey of 650,000 consumer PCs turns up 18 million instances of spyware.

Jacques, Robert. "PCs infested with 30 pieces of spyware." vnunet.com, April 16, 2004, www.vnunet.com/news/1154438. Most PCs can easily carry as many as 30 pieces of spyware; over 90 percent of machines surveyed show signs of infection.

Thompson, Roger. "We Must Beat Spyware." eweek.com, August 9, 2004.

Additionally, Steve Gibson is a long-time computer wizard who has done a lot of interesting work in the area of computer security including with spyware and adware. His OptOut Web pages are a must-read on this general topic. His free tool is both trustworthy and a real gem: http://grc.com/optout.htm.

Summary

As people venture onto the Internet, they soon learn that unwanted, uninvited, and downright sneaky software, messages, and data elements find their way onto their computers. Without taking appropriate preventive measures, and practicing safe computing, it's easy to catch something you'd rather not keep. But when unexpected changes, performance slowdowns, or lots of ads start showing up on a PC, it's time to start wondering if something's up to no good on that machine. In this chapter, you learned about three potential forms of unwanted software or data to which many PCs can fall prey:

- **Spyware** — which generally installs itself on computers unannounced, and gathers data about user activities, Web sites visited, preferences, (and sometimes more).
- **Adware** — which finds ways to make your computer show you lots of advertisements, which can come either in the form of banners (inline text and graphics inside Web pages you visit) or pop-ups (separate Web browser windows that come between you and your work, sometimes in great numbers).
- **Spam** — unsolicited e-mail that can show up in your inbox from bulk e-mailers trying to sell or tell you something you probably don't want to know, or from malware that's trying to reproduce from inside as many inboxes as possible.

In Chapter 2, you learn more about malicious software, or malware, including viruses, worms, Trojans, and other nasties that can not only move in and start using your computer without permission, but that can also wreak havoc on the systems they infect.