17

WEB BUGS, ADWARE, POP-UPS, AND SPYWARE

IN THE WORLD OF ADVERTISING, NOTHING IS REALLY FREE. When you listen to a radio or watch a television show, advertisers pay the costs and earn the right to broadcast their messages any time they want. Most people tolerate radio and television advertising since they've grown accustomed to its constant interruptions.

However, in the world of the Internet, people have a much lower tolerance level for advertisements. While advertisements pay for many free web hosting services and free or low-cost Internet services, there's a fine line between product promotion and invasion of privacy. When you hear or see a commercial on radio or television, you can freely ignore it. Unfortunately, advertisements on the Internet aren't always like that.

Ideally, an Internet advertisement would pop up once and give you the option of making it go away. Instead, Internet advertisements not only pop-up (and keep popping up over and over again), but they may also track which web pages you visit, to determine your preferences, which would be like having a radio or TV that could peek into your living room to see which brand of potato chips you might be eating at the moment. To intrude upon your privacy, Internet advertisers use a variety of tools including web bugs, adware, and a never-ending cascade of pop-up windows.

> Technological progress has merely provided us with more efficient means for going backwards.
>
> —ALDOUS HUXLEY

WATCHING OUT FOR WEB BUGS

Advertisers always need to know how effective their current marketing campaign may be. Since the Internet spans the world, it's nearly impossible to tell how many people looked at a particular ad and who they might be. To solve these two problems, advertisers created *web bugs*.

Tracking the websites you visit

When you visit a website, your browser asks the website server to send your computer all the text and graphic images that make up the web page. Thus, every webserver needs to know the IP address of your computer so it knows where to send the text and graphics.

When your browser receives information about a web page, that information appears in the form of *HTML* (Hypertext Markup Language) code, which tells your browser exactly how to display and position text and graphics. The specific HTML code that your browser receives from a web page defines the name of the graphic file, its size, and the name of the server it came from. In the following HTML example, the graphic file is called dotclear.gif, its width and height are both one pixel, and the server it came from is http://ad.doubleclick.net:

```
<IMG SRC=http://ad.doubleclick.net/dotclear.gif width=1 height=1>
```

Web bugs hide on ordinary web pages as invisible, one pixel by one pixel size images so you won't notice when you're being tracked. When the server sends the web bug to your browser, the server can immediately identify the following:

- The IP address of the computer that fetched the web bug
- The specific web page that contains the web bug (useful for seeing which web pages someone might have visited)
- The time and date the web bug was retrieved
- The type of browser that fetched the web bug

At the simplest level, web bugs help advertisers determine how many people have visited a particular website and viewed a particular web page. On a more insidious level, web bugs can work with cookies to track which websites each person visits so they can display advertisements specific to that individual.

Using web bugs in spam

Web bugs can sometimes appear in spam too (see Chapter 16), buried inside email so an advertiser can see how many times people read (or at least open) a particular message. If someone doesn't bother to view a web bug in an email, this tells the advertiser that the email address may not be valid or that this particular person didn't bother to read it. In either case, the advertiser will likely remove that person's email address to avoid wasting time sending advertisements that no one will read.

Some companies accused of planting web bugs in email marketing messages include Experian (http://www.experian.com), Digital Impact (http://www.digitalimpact.com), and Responsys (http://www.responsys.com). By browsing their websites, you can get a better idea of how email marketing firms work, and how they might target you sometime in the future.

Bugging newsgroups

Besides slipping web bugs in target email messages, it's possible to embed a web bug into a newsgroup message, too. Not only could this tell an advertiser how many times someone looked at the ad, but it can also track down the specific IP address of each person who downloaded the web bug.

The extremely paranoid believe that web bugs can identify people who subscribe to politically incorrect newsgroups, while less-conspiracy-minded people believe that governments might use web bugs to track down anyone trading child pornography or illegal MP3 files. Since web bugs are invisible, and you aren't likely to even notice their presence, it's possible that a web bug has already given away your IP address and browsing habits to a faceless corporation without you even knowing it.

Protecting yourself against web bugs

Since web bugs often work with cookies to track your browsing habits, your first line of defense is to make sure your browser refuses all cookies. Since this won't always be practical, especially when you visit online shopping sites, visit Bugnosis.org (http://www.bugnosis.org) and download their free Bugnosis tool (see Figure 17-1).

Figure 17-1

The free Bugnosis tool can identify websites that use web bugs.

As you browse through different websites, Bugnosis scans each web page, gives an audible warning, and highlights suspicious web bugs on a web page. By using Bugnosis with Internet Explorer, you can see how prevalent web bugs may actually be, especially if Bugnosis finds suspicious GIF images on your favorite websites, such as the DM News site (http://www.dmnews.com), the *Detroit News* (http://www.detnews.com), or the *New York Times* (http://www.nytimes.com).

ADWARE—SOFTWARE WITH BUILT-IN ADVERTISING

For the longest time, there were four categories of software: commercial programs that you purchased before you could try them, shareware that you could try and purchase if you found it useful, freeware that you could use without ever paying for it (although the programmer retained the copyright), and public domain software that nobody owned so you could freely use it and modify it if you wanted.

When programmers wanted to make money selling a program, they often released their creations as shareware, so people all over the world could try it for free. If the program proved popular, they usually turned it into a commercial product.

Although a handful of shareware programs turned their creators into millionaires, many more simply earned a small amount of change for the programmers and that's it. To increase their odds of success, many shareware programmers decided to turn their creations into a new category of software dubbed *adware*.

As the name implies, adware displays advertisements as the program runs (see Figure 17-2). If you're connected to the Internet, the adware program may access a server and display an ever-changing array of advertisements every time you use the adware program.

Figure 17-2

Adware programs display advertisements every time you run the program.

By incorporating advertisements in their programs, programmers can ensure that they earn a certain amount of money whether people ultimately register and pay for the program or not. Advertisers love adware because it provides access to more potential customers. Unfortunately, the only people who don't seem to care for adware are the people using it.

By itself, adware can be annoying but harmless. However, instead of being content to just display advertisements, some adware programs secretly retrieve information from the user's computer and transmit this information back to the advertiser, which is a characteristic of programs known as *spyware*. This information could be as simple as the type and version of the operating system on your computer, or your IP address along with a list of all the cookies stored on your computer, which an advertiser can examine to determine your browsing habits. When you run an adware program, it's possible that the adware program could be transmitting your browsing and online shopping habits to the advertiser without your consent, which can be as disconcerting as finding a stranger in your kitchen making a note of all the name-brand food products you bought in the past three days.

For more information about adware, visit the Adware.info site (http://www.adware.info). In case you're curious about the types of companies that help programmers develop adware, visit the Software Marketing Resource page (http://www.softwaremarketingresource.com/adware.html).

Defending against adware

Because so many people find the idea of their programs bombarding them with advertisements less than appealing, most adware programs disguise their built-in advertising. To help you find adware programs that may be lurking on your computer, download a free copy of Ad-aware, as shown in Figure 17-3 (http://www.lavasoft-usa.com).

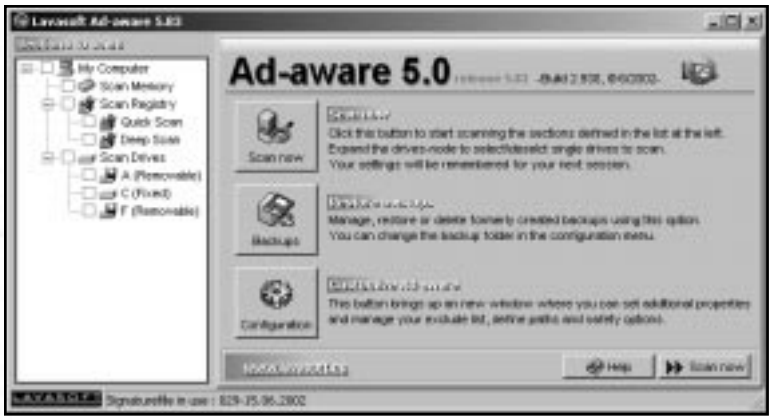

Figure 17-3

Ad-aware can detect and remove adware programs that may be hidden on your computer.

Like an antivirus program, Ad-aware scans your memory, hard disk, and registry file to look for files that may be unique to known adware programs, such as CuteFTP, NetSonic, or Go!Zilla. Once it finds a known adware program, Ad-aware gives you the option of removing it completely from your system.

For another adware removal tool, visit Bulletproof Software (http://www.bulletproofsoft.com) and try their BPS Spyware/Adware Remover. Unlike Ad-aware, BPS Spyware/Adware Remover isn't free, but it does include features to scan and remove any spyware it finds on your computer. (For more information about spyware, see the "Detecting Spyware" section later in this chapter.)

Better yet, visit the Spychecker site (http://www.spychecker.com) before you download that shareware or freeware program. Spychecker has a database of all known adware programs, so you can find out if a program will spy on you before you decide to download and install it.

Adware vs. Ad-aware

Not surprisingly, Ad-aware's efforts have upset a great many advertisers and adware programmers, who see Ad-aware as a threat to their sources of income. One adware program in particular, RadLight version 3.03 release 5.0 (http://www.radlight.net), would scan your hard disk for Ad-aware. If it found Ad-aware lurking on your computer, RadLight would secretly uninstall it without your knowledge. That way it could continue flooding your computer with advertisements and transmitting your data back to the advertiser without Ad-aware's interference.

At the time Igor Janos, author of the RadLight software claimed, "As Ad-aware's behavior was hostile to our bundle, I had to defend."

This immediately set up a backlash against RadLight, so the later version of RadLight 3.03 release 5.2 gives you the option of uninstalling Ad-aware or not. To further distance itself from the negative label of "adware," RadLight now promotes its ad-supported version as "helpware," as if advertisements somehow "help" the user in any way. While this compromise isn't perfect, at least it gives you, the user, a choice in the matter. Naturally, a far more effective choice is to simply avoid using any adware programs at all, while using the Ad-aware program regularly to keep your computer free of such annoyances.

Killing ads in AOL Instant Messenger

With ads popping up in shareware programs, email, and web pages, it was inevitable that ads would start appearing in instant messenger programs. Ads have started appearing in AOL Instant Messenger (AIM), one of the more popular instant messenger services around. As you chat, ads pop up in your AOL Instant Messenger window.

In case you find these ads annoying, you can try to manually kill them by editing the "aim.odl" file with any text editor, such as Notepad. Look for the following code:

```
on_group(5)
{
load_ocm          advert      required
```

```
}
on_group(11)
{
load_ocm           advert      required
}
```

Just put semicolons in front of the load_ocm lines, like this:

```
on_group(5)
{
;    load_ocm      advert      required
}
on_group(11)
{
;    load_ocm      advert      required
}
```

Save the file as "aim.odl" in its original location, and AOL Instant Messenger should no longer annoy you with advertisements. If you don't want to mess around with editing strange files on your hard disk, grab a copy of the DeadAIM program (http://www.jdennis.net/index2.htm), which can remove those annoying advertisements from AOL Instant Messenger automatically.

STOPPING POP-UP/POP-UNDER ADVERTISEMENTS

In the beginning, advertisers relied on banner ads strategically placed around a web page. However, they found that people routinely ignored them, so to force people to at least acknowledge the advertisement's existence, they created pop-up and pop-under ads.

Pop-up ads blanket your screen with windows, advertising anything from lower mortgage rates to vacation trip giveaways (see Figure 17-4). Since these windows cover any web page you're currently browsing, you can't see anything until you close the pop-up ad window. Pornography advertisers have created particularly annoying pop-up ads that spawn three or four more pop-up windows every time you close one.

Pop-under ads are a bit more subtle. They also appear in little windows all over your screen, but they hide under your currently displayed web page, so you won't even see them. The moment you close your browser, though, those pop-under ads seem to magically appear, cluttering up your screen. Since pop-under ads don't intrude upon your browsing activities, advertisers hope that more people will be more receptive to them.

One of the largest email and Internet marketing companies is DoubleClick (http://www.doubleclick.com). It offers the public a way to store a special cookie from DoubleClick that prevents your computer from receiving any more advertisements

Figure 17-4

Pop-up ads can keep appearing on your screen faster than you can get rid of them.

from DoubleClick. Just visit the DoubleClick site, click to view their Privacy Policy, and follow the directions to opt out from DoubleClick's advertising. Now you just have to worry about online advertising from other companies.

Even if you decide to opt-out from DoubleClick's ads, you may still find yourself bombarded by pop-up and pop-under advertisements. To learn how to stop pop-up and pop-under ads from wrecking your Internet experience, visit the Web Ad Blocking site (http://www.ecst.csuchico.edu/~atman/spam/adblock.shtml).

If you want to automatically block pop-up and pop-under ads from appearing, you'll need to get a pop-up blocker program. Go to WebAttack.com (http://www.webattack.com) or Tucows (http://www.tucows.com) and search for "pop-up blocker." Both sites offer plenty of free and shareware pop-up ad blockers, such as the one shown in Figure 17-5, and you can try to find the one you like best.

For a free way to block pop-up ads, stop using Internet Explorer or Netscape and grab a copy of Mozilla (http://www.mozilla.org) or Safari (http://www.apple.com). Both browsers offer commands that let you block pop-up ads from appearing and disturbing your web surfing experience.

DETECTING SPYWARE

The thought of unseen advertisers peeking at your browsing habits may unnerve you, but what may be more disconcerting is finding that someone you know,

Figure 17-5

A pop-up blocker like Stopzilla keeps track of all the pop-up ads it stops.

such as your boss, your spouse, or your parents, are secretly monitoring what you do on your computer through a desktop-monitoring program, otherwise known as *spyware*.

Spyware can capture screenshots of your activity, record every keystroke you type, track every program you use, and log how much time you spend using each program on the computer. Bosses use spyware to catch employees using their computers for personal activities, parents use spyware to make sure their kids don't visit forbidden sites, hackers use spyware to snare credit card numbers and passwords from unsuspecting victims, and spouses use spyware to gather proof that their husband or wife may be cheating on them. To see what type of spyware someone could plant on your computer, visit the Top Secret Software site (http://www.topsecret-software.com) and read about the different capabilities of various spyware programs.

Unlike ordinary programs that appear in a list of running programs tracked by the operating system, such as Windows XP, spyware programs bury themselves out of sight, so unsuspecting victims don't accidentally stumble across the program while it's running. Unless you suspect someone has planted spyware on your computer and you know where to look, chances are good that you'll never detect any spyware on your computer.

Several companies sell anti-spyware programs, such as Nitrous Anti-Spy (http://www.nitrousonline.com), PestPatrol (http://www.pestpatrol.com), SpyGuard (http://www.spyguard.com), and SpyCop (http://www.spycops.com). These programs, like the one shown in Figure 17-6, can search your hard disk for any traces of known spyware programs and keystroke loggers that someone may have slipped onto your computer.

WARNING: Anti-spyware programs will not be able to detect hardware-based keystroke loggers that connect between a computer and the keyboard.

Besides rooting through your hard disk for known spyware files, anti-spyware programs can also monitor the ports on your computer to detect any unauthorized communications being sent from your computer. Such clandestine communication is

Figure 17-6

Anti-spyware programs can keep someone from secretly monitoring your activity on the computer.

almost always the result of either adware, a remote access Trojan horse (see Chapter 8), or spyware, which may be trying to send a record of your activity to the email account of the person spying on you. An anti-spyware program can block such stealth communication from taking place, effectively shielding your privacy.

THE ONLY SURE WAY TO PROTECT YOUR PRIVACY

If you never connect to the Internet, you can protect yourself against the large majority of web bugs, adware, pop-up ads, and spyware. Since that isn't an option for many people, your next best solution is to understand how various threats to your privacy work, and then use protective programs to defend against each threat, such as Bugnosis, Ad-aware, and anti-spyware programs.

Maybe your computer isn't bugged, and maybe nobody is spying on you. But is it worth the risk of losing your privacy not to find out?