2

Protecting Your Security and Privacy

DO OR DIE:

- >> "Button up your overcoat..."
- >> Maintaining your privacy
- >> Passwords and master passwords
- >> Have a cookie or not, as you wish

How Firefox Protects Your Security

It used to be that the Internet was like a park in a small, friendly town. You could go there most any time of the day or night and have a good time without worrying about security or privacy. Now the Internet is still like a park, but it's a park in a big urban area and it's not always so friendly. There are some serious security threats out there: spyware, viruses, Trojan horses. If you'll be doing any serious surfing at all—and you are, or you wouldn't be reading this—you need to learn about ways to make things a little safer.

One of the biggest advantages that Firefox—and all other Mozilla-based products, for that matter—offers is that it's more secure than Internet Explorer. (Don't take my word for it; check out the U.S. government's Computer Emergency Readiness Team [US-CERT] warnings at http://www.kb.cert.org/vuls/id/713878. Their findings point out that there are "a number of significant vulnerabilities" with IE. Among other things, the report recommends using a different web browser.)

Here are some of the reasons that Firefox is more secure:

- Firefox is not integrated with Windows, so even if Firefox is compromised, viruses and trojan horses do not gain automatic access to many parts of Windows. The reverse is also true: if Windows is compromised, the attacking program does not necessarily gain access to Firefox.
- Firefox does not support VBScript and ActiveX, which are frequently used to exploit security holes in IE.
- Visiting a website with Firefox doesn't allow spyware or adware to be automatically installed.
- Firefox gives you complete control over web cookies.

These and many other reasons add up to a really great reason to use Firefox: you'll be safer.

Protecting Yourself on the Web

There are a number of problems to look out for on the web:

- **Viruses**, which are programs or scripts that get into your computer and cause damage in a myriad of ways
- **Worms**, which are like viruses that replicate independently over a network without any human intervention
- **Trojan horses**, which are programs that appear to be innocuous but that cause damage to your system when you run them

There's some overlap between these definitions. A worm may not have been designed to do harm but, owing to the number of instances on your computer, it could clog up your file system or damage your email files, which might classify it as a virus. Is a program that releases a worm but that doesn't cause damage to your system a worm or a trojan horse? While the distinctions are sometimes blurry, all of these are Bad Things from Bad People. You don't want them on your computer. Using a good anti-virus program (with up-to-date virus definitions) is essential. The biggest vector for viruses is any email program that automatically loads and runs scripts. Thunderbird, described later in this book, is much safer because, among other things, it doesn't load and run scripts unless you actively tell it to.

One of the most recent computer plagues is *spyware*. Spyware is programs or scripts that are installed without your explicit permission that sit quietly in the background and do things to your system that you don't want to be done. What kinds of things? Here are some of the basic types of spyware:

- **Adware** (also known as "popupware") is certainly the most common type of spyware. When you go online, the adware displays ads in popup windows (aka "popups") about all kinds of products: hair loss remedies, herbal Viagra substitutes, cheap car rentals, you name it. Adware usually also transmits information about your web surfing habits and preferences to someone collecting information about you, who then sells it to spammers and marketers so that you get hit with targeted spam and probably more popups. (This process is known as "data mining," and there are pieces of adware that are just data miners.)
- **Search hijackers** (also known as "browser hijackers" or just "hijackers") change your browser's home page and your preferred search engine to something you didn't plan on (usually porn sites or some cheesy web scam). Search hijackers are also frequently data miners, just like many versions of adware.
- **Keystroke loggers** are particularly nasty. While all the other types of spyware are busy trying to sell you stuff—stuff you really don't want, but still—or gather information about you so that other people can try to sell you stuff, keystroke loggers are tracking the actual keystrokes you enter on the computer. Anytime you log in to your email account to pay websites you patronize or (worst of all!) to your credit card site to make a payment, the keystroke logger records *everything* and then sends it to someone.

Note

Popups and how to suppress them are discussed in Chapter 3, aptly titled "Ridding Yourself of the Annoyances of the Web."

There are a few other classes of spyware—dialers that look for a phone line via a modem and then dial long distance 900 numbers to rack up bills on your account, for instance, or programs that look for Quicken on your computer and then have Quicken transfer money to someone else's bank account (as demonstrated by Germany's Computer Chaos Club in 1997)—but the bottom line is that spyware and the people who create or use it have no reason for continued existence on any planet that's discovered penicillin.

Fortunately, you can do a number of things to detect and remove spyware and to avoid it in the future. Some of the best detection tools for Windows are free: Ad-Aware SE Personal Edition from Lavasoft (www.lavasoftusa.com) and Spybot Search & Destroy (http://www.safer-networking.org) are my personal favorites. I use both of them, because each tends to catch some things that the other doesn't. I also use ZoneAlarm (www.zonealarm.com) as a software firewall so that I can see if something on my computer is trying to send information elsewhere. It's also free and cheap at twice the price.

Spyware is primarily a problem for Windows computers, but Mac users may want to try a product like MacScan (http://macscan.securemac.com). You might also want to look at general Mac security sites, such as MacSecurity.org (http://www.macsecurity.org) and SecureMac (http://www.securemac.com), for information on how best to protect your Mac. Linux users have nothing to fear: spyware is not an issue for Linux computers at this time.

To avoid getting spyware in the future, first use Firefox (you knew that was coming, didn't you?). Here's why: Microsoft's approach to designing Internet Explorer was an optimistic view of security. Internet Explorer provided the maxiumum amount of capability with the hope of providing mechanisms that could and would be used to avoid risks. Unfortunately, it didn't quite work that way: ActiveX lets people silently access the operating system, the browser itself, and applications, and the Security Zone Model can allow the silent downloading, installation, and execution of programs without your knowledge. Powerful stuff that you can use to do great things? Sure! But sadly, it doesn't have enough safeguards, and as a result, ActiveX and the Security Zone model are used together as the primary mechanism to deploy spyware.

Warning

Some spyware detection and removal programs actually don't do much of anything. Some of them are even loaded with spyware themselves. Before you install just any old spyware checker on your system, look around and see what people are saying about its effectiveness.

To be fair, Microsoft has recently addressed some of the issues in SP2 for Windows XP, but only a couple years after the dangers of Internet Explorer and its architecture were discussed in an article entitled "The Most Dangerous Software Ever Written" (www.networkmagazine.com/article/NMG20020701S0007). Worse, because Microsoft is focusing on Windows XP, over 200 million users of Windows 95, Windows 98, and Windows 2000 are being left out in the cold.

In contrast, Firefox takes a pessimistic, Murphyistic view of vulnerability: "Anything that can go wrong, will go wrong." Firefox attempts to create a firewall around the browser and remote content and other applications that might be available on the PC. In every case where potentially dangerous actions can happen, Firefox attempts to warn users about the risk. Furthermore, because Firefox doesn't support ActiveX and the security zone architecture, Firefox doesn't allow websites to install software automatically. Without the ability for websites to silently download and install spyware, Firefox has some immediate security advantages over Internet Explorer.

For further safety, don't put yourself in harm's way. Avoid software and websites that are likely to be infested with spyware. As you might expect, websites focusing on warez, porn, illicit mp3s, and file sharing are all likely to have spyware (you all look like nice people and would never go to places like these, but you need to know). Unfortunately, lots of sites that even a nice person like you might go to that also have spyware: online games, dating sites, contests, free software, and even some major companies' websites can all try to download spyware on your computer. The trick is to be cautious, use Firefox to filter out a lot of the spyware, use Ad-Aware and Spybot to check for spyware regularly (daily's not too often to check if you surf a lot), and use ZoneAlarm to watch what's trying to talk from your computer to elsewhere without your knowledge.

FRIDGE

Spyware can be bundled as part of another program so that the spyware installs when you install the program, but it's most commonly downloaded from websites. But just to be on the safe side, consider checking your system by running Spybot or Ad-Aware immediately after installing a new program. You should routinely check the Add/Remove applet in the Control Panel as well as checking your system's Pogram Files directory for things you don't recollect. (This is sort of like walking through your house and saying, "Where'd that vase come from?")

TOOL KIT

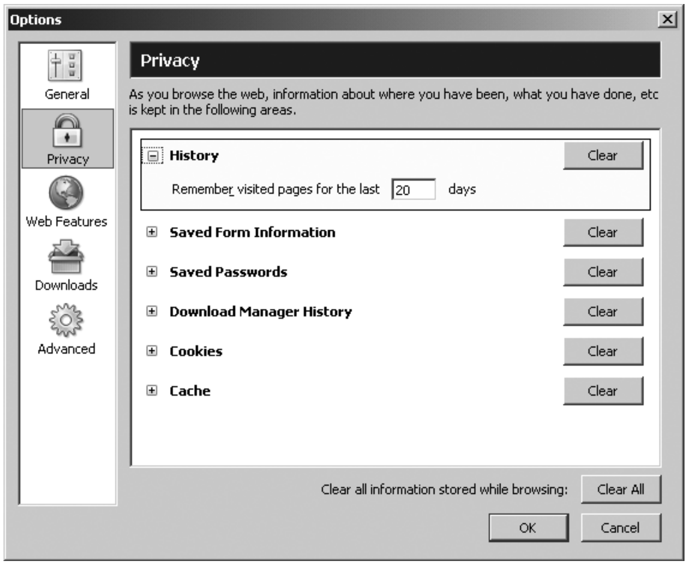
Dealing with the Windows Registry

If you're using Windows, you should also use a registry cleaner periodically to check for spyware as well as to clean up stray registry entries. Several good registry cleaners are available, the Norton Utilities version being one of the best-known, but you can find a variety of shareware registry cleaners through www.shareware.com. If you're really technically savvy, you may want to take a tour through your registry every so often using RegEdit. This is a really tedious job and it's not for the faint of heart, but it can help you find traces of buried spyware. Be sure to back up your registry before you touch anything in it.

Setting Privacy Options in Firefox

Now that you have learned how to set some of the basic Firefox options (refer to Chapter 1, "Getting Started," if necessary), you are ready to see how to set privacy options in Firefox.

To set privacy options, start by going to Tools | Options | Privacy. The Options screen with the Privacy options appears, as shown in Figure 2-1.



Privacy

As you browse the web, information about where you have been, what you have done, etc is kept in the following areas.

⊟ History

Remember visited pages for the last 20 days

⊞ Saved Form Information

⊞ Saved Passwords

⊞ Download Manager History

⊞ Cookies

⊞ Cache

Clear all information stored while browsing:

Figure 2-1

The Options screen with the Privacy options displayed.

As you browse the web, information on where you have been, what pages you have visited, and so on, is stored in Firefox. The privacy options in Firefox give you control over what's stored and for how long. In addition, you can set controls to exclude specific websites from doing potentially intrusive or insecure things on your computer.

The following sections show you how to set the security and privacy options on this screen. To display a specific option, expand a section by clicking the small + button to the left of the option.

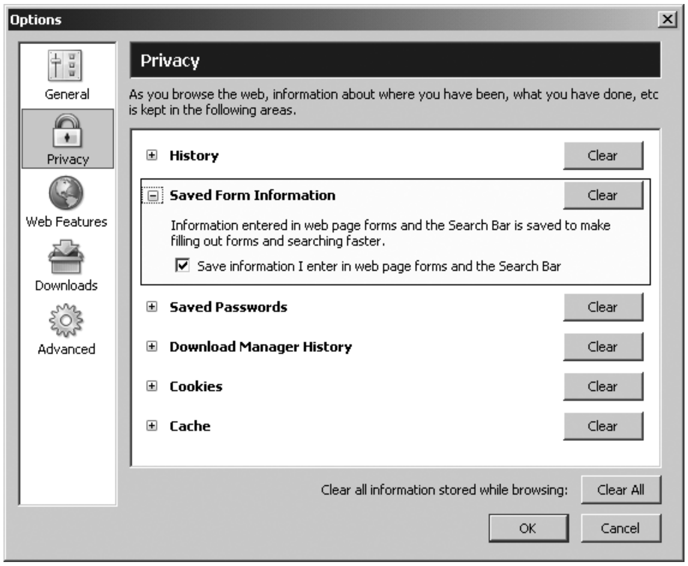
History

Firefox, like every other browser, tracks the pages you've visited and displays them in the History sidebar. You can set the number of days you want Firefox to remember your history (there's no practical upper limit of days). Clicking Clear clears all your surfing history up to the current page. If the button's grayed out, the history is already clear. (You'll read more about how the History sidebar works in Chapter 5, "Bookmarks and History.")

Before you get frisky and clear your history, keep in mind that Firefox changes the color of the links of web pages you've visited, but if you clear the history, all the links will look like you've never clicked them. If you're working through a large page of links, you may end up losing your place and revisiting websites because you have no point of reference for where you left off. Similarly, a Google search on a topic you look up frequently will no longer show what you've already looked at. The autocomplete information when you enter the first few characters of a web address is also cleared. If you can't remember the exact site address, Firefox won't be able to help you by suggesting all the different addresses you've entered that start the same way.

Saved Form Information

The Saved Form Information option (displayed in Figure 2-2) automatically saves information from web forms and the Firefox search bar. With this option on, common types of information such as your name, email address, address, and the like all show up on dropdown lists when you start entering information in a similar field—very convenient for quick form entry. In the same fashion, Firefox saves the things you enter in the search field. Just type the first few characters of a search entry you entered previously, and Firefox will proffer a list of search criteria that start with the same characters. If you don't want Firefox to save information, uncheck the box. Click **Clear** to wipe all the form information and search criteria you entered since the last time this was cleared.



As you browse the web, information about where you have been, what you have done, etc is kept in the following areas.

Information entered in web page forms and the Search Bar is saved to make filling out forms and searching faster.

☑ Save information I enter in web page forms and the Search Bar

Clear all information stored while browsing:

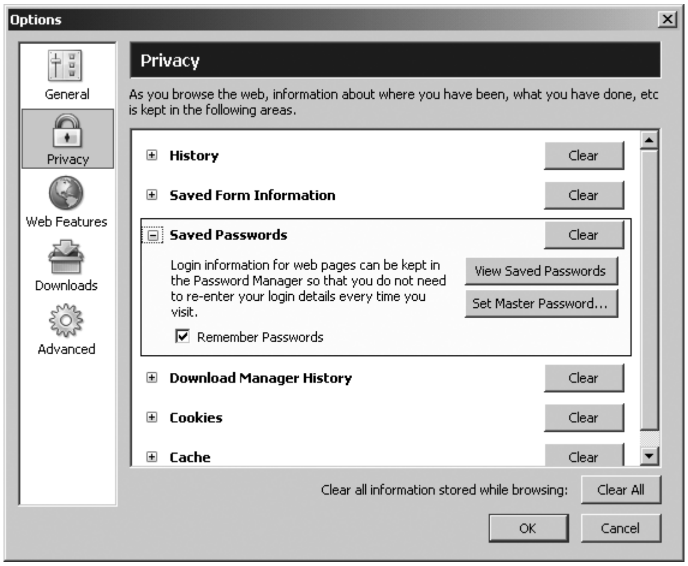
Figure 2-2

The Options screen with the Saved Forms Information option expanded.

Saving Passwords

If you're like me, you probably have one or two email accounts, online bill paying with your bank and a couple of credit card websites, an online game account, logins to a few job websites, a few web forums or listservs for professional and personal interests, and at least three or four other miscellaneous things. That's a lot of user IDs and passwords! It's a really bad idea to use the same password for everything—if someone cracks your password once, he'll have access to everything you do—but it's also a bad idea to write your passwords down somewhere—again, if someone finds your list, he'll have access to everything. But remember that having a dozen or more user ID/password combinations is a real pest. Better to have Firefox do the remembering for you.

The Saved Passwords option (shown in Figure 2-3), which is turned on by default, actually saves user IDs and passwords.



Privacy

As you browse the web, information about where you have been, what you have done, etc is kept in the following areas.

Login information for web pages can be kept in the Password Manager so that you do not need to re-enter your login details every time you visit.

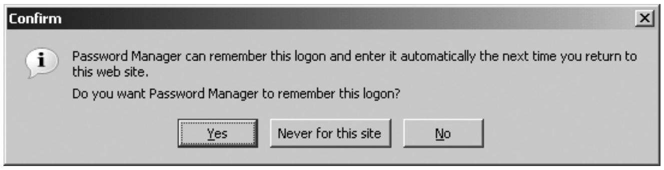
☑ Remember Passwords

Clear all information stored while browsing:

Figure 2-3

The Options screen with the Saved Passwords option expanded.

When you log in to a website, Firefox displays a dialog box (shown in Figure 2-4) and asks if you want to save the logon information. You can click **Yes** to save it, **No** to skip it this time, or **Never** for this site to disallow password saving for this site. As with previous options, you can click Clear to clear all the passwords in Firefox.



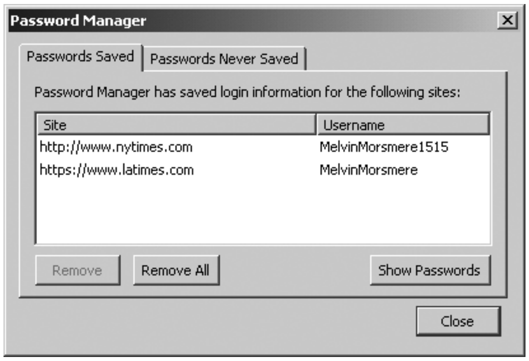
Password Manager can remember this logon and enter it automatically the next time you return to this web site.

Do you want Password Manager to remember this logon?

Figure 2-4

The Confirm dialog box for saved logon information.

You can examine and edit individual user IDs and passwords by clicking **View Saved Passwords**, which displays the Password Manager screen (shown in Figure 2-5). You can see the sites that have been saved and edit the list by highlighting the site(s) you want to delete and then clicking **Remove**. Clicking **Remove All** flushes all the saved sites and passwords, which is handy if you're cleaning traces from the computer.

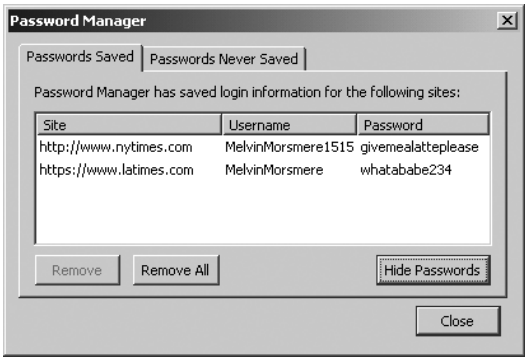


Password Manager has saved login information for the following sites:

Site	Username
http://www.nytimes.com	MelvinMorsmere1515
https://www.latimes.com	MelvinMorsmere

Figure 2-5

The Passwords Saved tab of Password Manager.

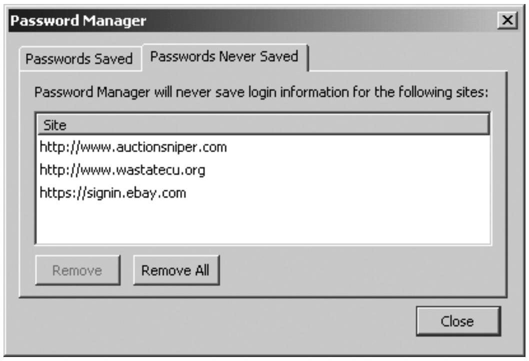


Password Manager has saved login information for the following sites:

Site	Username	Password
http://www.nytimes.com	MelvinMorsmere1515	givemealatteplease
https://www.latimes.com	MelvinMorsmere	whatababe234

Figure 2-6

The Passwords Saved tab with the passwords displayed.



Password Manager will never save login information for the following sites:

Site
http://www.auctionsniper.com
http://www.wastatecu.org
https://signin.ebay.com

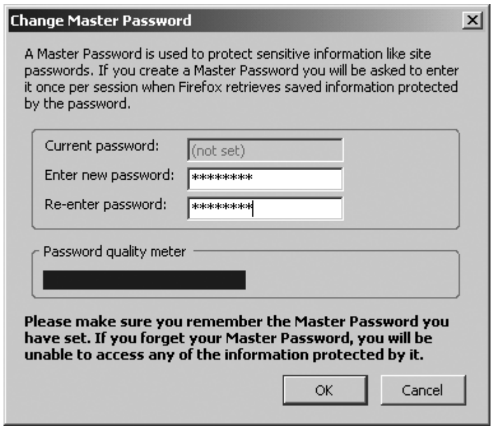
Figure 2-7

The Passwords Never Saved tab.

The default is for the Password Manager to show just the site and the user ID. You can also show the associated passwords by clicking **Show Passwords**, as shown in Figure 2-6. Hide the passwords again by clicking **Hide Passwords**.

You can also edit the sites you've designated to never save logon information for by clicking the **Passwords Never Saved** tab (shown in Figure 2-7). You can remove some or all of the websites by clicking **Remove** or **Remove All**, as you did before. When you are satisfied with your entries, click **Close**.

Having your logon information set up in Firefox is really handy. However, anyone who has access to your computer can get into the Password Manager and look up your account usernames and passwords. To prevent this, you can set a master password that locks the information in the Password Manager itself so that someone can't casually extract your logon information. To set a master password, click **Set Master Password** on the Options screen shown earlier in Figure 2-3 to display the Change Master Password screen, shown in Figure 2-8.



Change Master Password

A Master Password is used to protect sensitive information like site passwords. If you create a Master Password you will be asked to enter it once per session when Firefox retrieves saved information protected by the password.

Current password: (not set)
Enter new password: ********
Re-enter password: ********

Password quality meter

Please make sure you remember the Master Password you have set. If you forget your Master Password, you will be unable to access any of the information protected by it.

Figure 2-8
The Change Master Password screen.

The Change Master Password screen is much like any other password screen. The first time you set up a master password, you don't need to enter the current password. You do need to enter the password (which is case-sensitive, by the way) in both the new password fields. As usual, the characters are replaced with asterisks as you type. When the passwords match, the OK button is activated. Without the master password, the passwords aren't displayed in the Passwords Saved tab of the Password Manager, and you can't add or change any passwords.

One really slicko feature of the Change Master Password screen that I've never seen anywhere else is the password quality meter. Everyone's familiar with the idea of not using names of partners, children, or pets, birthdates, or common words like "secret," "keepout," or "spiderman." The password quality meter actually rates the value of your password on criteria such as mixing capital and lowercase letters, adding numbers and characters, and uncommon groupings.

TOOL KIT

What to Do If You Forget Your Master Password

If, despite everything, you've forgotten your password (hey, it happens—I've even forgotten passwords an *hour* after I set them up!), things aren't hopeless. With a little hacking, you can reset the master password on your computer.

Start by closing Firefox, and then go to where your `key3.db` file is stored on your computer. The `key3.db` file is where the master password information is stored.

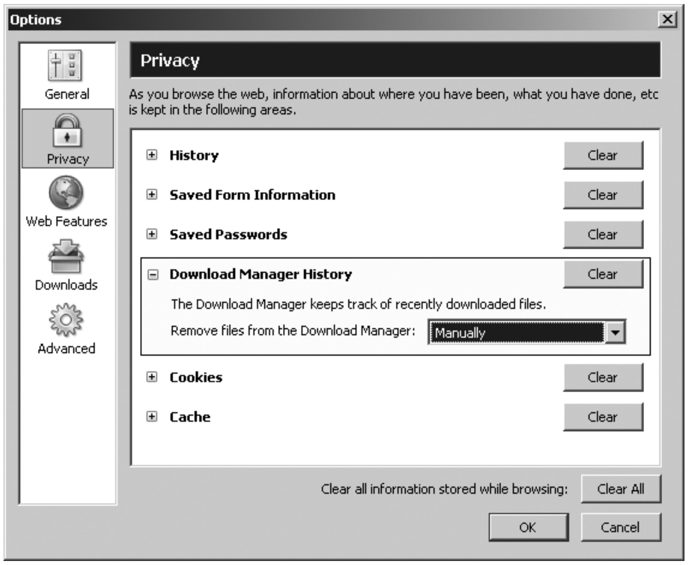
- On Windows, this is in C:\Documents and Settings\<useraccountname>\Application Data\Mozilla\Firefox\Profiles\default.<3-character ID>\key3.db
- On Linux, this is in ~/.mozilla/firefox/default.gdd/key3.db
- On a Mac, this is in users\<useraccountname>\Library\Application support\Firefox\Profiles\xxxxxxxx.default\key3.db

Now rename the `key3.db` file to `!key3.db.save` so that Firefox doesn't know where to read the old master password information. Restart Firefox and go to Tools | Options | Privacy | Saved Passwords | Set Master Password to display the Change Master Password screen. (On Linux and Mac computers, go to Edit | Preferences | Advanced... instead.) The current master password field on the Change Master Password screen will now be empty, and you'll be able to set a new master password as if you'd never set one at all.

This isn't particularly secure when you think about it—the master password can be reset and even set back to where it was without an audit trail—but it's enough to keep casual users from getting into your passwords.

Download Manager History

The Download Manager is discussed in detail in Chapter 8, "Other Interesting Features," but take a moment now to look at how to set the privacy option for it (shown in Figure 2-9). As part of its job, the Download Manager logs the files you download. You may not want everything you've downloaded to show up for the world to see, so you can set a few options for removing files from the Download Manager. You can use the dropdown list to set the Download Manager so that you can remove the download history manually one file at a time (the default), upon a successful download, or whenever you exit Firefox. To clear the Download Manager of everything all at once, click **Clear**, and poof! All traces of download history are removed.



As you browse the web, information about where you have been, what you have done, etc is kept in the following areas.

The Download Manager keeps track of recently downloaded files.

Remove files from the Download Manager: Manually

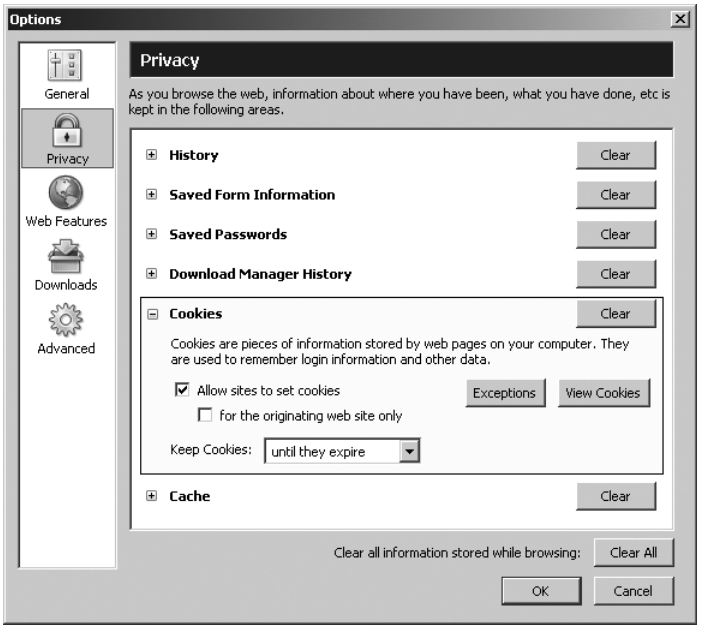
Clear all information stored while browsing:

Figure 2-9

The Options screen with the Download Manager History option expanded.

Cookies

Cookies are small information files saved on your computer by websites. Most cookies are pretty innocuous—they let Firefox remember your logon information or your website preferences—but some can be a potential security breach because they contain logon info or because they're actually cookies left by adware. The Cookies option (shown in Figure 2-10) lets you manage cookies in several different ways.



Privacy

As you browse the web, information about where you have been, what you have done, etc is kept in the following areas.

⊞ History

⊞ Saved Form Information

⊞ Saved Passwords

⊞ Download Manager History

⊟ Cookies

Cookies are pieces of information stored by web pages on your computer. They are used to remember login information and other data.

☑ Allow sites to set cookies

☐ for the originating web site only

Keep Cookies: until they expire

⊞ Cache

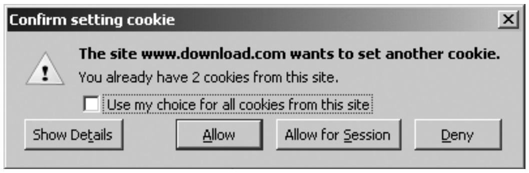
Clear all information stored while browsing:

Figure 2-10

The Options screen with the Cookies option expanded.

The default cookie option is to allow websites to set cookies. This is generally a good idea; cookies are just too useful to disable completely without some consideration. You can, however, restrict this so that only the originating websites can save cookies by checking that box. This means that you can log on to a site like www.squidlips.org and have cookies for your logon information for that website, but the website can't set cookies for any advertisers who also have links on the website.

The Keep Cookies dropdown list defaults to keeping cookies until they expire (many websites set their cookies to expire by a certain date or by some period after the last time they've been used), but you can make this a good deal more draconian if you wish. You can have cookies be session-temporary: as soon as you exit Firefox, the cookies are erased. You can be even more strict about the settings and specify that Firefox should ask you every time a website wants to set a cookie. When Firefox is set to manage cookies this way, every time a website wants to set a cookie, you see a dialog box like the one shown in Figure 2-11.



The site www.download.com wants to set another cookie.

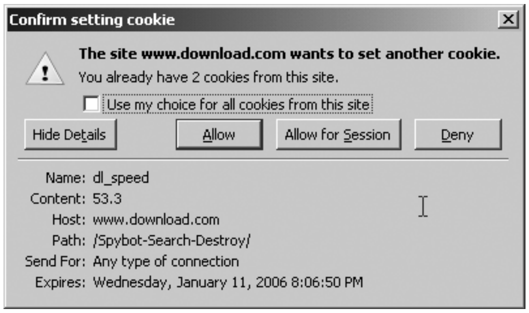
You already have 2 cookies from this site.

☐ Use my choice for all cookies from this site

Figure 2-11

The Confirm setting cookie dialog box.

The Confirm setting cookie dialog box tells you that the website wants to set (or sometimes just modify) a cookie. If you have several cookies from this website already, it shows how many cookies are already stored in Firefox for this website (two cookies in this example). You can click **Allow** to allow the website to set a cookie, **Allow for Session** to set a cookie that will be erased when you close Firefox, or **Deny** to prevent the website from setting a cookie at all. If you need more information, click **Show Details**. The information displayed is rather technical (as shown in Figure 2-12), but some people like knowing that sort of thing. One thing that's worth noting is the cookie's expiration date at the bottom of the screen.



The site www.download.com wants to set another cookie.
You already have 2 cookies from this site.

□ Use my choice for all cookies from this site

Name: dl_speed
Content: 53.3
Host: www.download.com
Path: /Spybot-Search-Destroy/
Send For: Any type of connection
Expires: Wednesday, January 11, 2006 8:06:50 PM

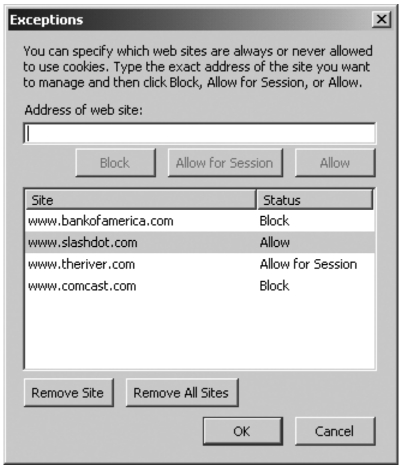
Figure 2-12
The Confirm setting cookie dialog box with the cookie information displayed.

If you're going to romp around a website for a while, it may well try to set several cookies. The second time the Confirm setting cookie dialog box appears, you may want to check the box so that Firefox automatically allows, allows for this session, or denies cookies for this website.

FRIDGE

Everyone should try setting their cookie options so that Firefox asks them if they want to save each and every cookie, and then surf the web with that option on for as long as they can stand it (probably about five minutes) before going to one of the other two cookie options. It's a valuable lesson in just how many cookies are being set and by whom.

In addition to the general cookie options, you can tell Firefox to always ignore or always permit specific websites. Click **Exceptions** to display the Exceptions screen (shown in Figure 2-13). Enter a website in the Address of website field, and then select the appropriate permission level—Block, Allow for Session, or Allow—to add the website to the list below. You can remove websites already in the list by highlighting the websites (hold down the Ctrl key and click to select multiple sites or hold down the Ctrl key and the



You can specify which web sites are always or never allowed to use cookies. Type the exact address of the site you want to manage and then click Block, Allow for Session, or Allow.

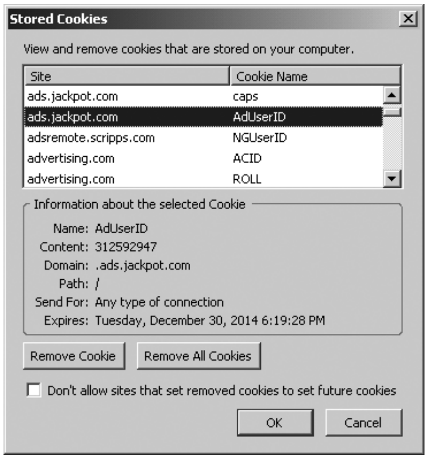
Address of web site:

Site	Status
www.bankofamerica.com	Block
www.slashdot.com	Allow
www.theriver.com	Allow for Session
www.comcast.com	Block

Figure 2-13
The Exceptions dialog box.

Shift key and click to select a range of websites) and then clicking **Remove Site**. You can wipe the slate clean by clicking **Remove All Sites**. When you are satisfied with your entries, click OK.

If you want to maintain really tight control over your cookies, it's a good idea to periodically review the cookies stored on your computer. Click **View Cookies** to display the Stored Cookies screen (shown in Figure 2-14). You can review the cookies and, if you wish, remove some or all of them. Like the Confirm setting cookie dialog box, the details of the highlighted cookie are displayed at the bottom of the screen. It's worth noting that, in this example, the cookie will expire in 2014, which may make the "keep cookies until they expire" setting a little silly. (I've even seen cookies that were set to expire in 2032. If you have any idea what kind of computer you'll be using in 2032, or which version of Firefox, please let me know.)


Stored Cookies

View and remove cookies that are stored on your computer.

Site	Cookie Name
ads.jackpot.com	caps
ads.jackpot.com	AdUserID
adsremote.scripps.com	NGUserID
advertising.com	ACID
advertising.com	ROLL

Information about the selected Cookie

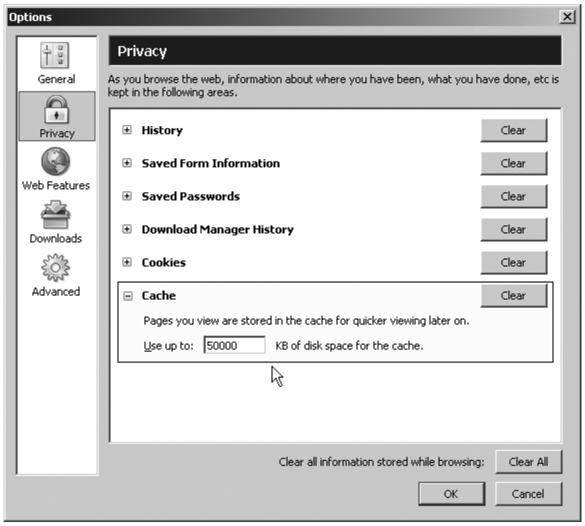
Name: AdUserID
Content: 312592947
Domain: .ads.jackpot.com
Path: /
Send For: Any type of connection
Expires: Tuesday, December 30, 2014 6:19:28 PM

□ Don't allow sites that set removed cookies to set future cookies

Figure 2-14
The Stored Cookies screen.

Cache

As with every other browser, Firefox stores a copy of the web pages—HTML, images, scripts, and so on—you've visited in a *cache* so that they can be displayed quickly the next time you go to the URL. Web pages are stored in the cache until you reach the preset limit (the default is 50 MB of disk space, as shown in Figure 2-15), after which Firefox starts deleting web pages on a first-in, first-out basis. Again, if you're security-conscious, you should clear your cache periodically by clicking **Clear** for this option.



Privacy

As you browse the web, information about where you have been, what you have done, etc is kept in the following areas.

Pages you view are stored in the cache for quicker viewing later on.

Use up to: 50000 KB of disk space for the cache.

Clear all information stored while browsing:

Figure 2-15
The Options screen with the Cache option expanded.

Getting Rid of Everything at Once

If you want to clear everything all at once—history, passwords, cache, and so on—click **Clear All** at the bottom of the screen and then confirm the deletion. Think of this option as a kind of security panic button. Pretty much everything you've been doing on the web will vanish in a puff of bits.

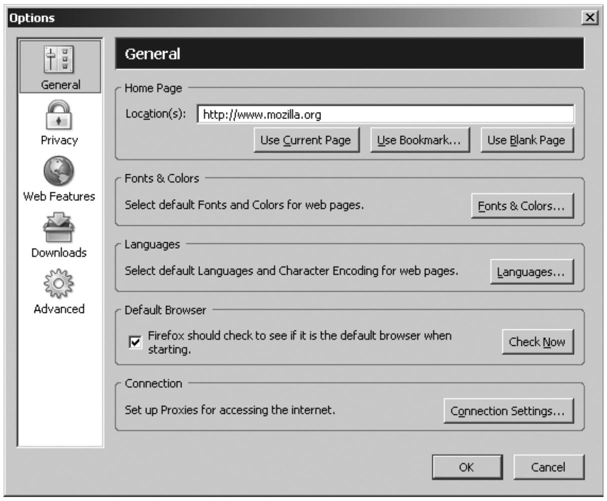
Limiting Web Access

For the record, I don't think much of parental controls. It's not that I disagree with the idea that kids should not be exposed to a lot of the seamier stuff on the web—they shouldn't, and parents should be the ones who set boundaries on what they consider acceptable. But parental controls aren't particularly effective if a child is really persistent.

Nevertheless, parental controls have some value that at least makes them worth considering. The first major parental control product to support Firefox was CyberPatrol (www.cyberpatrol.com). It's not bad; in fact, you can do a heckuva lot worse.

Another way to consider limiting web access is to set up a *whitelist*. A whitelist explicitly identifies the websites you can surf to. This probably won't be particularly helpful as a parental control, because there are probably lots of different sites that you'd like your kids to be able to go to, and coming up with even a partial list is likely to be impractical, but you can use the whitelist technique in any situation where you want to provide web access to a limited number of sites. For example, you may want to point a computer to an online catalog, a directory, or a single informational website.

To limit browser access, start by going to Tools | Options | General. The Options screen with the General options appears, as shown in Figure 2-16.



Location(s): http://www.mozilla.org

Select default Fonts and Colors for web pages.

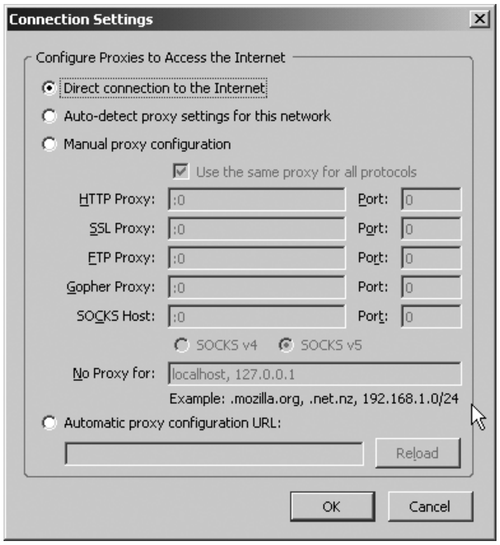
Select default Languages and Character Encoding for web pages.

☑ Firefox should check to see if it is the default browser when starting.

Set up Proxies for accessing the internet.

Figure 2-16

The Options screen with the General options displayed.



● Direct connection to the Internet
○ Auto-detect proxy settings for this network
○ Manual proxy configuration
☑ Use the same proxy for all protocols
HTTP Proxy: :0 Port: 0
SSL Proxy: :0 Port: 0
FTP Proxy: :0 Port: 0
Gopher Proxy: :0 Port: 0
SOCKS Host: :0 Port: 0
○ SOCKS v4 ● SOCKS v5
No Proxy for: localhost, 127.0.0.1
Example: .mozilla.org, .net.nz, 192.168.1.0/24
○ Automatic proxy configuration URL:

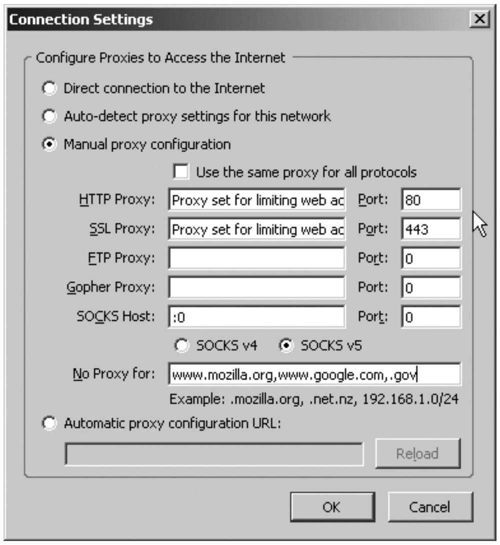
Figure 2-17
The Connection Settings screen.

Click **Connection Settings** to display the Connection Settings dialog box (shown in Figure 2-17).

Click the **Manual proxy configuration** radio button, which activates the fields in the middle of the Connection Settings screen. Uncheck the **Use the same proxy for all protocols** checkbox.

In HTTP Proxy, enter a message like "Proxy set for limiting web access." (This message is for your own reference.) Enter 80 in the corresponding Port field. Next, in SSL Proxy, enter the same message you entered in the HTTP Proxy field, and set the corresponding Port field to 443.

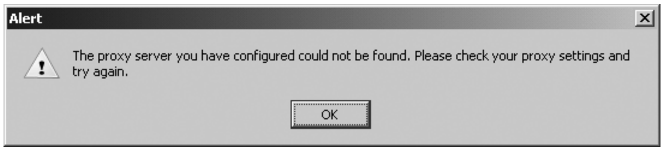
In **No Proxy for**, enter the names of the websites you want to allow access to. You can enter specific websites, such as www.mozilla.org and www.google.com, which will allow you to access anything within these domains. You can enter broader ranges of websites as well. For example, entering .gov lets you surf to any website ending in .gov. You can be even more specific as well: entering www.mozilla.org/support lets you go to any of the pages in the mozilla.org/support subdomain. Figure 2-18 shows an example of what the Connection Settings screen looks like with the whitelist information added.



○ Direct connection to the Internet
○ Auto-detect proxy settings for this network
● Manual proxy configuration
☐ Use the same proxy for all protocols
HTTP Proxy: Proxy set for limiting web ac Port: 80
SSL Proxy: Proxy set for limiting web ac Port: 443
FTP Proxy: Port: 0
Gopher Proxy: Port: 0
SOCKS Host: :0 Port: 0
○ SOCKS v4 ● SOCKS v5
No Proxy for: www.mozilla.org,www.google.com,.gov
Example: .mozilla.org, .net.nz, 192.168.1.0/24
○ Automatic proxy configuration URL:

Figure 2-18
The Connection Settings screen with proxy information entered.

When you are satisfied with your entries, click OK. At this point, you can only go to the specified websites. If you try to access any other website, you'll see the message shown in Figure 2-19.



The proxy server you have configured could not be found. Please check your proxy settings and try again.

Figure 2-19

Alert for a website blocked by the whitelist.

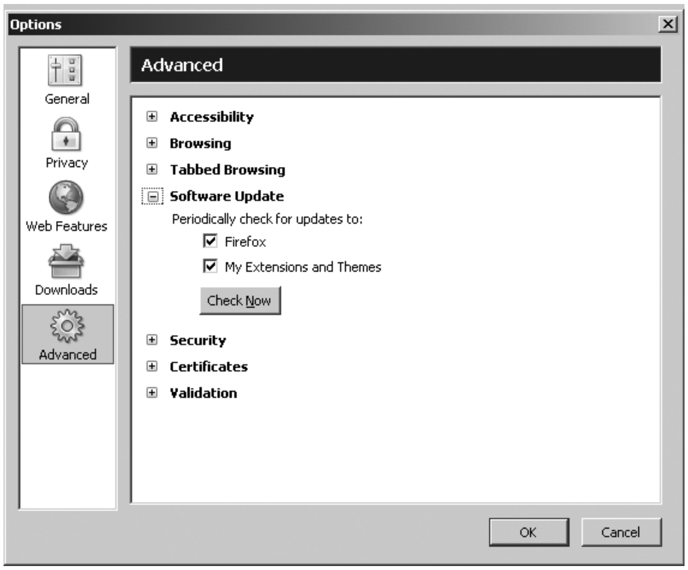
You can always go back to the Connection Settings screen and check the **Direct connection to the Internet** radio button to remove the access limitations.

FRIDGE

There's another way you can use whitelists. Suppose you want to set up a dedicated terminal at a conference or a public information kiosk. You can use a whitelist together with a list of bookmarks on the Bookmarks toolbar (a technique you'll see in Chapter 5) to point the users to a specific and very limited group of websites on the Internet.

Setting Other Security Options

In addition to what you've seen so far, you can set a few additional security options. Start by going to Tools | Options | Advanced. The Advanced options are displayed, as shown in Figure 2-20.



Periodically check for updates to:

☑ Firefox

☑ My Extensions and Themes

Figure 2-20

The Options screen with the Software Update option displayed.

The Advanced options cover a lot of ground, not all of it security-related. As with the other options screens, you can expand an option by clicking the button next to the option. For now, you only need to worry about software updates and security.

Software Update

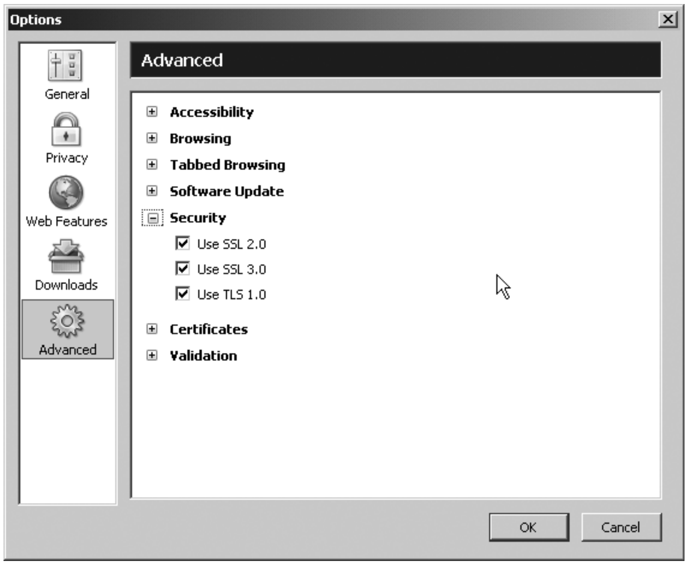
The software update option lets you tell Firefox to check for updates to the Firefox software itself for any extension or theme you may have installed. (Extensions and themes are discussed in Chapter 7, "Customizing Firefox with Third-Party Extensions and Themes.") When these two boxes are checked (the default), Firefox checks periodically for updates to the software. When there's an update, a small icon appears in the top right of the Firefox screen near the Google search bar. If the icon is red, a critical update of Firefox is available for download. A green icon indicates that there are up to four updates to extensions and themes; a blue icon indicates that there are more updates than that. Click the icon and follow the instructions to update the assorted software. If you don't want to wait, you can click **Check Now** to force Firefox to check for updates. If there's an update, Firefox displays a small screen telling you what's been updated and asks if you want to install the update.

No matter what your settings or the updates, Firefox always requires you to approve the installation of *any* software on your computer.

Security

The Security option (shown in Figure 2-21) specifies how information is transmitted between your computer and a website. *Secure Socket Layer*, or *SSL* for short, is a standardized protocol for sending and receiving information over the Internet in an encrypted form. There are several levels of SSL security. The most common is SSL 2.0, but there is a more secure version, SSL 3.0. Transport Layer Security, or TLS, is an open security protocol that is similar to SSL 3.0. Both SSL and TLS are used to encrypt your data using an encryption method agreed upon by your browser and the website you're communicating with. This ensures that the data can be read only by your browser and the website, and no one else.

You can select SSL 2.0, SSL 3.0, and TLS 1.0 (the two SSL options are already selected by default) for the Security option. SSL and TLS are most commonly used by shopping websites for transmitting and receiving confidential information, such as credit card numbers. Every secure website these days supports SSL 2.0, which provides server authentication. SSL 3.0 and TLS 1.0 are better—they provide server and client authentication—but they're not universal. If you select all three options, Firefox will use the best security communications option available, depending on the capabilities of the website you're talking to at the moment.



☑ Use SSL 2.0

☑ Use SSL 3.0

☑ Use TLS 1.0

Figure 2-21

The Options screen with the Security option displayed.

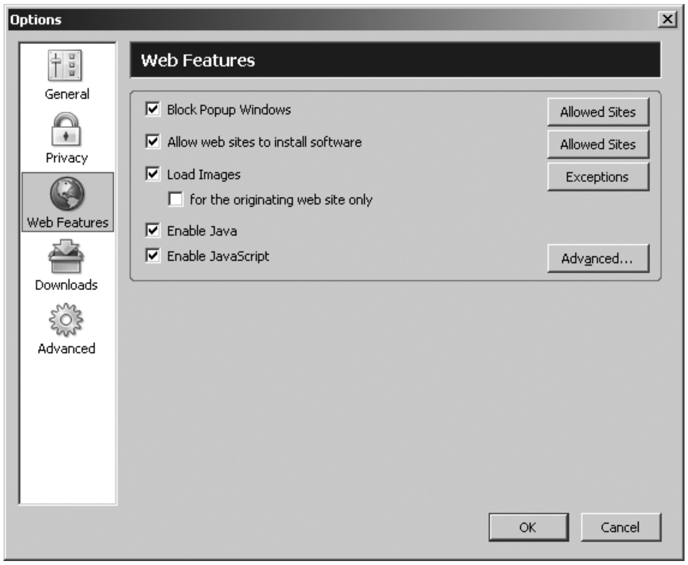
Getting Really Secure

For the hyperconscious, Firefox offers a number of settings for working with digital certificates and validation. Almost everyone who uses Firefox will be completely happy—and secure—with the default settings, but if you want to be impeccable, check out the technical information on using digital certificates in Firefox in Appendix F, "Security, Certificates, and Validation."

Setting Web Features Options

The final set of security options appears on the Web Features Options screen, shown in Figure 2-22. To display the Web Features options, go to Tools | Options | Web Features.

The options described in the following sections can give you more control over your web security.



Web Features

☑ Block Popup Windows

☑ Allow web sites to install software

☑ Load Images

□ for the originating web site only

☑ Enable Java

☑ Enable JavaScript

Figure 2-22

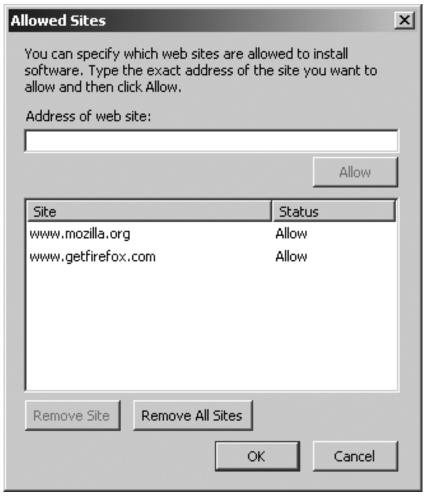
The Options screen showing the Web Features options.

Block Popup Windows

This option, which blocks popups, is described in Chapter 3.

Allow Websites to Install Software

When you install Firefox, websites can install extensions and themes on your computer. Adding extensions and themes is a pretty good thing, because you can augment Firefox's capabilities and change the way it looks. (Extensions and themes are discussed in Chapter 7.) However, the installation process isn't completely uncontrolled. Firefox blocks any website from installing software until you've added the website to a whitelist of allowed sites. A small bar appears at the top of the screen telling you that Firefox has blocked the website from installing software on your computer. You can click **Edit Options** to display the Allowed Sites screen, shown in Figure 2-23, to add the website.



You can specify which web sites are allowed to install software. Type the exact address of the site you want to allow and then click Allow.

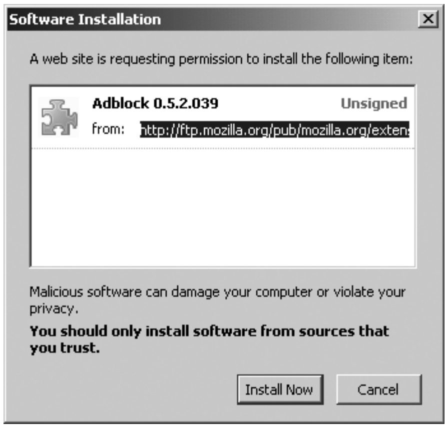
Address of web site:

Site	Status
www.mozilla.org	Allow
www.getfirefox.com	Allow

Figure 2-23

The Allowed Sites screen.

When a website has been added to the list, click the link again to install the software. Firefox displays a small confirmation screen to ask if you want to download this specific piece of software (an example appears in Figure 2-24).


Software Installation

A web site is requesting permission to install the following item:

Adblock 0.5.2.039 Unsigned

from: http://ftp.mozilla.org/pub/mozilla.org/exten

Malicious software can damage your computer or violate your privacy.

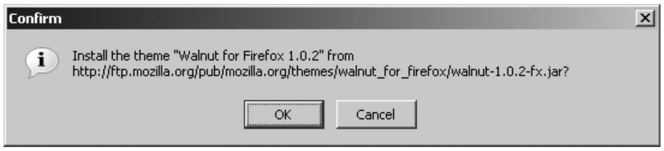
You should only install software from sources that you trust.

Figure 2-24

The Software Installation screen.

The Allowed Sites screen lets you edit the list of websites that are allowed to install extensions and themes on your computer. To manually add a website to the list, click **Allowed Sites** on the Web Features Options screen, enter the website address in the Allowed Sites screen's address field, and click **Allow**. (Any websites that you've previously allowed already appear on the list.) You can remove previously allowed websites from the list by highlighting the site(s) in question and clicking **Remove Site**, or click **Remove All** to block every website from installing software on your computer. When you are satisfied with your entries, click OK.

Themes are handled a little differently: when you try to install a theme and you have this option checked, Firefox does not require you to add the website name to the whitelist. You're just asked to confirm the download in a simple message like the one shown in Figure 2-25.


Confirm

Install the theme "Walnut for Firefox 1.0.2" from http://ftp.mozilla.org/pub/mozilla.org/themes/walnut_for_firefox/walnut-1.0.2-fx.jar?

Figure 2-25

Confirming a theme download.

By default, downloads are allowed, but unchecking **Allow websites to install software** prevents any downloads from occurring unless you first re-enable this option.

Load Images

The Load Images option lets you selectively display or block banner ads and other images and is described in Chapter 3.

Enable Java

Java is a programming language developed for web programming by James Gosling of Sun Micrososystems. Java is very portable: the same Java program can run on a wide variety of computers, making it unnecessary to create multiple versions for differing platforms. Java programs that are downloaded and run in web browsers are typically known as *applets*. Lots of websites use Java applets to add custom features, such as dropdown menus, web buttons, image scrolling, and other features, such as animation and slide shows. Many online, web-based games are written in Java. There are lots of complex and more esoteric Java applets as well; for example, many online accounting systems and other web-based systems make extensive use of Java for reporting and printing information.

Note

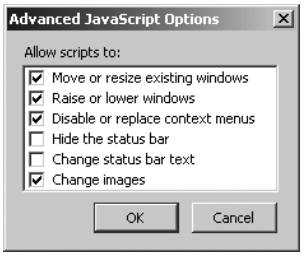
If you want to run Java applets of any kind, you must also install the Java plug-in in Firefox. For information on installing plug-ins, see Chapter 8.

By default, Firefox allows Java applets to run, but you can prevent this by unchecking Enable Java.

Enable JavaScript

JavaScript is a simple, effective scripting language created by Brendan Eich while he was at Netscape. It isn't the same as Java. JavaScript and Java have some things in common (that would only be of interest to a programmer—trust me), but the biggest difference is that JavaScript is used for small things like checking and formatting input on web forms. JavaScript code is integrated in the web page's HTML code, so a lot of functions can be done directly on your computer within the browser without having to go back to the server for computing power. (In contrast, Java applets are compiled programs that are separate from web pages, although they can be called from a web page and downloaded to your computer.)

There probably isn't any good reason to stop JavaScript from running on your browser: it's clean, it's pretty secure as things go, and a lot of websites depend on JavaScript. On the off chance you know why you want to disable JavaScript on your computer, uncheck Enable JavaScript. However, you may want to disable only certain features of JavaScript, which you can do by clicking **Advanced** to display the Advanced JavaScript Options screen (shown in Figure 2-26).



Advanced JavaScript Options

Allow scripts to:

☑ Move or resize existing windows
☑ Raise or lower windows
☑ Disable or replace context menus
☐ Hide the status bar
☐ Change status bar text
☑ Change images

Figure 2-26

The Advanced JavaScript Options screen.

Through this screen, you can enable and disable any of the following:

- Move or resize existing windows: Enables or disables moving and resizing windows with scripts.
- Raise or lower windows: Enables or disables raising and lowering windows with scripts.

- Disable or replace context menus: Enables or disables web pages from changing or disabling the Firefox context menu.
- Hide the status bar: Enables or disables forcing the display of the status bar in popup windows.
- Change status bar text: Enables or disables status bar text scrolling and hiding web addresses when you hold the mouse over them.
- Change images: Enables or disables changing images. These are often called *rollover* or *mouseover* images; they change when you move the mouse over them. Use this carefully, because disabling this feature can make it difficult to navigate some menus.

Even with all these security and privacy options, Firefox isn't absolutely, totally secure. No web application is 100% risk-free. Nevertheless, Firefox is pretty darned good: it excludes the riskiest technologies found in other browsers, and, while it's not impossible for someone to come up with a way to attack Firefox's security, the amount of effort to do so is much greater because of Firefox's better architecture.

I know what computers are supposed to be: they're supposed to be like the computer on *Star Trek*. I should be able to talk to it in plain English and have it sift through my idioms and syntax and implied questions and still come up with exactly what I really want to know. That computer operates like an appliance: efficiently, accurately, with only very rare hiccups in its otherwise seamless performance. Unfortunately, that's not the computer I have on my desk. (I don't think they're going to sell the *Star Trek* make and model for quite a while, darn it!) As a result, I have to know a lot more about how it works, how it connects to the Internet, and what I need to do to protect it from bad people doing bad things. All of this is work that doesn't add anything to the task at hand. It's all overhead. Ugh.

With that in mind, I'm glad that using Firefox means that I don't have to worry about half as many security problems as I used to. As you've seen, it's relatively simple to set up a number of basic security and privacy options that you usually don't have to worry about again. The next chapter gives you the other part of this picture by telling you how to deal with two of the biggest annoyances on the web these days: popups and banners. These aren't security risks of the same caliber as spyware, but they're just as pestiferous. You'll be glad to know that Firefox offers several direct ways of dealing with these problems, too.