Other Vulnerabilities (Spam, Cookies, Pop-Ups, Spyware, and Scams)

In addition to viruses and worms, there are some other annoying programs and files out there that you need to protect your home network from. This chapter focuses on spam, cookies, spyware, and scams—what they are, how they work, and how to get rid of or at least control them. For the most part, these types of files are not as dangerous as the others we discussed in Chapter 15, "Viruses and Other Malicious Software"—none of them will remove or destroy data for example—but they are still common, extremely annoying, and in some cases, they can do things without you knowing about it.

Spam

Spam is the common name for unsolicited commercial e-mail and it is a problem that is rampant on the Internet today. Because of spam, a whole sub-industry of spam blockers has cropped up and is a major concern of Internet service providers (ISPs). Major service providers claim that they block on the order of 2 billion (yes, billion) unsolicited e-mails every day and have put the effort to stop spam at the top of their priority lists. One of the reasons that spam is so widespread is that it is extremely easy to send out millions and millions of e-mails with little cost.

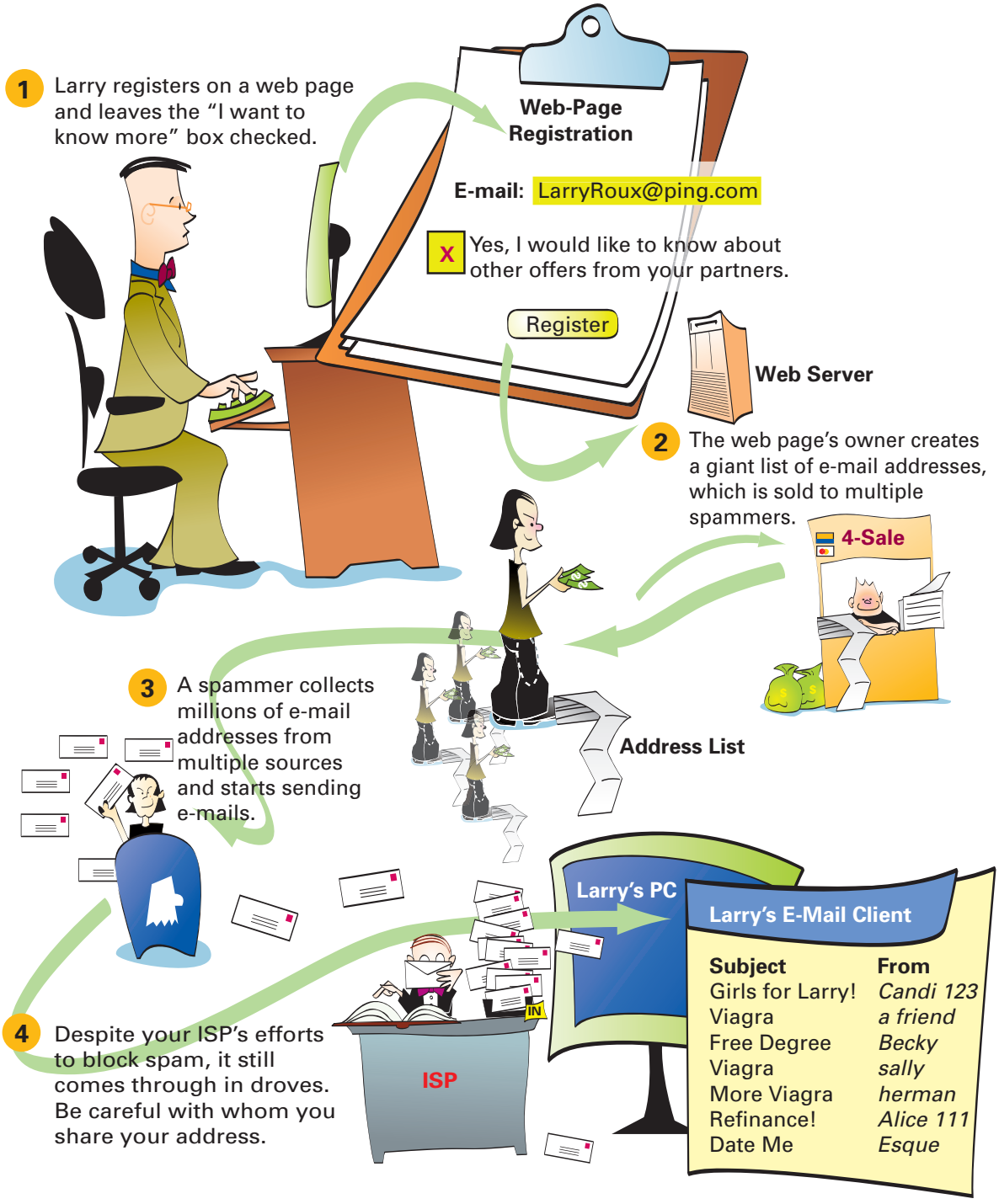
How Spam Works

Spammers do their dirty work by purchasing or creating giant e-mail lists and automated mailing tools called *spambots*. The lists are usually compiled from web pages where people provide their e-mail address as part of a registration process. Usually, there is a box that is checked "yes" by default saying something along the lines of "Yes, please share my e-mail with your sponsors for related offers." If you agree, by leaving the box checked, you have just given the site permission to sell and resell your e-mail address to spammers. Although most spam gets caught by filters or deleted by the recipient, some of it is answered and that is why the spammers keep at it. It is really a matter of odds. Even if the response rate is 0.5%, it cost next to nothing to send spam to upward of 10 million e-mail addresses. At that rate, the spammer just pulled in 50,000 new customers.

GEEK SQUAD Spammers also collect e-mails from web page "guest books" and message boards. Be careful where you leave your e-mail address. If you are lonely, this is a great way to make sure you always have new mail in your inbox.

Spam

Spam is unsolicited commercial e-mail, and it is a huge problem. Some large ISPs claim that they block over one billion e-mails a day and some still gets through. Here is one example of how spammers get their info.



Visit ciscopress.com to buy this book and save 10% on your purchase.

Register to become a site member and save up to 30% on all purchases everyday.

How to Block Spam

There is a good chance that your ISP has some sort of spam-blocking feature available and, if spam is a problem for you, we suggest starting there. Your ISP probably uses some basic filters such as looking for keywords or multiple (100,000+) instances of an e-mail from the same source IP address. Unfortunately, spammers (those who create and send spam) are pretty good at staying ahead of the ISPs by using random or misspelled words or by constantly changing IP addresses as they send e-mails. (There is also talk of anti-spam legislation, but spammers can easily set up shop in countries with looser laws.) If the ISP filters are not blocking enough spam, you can purchase or download software that will provide a second layer of protection on your system. Typically, these programs use advanced algorithms to recognize and block spam but they are not perfect because sometimes spam gets through the filter, and sometimes legitimate e-mail gets blocked (essentially a false positive). You can modify the options in this program so that the blocking rules are customized. Be sure to check the folder that the spam blocker drops trash e-mail into every once in a while to make sure you don't miss "real" e-mail.

We recommend that in addition to using the ISP and commercial blockers that you set up a *dirty* e-mail address. What we mean by dirty e-mail address is an e-mail address that is only used for the purpose of registering on web pages. Given that most ISPs will allow several e-mail aliases with a standard account, you can reserve one for this purpose and still have plenty for the legitimate users in the home.

After you do this, only give your "real" e-mail out to people you know and use the dirty one for everything else. If you find that you do want some of the e-mail that comes into the dirty account, you can notify the sender to use your real e-mail address. Keep in mind that most legitimate commercial sites will not resell or share your e-mail address without your permission, but it's up to you to make sure that you read the fine print and uncheck any boxes that were pre-populated. This is always a red flag.

GEEK SQUAD Just in case you are wondering, replying to a spam e-mail does not stop it from coming. In fact, such replies are used by the spammers to confirm "live" e-mail addresses, which then get put on a verified list. After this happens, you might as well retire the e-mail address.

Cookies

Cookies are small text files that web pages place on your computer when you visit a web page. The text file contains information that helps web pages track users and allows site preferences so that when you re-enter a page, it's unique to your custom settings or has "one-click" purchase options.

How Cookies Work

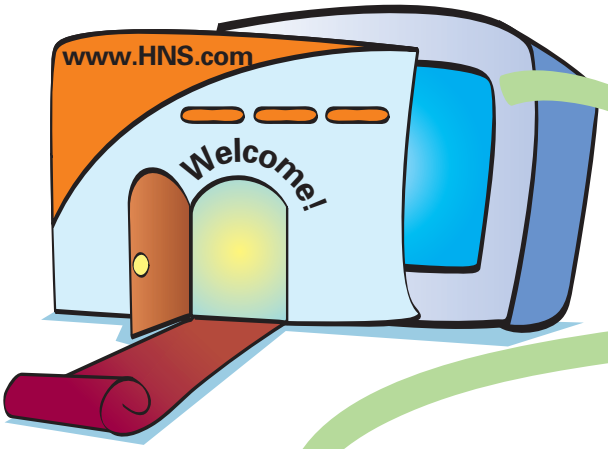
When you visit a website that tracks user data in this way, the site "drops a cookie" and creates a text file on your machine if it is your first visit, or updates a file that it left on your machine from a previous visit. The website does not change anything on your computer other than the file and, in all but the rarest of cases, the cookie does not contain any private information such as credit card numbers or home addresses and phone number. Most often, the cookie contains only the name of the web page and a unique identifier that the web page uses to pull information from a secure database where the private information about you is kept. This helps prevent problems associated with different people sharing the same machine, or a single user who switches between machines. It also allows web pages to keep track of users even when they have deleted all their cookie files.

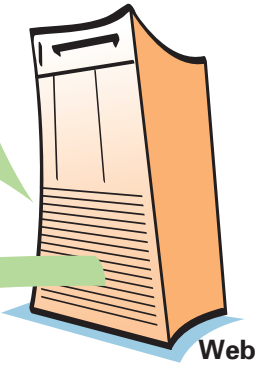
Cookies

Cookies are text files that websites place on your computer to help them keep track of visitors and customized settings. Most of the time, cookies are harmless, but you should set your privacy settings to at least "Medium High" to avoid cookies from sites that share your information with others.

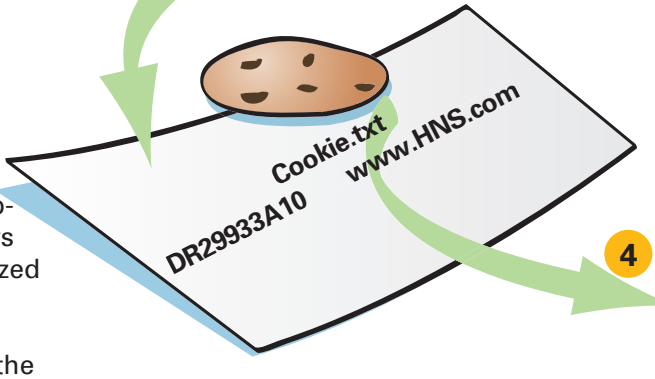
1 The first time you visit a website, it has no record of you.

2 To keep an accurate count of how many unique visitors come to the site, the web page places a "cookie" on your computer's hard drive.



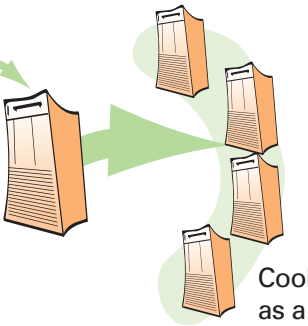


Web Server



3 If the web-site allows personalized views or purchase settings, the cookie helps the site load your settings so you do not have enter it every time you visit.

4 Your personal information is not sent within the cookie's file, only a number that points to a table in a secure database on the site.



Cookies can be used as a form of spyware when they are shared and aggregated among different sites.

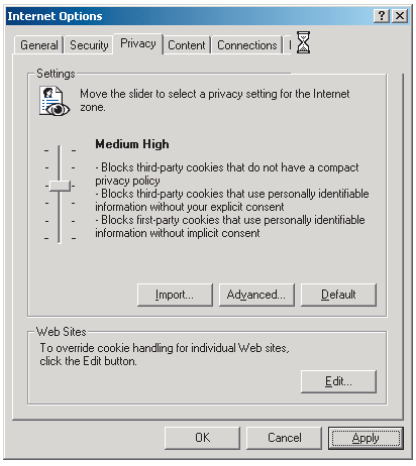
Bad Cookies

Not all cookies are bad things. For example, http://www.weather.com may place a cookie on your computer to store your ZIP code so that each time you return to its website, it can immediately bring up the local weather for your location.

However, one of the main issues with cookies is that marketing companies often use information about what you buy and where you click on a web page to better target you for advertising and spam. Some cookies are tracked across multiple sites by third-party companies. This is considered a privacy or security violation by many users. To protect your personal information, you can set your Internet browser to one of various privacy settings ranging from accept all cookies to block all cookies. Both these options are a bit impractical because accepting all will greatly increase security risks and blocking all will make it very difficult to browse many private and commercial websites (the pages will fail to load).

On Internet Explorer, we recommend a setting of Medium High as Figure 16-1 shows. (The screen is found by selecting the Privacy tab on the Internet Options dialog box, which is found under the Tools drop-down menu on the top of the browser.)

Figure 16-1 Setting Your Privacy to Medium High in Internet Explorer



If you are worried about the cookies you have previously accepted, you can delete all cookies by selecting the Delete Cookies button on the General screen of the window shown in Figure 16-1. If you had your privacy setting set to anything below Medium High, you should probably do this when you reset your settings.

Pop-Ups

Pop-ups refer to windows that are displayed on your computer screen for the purposes of advertising. Pop-ups occur when you browse certain websites. Some websites are funded by selling advertising space, some of which decide to hawk their wares by flooding your computer screen with clever ads.

How Pop-Ups Work

Pop-ups work using the same mechanism built in to web browsers, such as Internet Explorer, to open a URL in a new window. Sometimes this can be a useful function; for example, http://www.weather.com may use a pop-up window to display an urgent weather bulletin. But, in general, they are an annoying waste of your time.

GEEK SQUAD Our favorite pop-ups are the ones that insist your computer is vulnerable to pop-up ads and try and sell you pop-up blocking software.

How to Get Rid of Pop-Ups

Just like spam and other scams, pop-ups get a response rate or else companies would not use them any longer. So, first and foremost, stop clicking on them. Your PC will not run faster, you will not win free money by clicking on the monkey, and a pop-up IQ test is pretty ironic actually.

Second, get a pop-up blocker. Microsoft Internet Explorer 6 Service Pack 1 (SP1) running under Windows XP SP2 now has a built-in pop-up blocker. Turn it on by clicking **Tools > Pop-Up Blocker** in Internet Explorer.

If you are not running this version of Windows or Internet Explorer, download any number of free pop-up blockers and use it.

Spyware/Adware

Spyware or *adware* refers to programs that are installed on your machine for the express purpose of tracking your online movements. Spyware is typically installed without your knowledge. It can become a real problem by slowing down your machine's performance and slowing down your online activity because the network connection is being shared by the programs that are sending information back to the third-party vendors who paid to place the programs on your machine.

How Spyware or Adware Works

Spyware or adware is installed on your machine in a number of different ways:

- The most common by far is through the installation of programs that hide the spyware file within the main program.
- Through peer-to-peer sharing programs (such as Morpheus), certain websites install spyware programs.
- Some forms of cookies are considered spyware as well.

One company called Double-Click created a version of spyware by connecting cookies from tens of thousands of websites. This information is used to "spy" on you while you surf the Internet. Although this ploy was bad, it still only spied on your Internet browsing. Other more aggressive forms of spyware can and do collect personal information on you by scanning files, e-mails, and e-mail address books.

How to Get Rid of Spyware and Adware

Although some ISPs provide spyware blockers, we strongly recommend the purchase of a commercial spyware sweeper. If you have been using the Internet for any amount of time and have not run a spyware blocker on your machine, you will likely be shocked by the number of spyware files found on your machine when you first install the sweeper.

We found one site that has a nice comparison of various spyware sweepers called Adawarereport.com. You may also want to do some research by going to http://www.google.com and doing a search on spyware blockers.

Ultimately, your willingness to put up with spyware is a matter of your personal tolerance, but keep in mind that after the information leaves your machine, there is no telling where it goes or who sees it. You really should err on the side of caution.

GEEK SQUAD Almost everything we get called for on viruses and spyware is very preventable. Run a spyware blocker and, for goodness sake, don't ever click YES on pop-ups that say you have won free money.

Additional Scams

The Internet provides the perfect playground for scam artists, and by using the same principle as spammers, they figure that if they try a scam on enough people, sooner or later, someone will take the bait.

Phishing

In some cases, spam is actually used for the scam. One of the newest scams to make the news is *phishing*. In this scam, the target is sent a *very* official-looking e-mail from what they think is their bank or credit card company. A short note describes the "bank's" concern about identity theft and asks you to click a link so that they can confirm your account number. The link takes you to a very convincing website, complete with company's logo and trademarks and, in some cases, a 1-800 number. The site is bogus, however, and is operated by the actual identity thieves. The 1-800 number goes to them as well so if you call, everything seems legitimate. Figure 16-2 shows an example of a phishing e-mail (assuming that Pangea National Bank is an actual bank). Take a look at how official this looks and reads. However, clicking on the web link provided sends you to a website in China.

Figure 16-2 Sample Phishing E-Mail

Pangea ™ National Bank

Dear Pangea National Bank customer,
Recently there have been a large number of identity theft attempts targeting Pangea National Bank customers. In order to safeguard your account, we require that you confirm you banking details.

This process is mandatory, and if not completed within the nearest time, you account may be subject to temporary suspension

To securely confirm your Pangea National Bank account details, please go to:

https://web.da-us.pangeanationalbank.com/signin/scripts/login/user_setup.jsp

Thank you for your prompt attention to this matter and thank you for using Pangea National Bank!

Pangea National Bank
Identity Theft Solutions

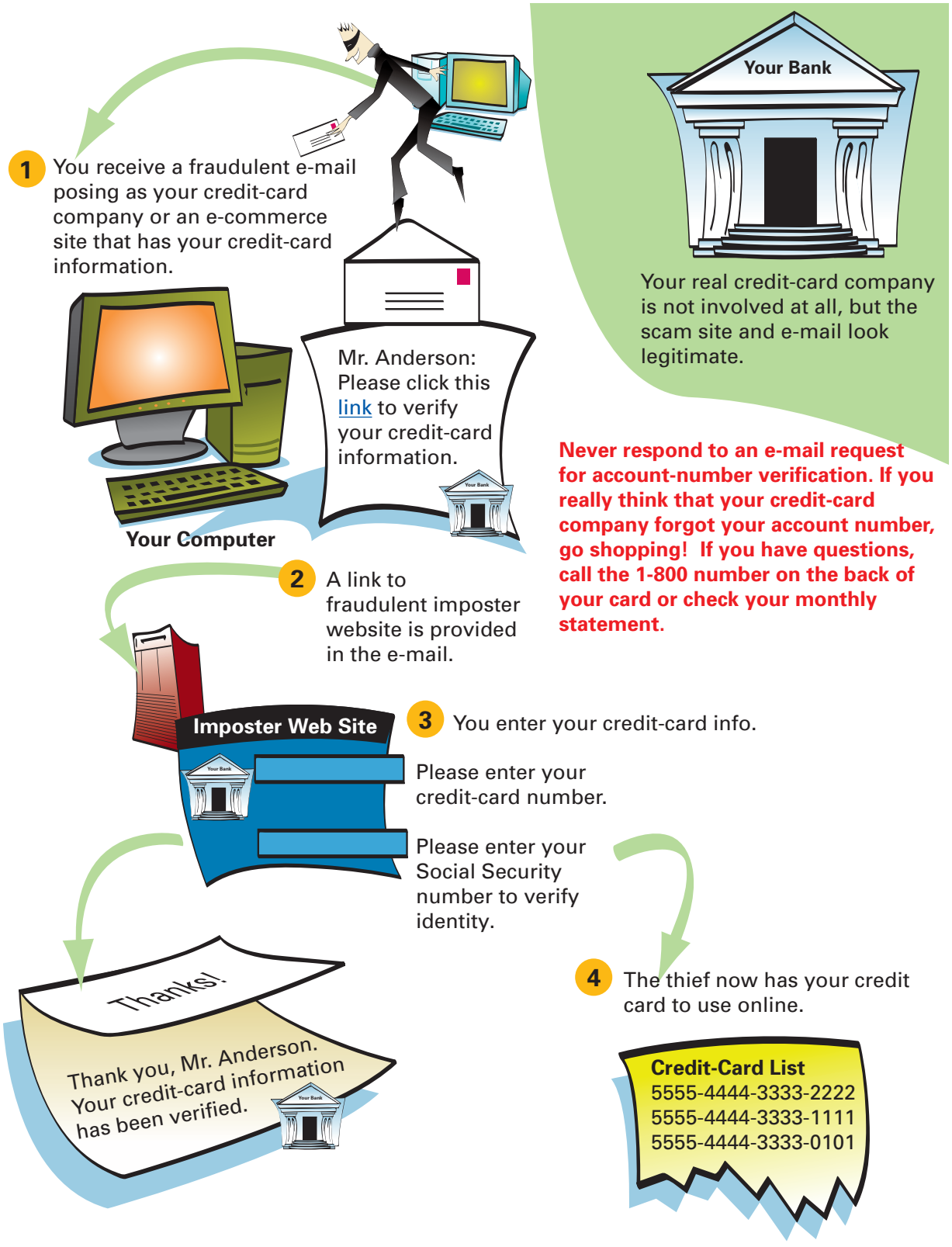
Do not reply to this e-mail as it is an unmonitored alias

Rest assured that any bank or credit card company that you deal with knows what your account number is. It is their business to know it, especially if you hold a balance on your credit card. If you get an e-mail like the one just described, you should immediately do these things:

- Report the scam to the Federal Trade Commission—Forward the e-mail you received to spam@uce.gov and identify that you believe it to be a phishing scam.
- Call your credit card company to notify them of the scam—Use the phone number on the back of your credit card or the one printed on your monthly bill, not the one in the text of the e-mail or on the scam page.
- Notify your ISP—You can reach most ISPs by sending an e-mail to the abuse reporting address for your domain. For example, if you subscribe to EarthLink, the e-mail would be abuse@earthlink.net. There will usually be a fraud alert link on the provider's main page as well.

As always, think before you act when it comes to giving out your personal information or responding to official looking e-mails. Phishing scams do not necessarily have to have money involved, it could just as easily be your e-mail account itself. To spammers and hackers, even an e-mail account is of value. Educate your friends, family, and strangers on the street about what you have just learned.

Phishing Scam Example



Urban Legends

The urban legend e-mail is also a popular Internet scam. An *urban legend* is one of those amazing or scary stories—you know, like the one about the couple that went to lover's lane and then found the bloody hook of the one-armed mass murderer on the passenger-side door.

If you get an e-mail about an incredible story, amazing opportunity, or terrible injustice that compels you to copy everyone in your address book: *Don't do it*! To our knowledge, terrorists are not buying UPS uniforms, Bill Gates is not giving away stock or money, there is no top-secret Neiman Marcus cookie recipe, and no one—not one person—has ever been slipped a mickey in his drink and then woke up in a hotel bathtub filled with ice, missing one of his kidneys.

GEEK SQUAD Our favorite variant was when the story was changed to say the person woke up missing a liver. Still someone forwarded it on.

Although some of these stories are amusing, they are nearly always false. To avoid annoying your friends, family, and colleagues, and to save yourself some embarrassment, check out the facts first. There are a number of sites that debunk these claims. http://www.scambusters.org covers urban legends, e-mail scams, and a lot more. http://www.scopes.com is also a winner. Take a quick look there before you forward that "Warning to All" e-mail.

How to Build It: Preventing Network Vulnerabilities

It would take an entire book to cover this area properly, so do not take the steps outlined in this section as the all-encompassing solution to online privacy. However, we do cover a few of the major issues, namely spam, phishing, spyware (including adware), and pop-ups.

We cover a few of these topics because the problems are very common, and because most people don't seem to have good information on where to start.

Here is an overview of the steps you follow to decrease your network's vulnerabilities:

- Turn on spam blocking at your service provider
- Set up spam blocking on your home computers
- Avoid phishing scams
- Set up spyware and adware blocking on your home computers
- Set up pop-up blocking on your home computers

Turn on Spam Blocking at Your Service Provider

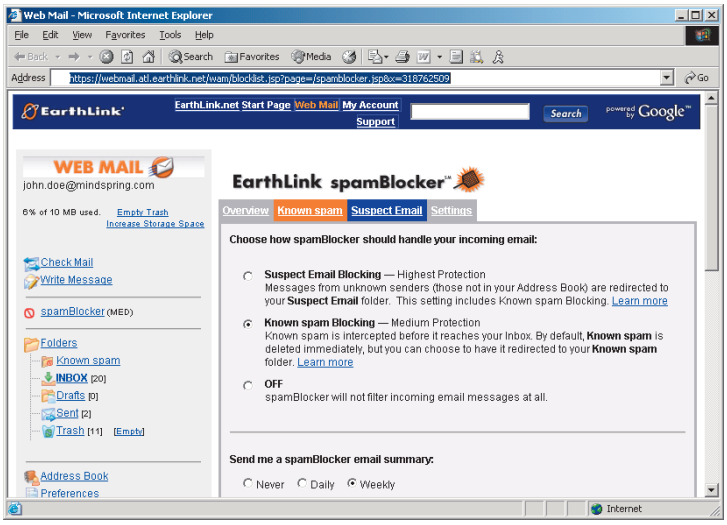
How to enable spam blocking with your service provider will vary highly and depend entirely on how the ISP has chosen to set up its services.

Enabling the protection is very easy. Just follow these steps (in this example, EarthLink is the ISP):

Step 1 Log in to the EarthLink My Account page using your account user ID and password.

Step 2 Click **Spam Blocker**. Choose the blocking setting that is appropriate (see Figure 16-3).

Figure 16-3 Enable Spam Blocking at Your ISP



There are three possible setting levels that we will take a moment to explain as they will also apply to spam blocking on home computers (which we will set up next). The three settings and how they operate are

- **Off**—All e-mail is forwarded; no spam checking is performed.
- **Medium**—E-mail is checked against known spammer lists, and matches are discarded.
- **High**—In addition to checks against known spammer lists, you create a list of e-mail senders that are in your address book. Matches against the known spammer list are discarded. Matches from your address book are forwarded to your inbox. If the sender is unknown (in neither list), the e-mail is held as "suspected" spam. You then have to go in periodically and sort out acceptable e-mail from spam.

If you receive e-mail from only a few known e-mail addresses (friends and relatives), put them in the address book and turn the spam blocker on High. If you receive considerable e-mail from new sources, you probably need to go with the Medium setting.

If your kids have e-mail accounts, we would *highly* recommend the High setting (no pun intended). Kids should never receive e-mail from sources that you don't go in and specifically authorize.

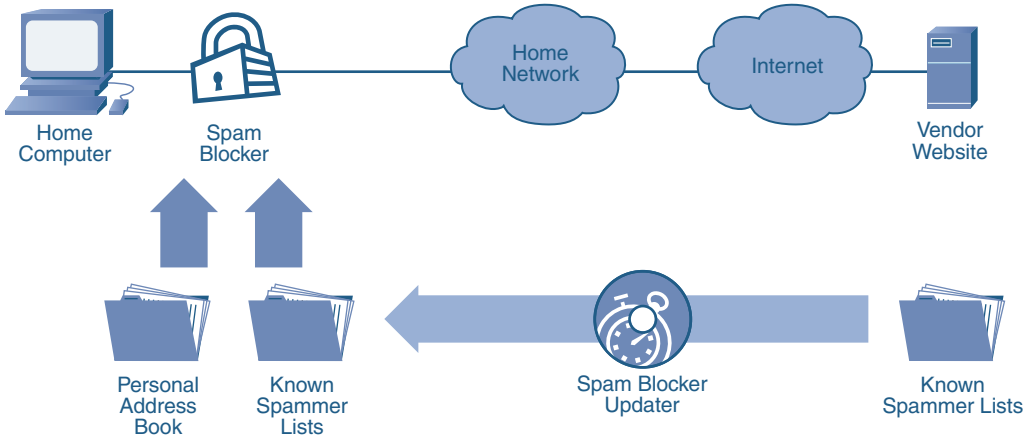
Set Up Spam Blocking on Your Home Computers

If possible, set up a first line of spam defense in the service provider network. This may be enough, so we recommend trying the ISP route first, and then see if you need additional protection.

If you need to enable blocking on each of the computers in your home network, as mentioned earlier, most security bundles contain a spam blocking component. This section shows the steps to enable this service.

First, it's helpful to understand a bit about how a spam blocker works. Spam-blocker vendors maintain lists of known spammers, which can be automatically updated on your home computers by the security bundle software. Figure 16-4 shows the components of a typical spam blocker.

Figure 16-4 Spam Blocker Components



The spam blocker works much like the description in the previous section on service provider spam blockers. There is typically a setting (like Medium) that discards e-mail matching known spammer lists, and a higher setting (like High) that additionally compares against a personal address book that you provide and maintain.

It is assumed that you already installed the security product bundle you have selected. Table 16-1 shows the process for enabling spam blocking on both the Symantec and McAfee products.

With the spam blocker enabled, you should see considerably less spam e-mail. We suggest starting off with a Medium setting, and moving up to a higher setting if you are not satisfied with the reduction in spam.

Table 16-1 Enabling Spam Blocking

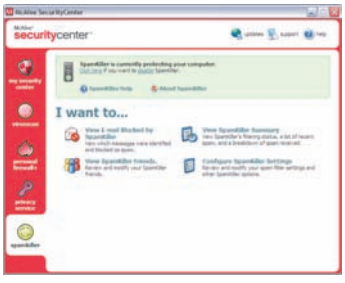
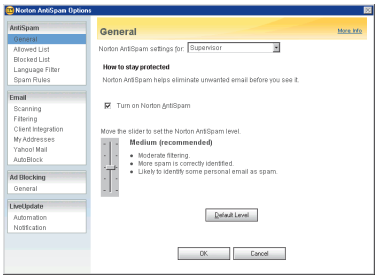
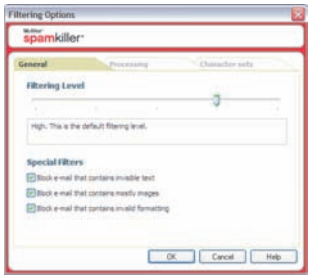
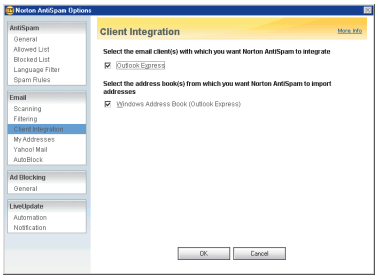
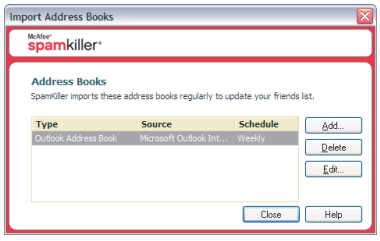
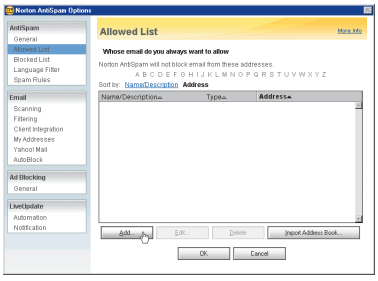
Steps	Symantec Norton Internet Security 2005	McAfee Internet Security Suite
Step 1: For Norton: click **AntiSpam**. For McAfee: click **SpamKiller**.		

Table 16-1 **Enabling Spam Blocking** *(Continued)*

Steps	Symantec Norton Internet Security 2005	McAfee Internet Security Suite
Step 2: Set the level of blocking. Start with the Medium or High setting. Click **OK**.		
Step 3: (This step may occur automatically during install.) It's possible to import address books from other e-mail programs. Click **OK**.		
Step 4: You can also add "friendly" addresses manually to your allowed list. Click **Add** to add new addresses.		

Avoid Phishing Scams

It's surprising that the security bundles, which so far have done just about everything for us, do not have specific tools to combat phishing scams. They *do* provide spam blocking, which would undoubtedly filter most if not all of them. But it is still surprising that this opportunity has not yet become apparent to the security software vendors.

On the other hand, at least one ISP (EarthLink) is hot on the trail. EarthLink provides a service they call ScamBlocker, which claims to be able to stop phishing scams in their tracks. The way it works is you have to download a web portal tool called EarthLink TotalAccess, which inserts functions into your Internet browser.

Figure 16-5 takes a quick look at the tool. (Note, however, that we did not actually test it with a real phishing scam to see if the claim is true.)

Notice the ScamBlocker icon on the toolbar after we have installed the service. We would expect the security product bundles to quickly incorporate specific scam blocking functions. (By the time this book is published and you read it, it's possible this will be a standard function, so check with your security bundle vendor.)

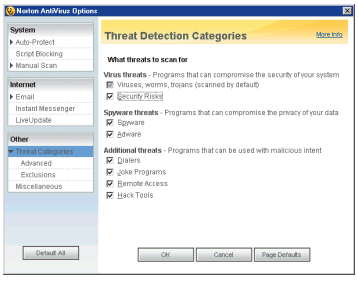
Figure 16-5 EarthLink ScamBlocker Toolbar

Set Up Spyware and Adware Blocking on Your Home Computers

So far, we have mitigated very serious security risks. We have set up firewalls, antivirus protection, and spam blockers. Now onward to some less serious threats, but nonetheless irritating. Fortunately, the security product bundles we have been talking much about do incorporate protection for spyware and adware also.

It is assumed that you already installed the security product bundle you have selected. Table 16-2 shows the process for enabling spyware and adware blocking on both the Symantec and McAfee products.

Table 16-2 Enabling Spyware and Adware Blocking

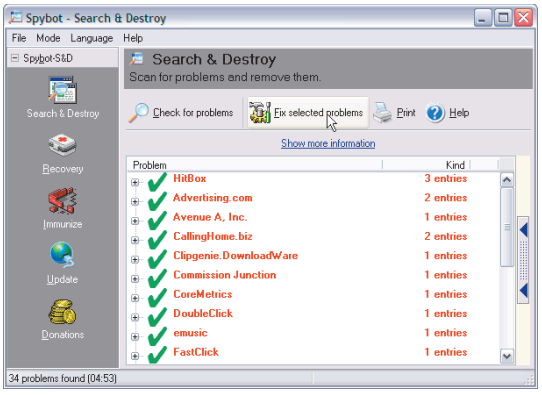
Step	Symantec Norton Internet Security 2005	McAfee Internet Security Suite
Symantec: Click **Options > Norton AntiVirus > Threat Categories.** McAfee: Click **Privacy Service > Configure Privacy Service Options** Checkmark **Prevention** of **Spyware**, **Adware**, and **Pop-Up Ads**. Click **OK**.		

To see if your computer contains spyware or adware, we highly recommend the Spybot Search & Destroy program, which is available here:

http://www.safer-networking.org/en/download/index.html

After installation, you can run a scan of your computer by double-clicking on the Spybot S&D icon, and then clicking **Check for Problems** (see Figure 16-6).

Figure 16-6 Using Spybot Search & Destroy



When the scan completes, click **Fix Selected Problems** to erase the spyware or adware.

Set Up Pop-Up Blocking on Home Computers

Blocking pop-up ads can be accomplished three ways:

- Enable built-in Internet Explorer pop-up blocker (Windows XP SP2 with IE 6 SP1)
- Install free pop-up blocker (such as the Pop-Up Stopper from Panicware)
- Enable pop-up blocking in the security software bundle you purchased

We trialed the pop-up blocking in the security software bundles and found them more difficult to disable temporarily when needed than the other two methods. So we recommend either the built-in IE approach or the free pop-up stopper program.

Figure 16-7 shows how to enable the pop-up blocker built in to Windows XP SP2. In Internet Explorer, click **Tools** > **Pop-Up Blocker** > **Turn On Pop-Up Blocker**

Alternatively, if you are not running XP, we recommend installing Pop-Up Stopper Free Edition from Panicware, available here:

http://www.panicware.com/product_psfree_download.html

After installation, a small white hand icon will appear in the lower left of your Windows toolbar. Right-click on the white hand and you can toggle the pop-up blocking function on and off very easily (see Figure 16-8).

Figure 16-7 Enable Windows XP Built-In Pop-Up Blocking

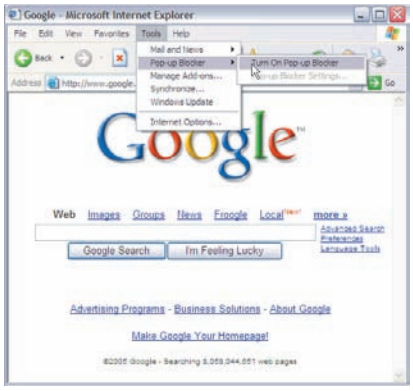
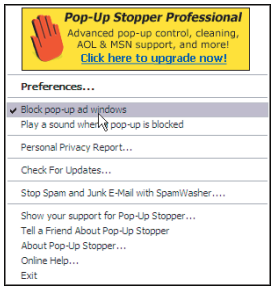


Figure 16-8 Using the Pop-Up Stopper from Panicware



Note that there are web pages that do use pop-up windows to convey legitimate information that you ask for. So, sometimes, pop-up windows are good. There is no easy answer to this problem except you can either disable pop-up blocking and endure the annoyance, or enable it and when you run into issues with some websites, disable it temporarily.

Where to Go for More Info

Visit these websites for more information on online privacy:

http://www.symantec.com/homecomputing/library/library.html

http://www.ftc.gov/bcp/menu-internet.htm

Reproduced from the book ***Home Networking Simplified***. ***Copyright© 2004, Cisco Systems, Inc.***. Reproduced by permission of Pearson Education, Inc., 800 East 96th Street, Indianapolis, IN 46240. Written permission from Pearson Education, Inc. is required for all other uses.