11 Protecting Your Privacy and Blocking Spam

DO OR DIE:

- >> Confront spam head on (you won't need a helmet)
- >> Block loading of remote images in mail messages
- >> Can I get a SPAM and cheese to go?

Ahh, spam. It's everywhere. Check out this 2004 quote from Bill Gates at the World Economic Forum: "Two years from now, spam will be solved." Well, he certainly took a rather optimistic view of how many inroads we would be able to make in the fight against spam. Instead of winning the war on spam, in many ways, we are continuing to fight a seemingly never-ending battle. Spam continues to flow into inboxes all over the world at an alarming rate. Companies scramble to implement server-side spam filters while consumers troll the web trying to find solutions to keeping spam out of their inbox and to keep themselves free of viruses, Trojan horses, and worms. Spam isn't only an annoyance—it carries a host of other threats that can be damaging to both you and your livelihood. It's also a very popular luncheon meat.

In many ways, this might be the most important chapter that you read in the Thunderbird section. First, you are probably concerned about protecting your privacy, especially when it comes to sending and receiving email. Second, you are most likely painfully aware of how precious time is and how annoying it can be to have to deal with large volumes of spam as well as the threat of viruses arriving via email messages. The takeaways from this chapter will be significant. You should come away with a better understanding of ways Thunderbird helps protect your privacy and keep you safe. You will confront spam head on by configuring Thunderbird's powerful junk mail controls so that spam will be a thing of the past, thus leaving you more time to focus on the mail that is really important to you. You will learn how to accept content from trusted

sources by blocking remote images. Finally, your odyssey will take you into the brave new world of password and privacy options as you learn about ways you can use digital signatures to protect your privacy and security.

FRIDGE

SPAM: Five Billion Cans and Still Going Strong

Monty Python has lampooned it, soldiers have feasted on it, and Nikita Kruschev claimed in his autobiography that it helped keep his army alive. What is it about this mystery pink meat encased in a blue tin that has enthralled people throughout the years?

Maybe it is because SPAM is so versatile. You can do just about anything with it—recipes abound on the Internet for various ways you can prepare this intriguing product. You can doctor it up so that it seems as if you are eating baked ham (you might try the original recipe for Baked SPAM that is on the side of the can and see if you can fool your grandmother). It also lasts a long time, so if you are one of those people who like to stockpile canned goods, SPAM might be your luncheon meat of choice. Hawaiians seem to prefer SPAM as their luncheon meat—they are currently the largest consumers of the product in the United States.

Finally, probably the most interesting question—how did SPAM originate? According to the www.hormel.com website, the story begins in 1936 when the Foods division created the recipe. Determined to find a unique name for the product, Jay C. Hormel offered a $100 prize to whoever could generate the best name for this new creation. However, there was a little nepotism involved when the finalist was selected, because Kenneth Daigneau, who was the brother of then-President Ralph Daigneau, was declared the winner. Daigneau created the unique brand name by using a combination of the "sp" from spiced ham with the "am" from ham. So if you are tired of the same old bologna, try some SPAM. I won't be trying any, though, because I'm a vegetarian.

How Thunderbird Protects Your Privacy and Security

Thunderbird does a few things that will immediately put your mind at ease:

- Thunderbird does not allow any scripts to run by default.
- Thunderbird's remote image blocking feature allows you to control remote content that is embedded in email messages.
- Thunderbird's junk mail controls offer a powerful way to filter out unwanted mail.

Why are these things important? Scripts can carry executable files that can cause irreparable damage to your email as well as to your computer. If you save your email locally to your hard drive, there are scripts that can run on your computer that can erase your hard drive—thus taking away all your saved mail in one fell swoop. Thunderbird puts you in control by not allowing these scripts to run by default.

Many spammers have now harnessed the power of remote content and are using it to harvest email addresses to propagate more spam. Thunderbird puts you in the driver's seat by allowing you to control who can send you messages and content.

Finally, fighting spam is an almost endless battle. Spammers can bring corporate mail servers to their knees and waste valuable resources. Even server-side spam filters can't catch every piece of spam. When trained, Thunderbird's junk mail controls helps keep your inbox spam-free.

Let's forge ahead and see some of these concepts in action. Pass the ham, and please hold the spam.

How to Train Thunderbird's Junk Mail Filter

Junk, junk, and more junk—it seems that some days I get more spam email than I do legitimate email. At least I don't get as much as Bill Gates, who reportedly receives four million emails a day, most of which are spam.[1] If you put your email address out in the Internet space, it is likely at some point that your address will be harvested by spammers and you will become a victim of spam email. Ready to enter a contest that has a prize that looks too good to be true? It just might be that the contest you are entering will lead you down the primrose path to an inbox full of spam (not surprisingly, the entry form probably only asked for your email address). Luckily, Thunderbird has an excellent way to keep spam in check.

Thunderbird uses Bayesian filtering to classify junk mail, which is a system that requires some degree of user intervention and training (see the FAQ on the next page for an explanation of how Bayesian filtering works). In order to train Thunderbird to weed out spam, you have to manually mark messages as Junk by either clicking the Junk icon or going to File | Message | Mark | As Junk. But the important factor to remember here is that you also need to mark your "good" messages by going to Message | Mark | As Not Junk (note that no icon is

[1] Steve Ballmer, the CEO of Microsoft, was quoted in the same story as saying that an entire department at Microsoft is devoted to doing nothing more than ensuring that nothing unwanted gets into Gates' inbox.

available for this in the toolbar). That way, you train the filter on both ends and ensure that a better percentage of spam will be captured.

Tip: In the Early Phase of Training, Check Your Junk Mail Folder

In the early days of training your filter, you will probably want to check your "Junk" mail folder just to make sure that mail has not been classified incorrectly. If it has, you will have the chance to mark it correctly so the next message that comes through will not be marked as spam.

Easy Way to Mark All Your "Good" Mail

In case you want to mark all your "Good" mail in one fell swoop, the best way to do this is to go to the View dropdown list and select Not Junk, and then go to the File menu and mark the messages as not junk. Going to the File menu and selecting View | Sort by | Junk Status is another way you can accomplish this.

Figure 11-1
The Junk icon.

Thunderbird marks junk mail with a junk icon (see Figure 11-1). Note that if you change Thunderbird's theme (see Chapter 13), the Junk icon will likely not look the same as it does in Thunderbird's default theme.

FAQ 

What Is Bayesian Filtering?

Bayesian filtering first came into vogue when Paul Graham covered it in his seminal paper "A Plan for Spam" (http://www.paulgraham.com/spam.html), even though Graham himself admits that Bayesian text classification methods have been used for years. Although Bayesian filtering is a technique that can be used to classify many types of data (it has been applied in a number of other disciplines, including the scientific realm, and has been applied in the machine learning environment in AI), programs such as Mozilla Thunderbird use it to distinguish spam email (junk) from ham email (non-junk).

The essence of Bayesian filtering boils down to examining probabilities and focuses on the probabilities of certain words appearing in ham or spam email. For example, a word such as "Rolex" might appear more frequently in your spam email, but not in your ham email (unless, of course, you are a watch dealer). Even though the filter isn't savvy enough to figure this out at first, it can be trained by the user over time.

When it is trained, a computation is made (using Bayes' theorem) regarding the probability of an email belonging to either the ham or spam category. This assessment is done by looking over all the words (or combinations of words) contained in the email. After the assessment is complete, if the total exceeds a particular threshold, the filter then identifies the email as spam. Mozilla Thunderbird has a handy feature that can automatically move these messages to a "Junk" folder.

The user-centric nature of Bayesian filtering does have some distinct advantages over systems that use other rule filter methodology or point value systems, such as Mailshield. This is largely due to the fact that we all get different types of spam and ham, and the Bayesian system allows the user the flexibility to make corrections over time in the event that email is classified incorrectly (one person's ham may look like spam to another). However, the downside of the Bayesian system is that it will not perform well if it is not trained (you must mark both the spam and ham email in the training phase), and it does need some degree of training data (a past collection of email messages is helpful in this regard).

Despite the fact that Bayesian filtering does a good job of nipping spam in the bud after it is trained, spammers are constantly developing new techniques to get mail into your inbox. Recently, I have started to see emails that have my coworkers' names inserted in the subject line. In this instance, they are attempting to defeat the Bayesian system by using familiar name patterns. While Bayesian filtering isn't perfect, it is just one method that is being used to fight the seemingly never-ending battle against spam.

Configuring Junk Mail Controls

Junk mail controls are configured by going to Tools | Junk Mail Controls, which displays the screen shown in Figure 11-2. You should first make sure that you select the account that you want the controls to apply to in the drop-down list. It is possible to define different controls for different accounts.

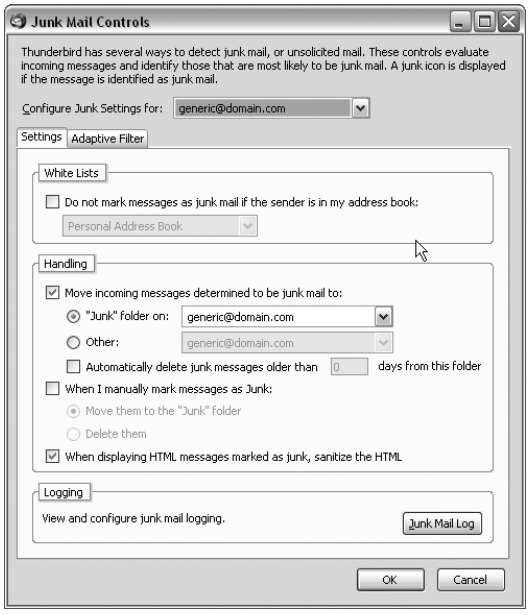

Figure 11-2
The Junk Mail Controls screen.

White Lists

Thunderbird allows you to identify your trusted senders by setting this preference. If you enable the checkbox, Thunderbird honors the address book choice from the drop-down menu and does not mark messages as junk if the sender is in the selected address book. The default setting for this preference is Personal Address Book.

Handling

In this section, you can define where you want junk mail to be routed. I prefer to select Thunderbird's Junk folder, but you can also define another place where you want junk mail to be housed. You can also define where you want junk messages to go when you delete them manually. Finally, there is a preference you can enable to have Thunderbird sanitize the HTML when messages are marked as junk.

What does sanitizing HTML mean, and how can it help protect you? By checking this preference in Thunderbird, you effectively strip out all remote requests, images, JavaScript, cookies, and tables from messages that have been identified as junk. This is another feature that protects you from HTML that may come through embedded with potentially harmful scripts or tags. This preference is on by default, and you should leave it on for the fullest level of protection.

Logging

The junk mail log allows you to keep track of the operations that are made on junk mail. To turn on the log option, click the Junk Mail Log button and then check the box that says "Enable the Junk Mail log."

Adaptive Filter

The Adaptive Filter tab (shown in Figure 11-3) allows you to manage your junk mail settings. This preference is enabled by default. It is probably a good idea to keep this checked unless you are planning to possibly use regular filters to manage your junk mail. There is also a button to reset your training data, but you probably should never have to use this button unless you want to start your filter training from scratch. Thunderbird stores your training data in a file called `training.dat` that is stored in your Profile folder. Remember, if for some reason your profile folder gets deleted, you will lose your training data and will have to retrain Thunderbird to identify junk mail (yet another reason it is a good idea to back up your Profile folder—see the Toolkit in Chapter 10, "Setting Up Your Email, RSS, and Newsgroup Accounts Using Mozilla Thunderbird," for some ideas on how to do this).

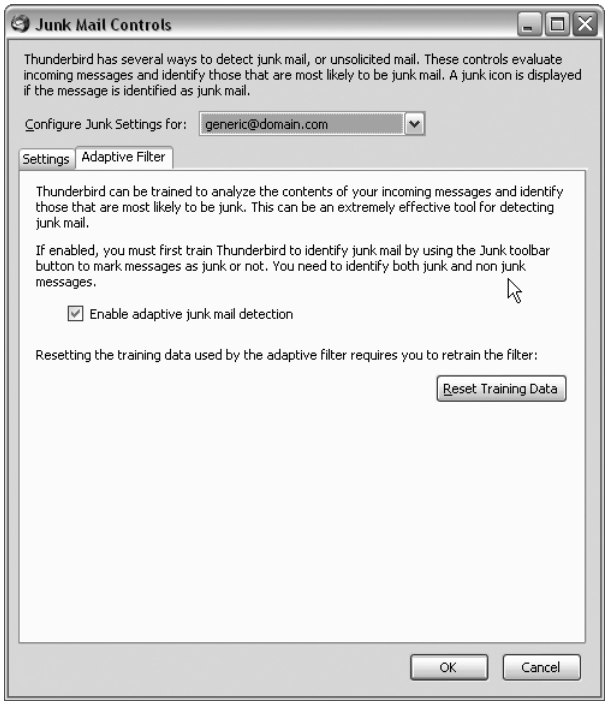

Figure 11-3
The Junk Mail Controls screen with the Adaptive Filter options displayed.

Thunderbird also gives you the ability to run junk mail controls on individual folders and delete mail marked as junk that resides in a folder. To do this, highlight the folder you want to run the controls on and then go to Tools | Run Junk Mail Controls on Folder or Tools | Delete Mail Marked as Junk in Folder.

Blocking Remote Images

Thunderbird's remote image blocking feature is a good way to protect yourself from possible contamination from viruses as well as protect you from spammers who are trying to capture your email address. This preference is on by default in Thunderbird and is set to allow the display of remote images from people in your personal address book. You can change this option by going to Tools | Options | Advanced, where you see a dropdown box that allows you to select the address book you want to use to manage who can send you remote content.

As shown in Figure 11-4, Thunderbird lets you know when it has blocked images by issuing an alert at the top of the mail message (similar to the alert Firefox uses to warn you about popups that have been blocked). If you view the email message and decide you want to see the content, you can simply click

Show Images to see the images that have been blocked. Note that after you click this option, there is no way to undo this action, so be certain that you really want to see the images before you click **Show Images**.

Figure 11-4
Thunderbird's remote image blocking feature in action.

Other Ways You Can Protect Yourself

There is another setting available in Thunderbird that you can configure to help protect your privacy and security: Return Receipt settings. You can also choose to digitally sign and encrypt your mail for an extra layer of protection, or use certificates and security devices. This section provides some other avenues to explore to get maximum protection.

Return Receipt Settings (Tools | Options | Advanced)

It is probably a good idea to configure your settings so that Thunderbird prompts you when you receive a request for a return receipt. That way, you will prevent spammers from even knowing that your account exists. (I do not recommend checking the "Always Send" box in this area—either "Ask me" or "Never send" are better choices to protect your privacy.) Figure 11-5 shows one way you can configure your settings.

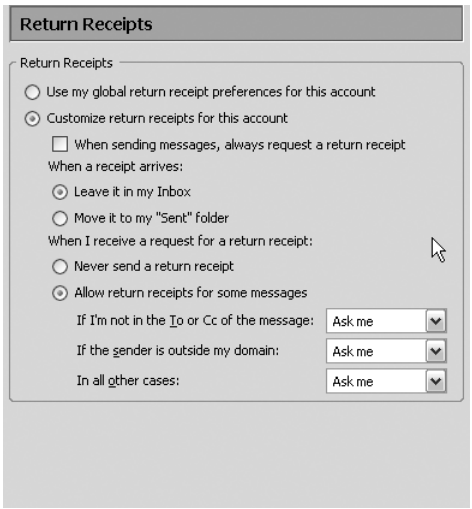

Figure 11-5
A good way to configure your Return Receipts options for maximum protection.

Anti-Virus Programs

It is important that you have an anti-virus program installed on your computer. A number of anti-virus programs are compatible with Thunderbird. See the sidebar for some tips on programs that play well with Thunderbird.

Signing and Encrypting Your Email

Signing and encrypting your email are simple but effective ways to maintain your privacy while ensuring that no one is masquerading as you online.

Digitally Signing Your Email

Signing your mail is a good thing, especially because it is often difficult to discern by looking at the email header who actually sent the mail. If more people began signing their mail, spam would probably be nipped in the bud considerably because it would be possible to configure Thunderbird to not accept mail from unsigned senders.

By using specialized cryptographic techniques such as S/MIME, you can actually include a signature that lets you stamp your outgoing messages with a signature that proves you are the person who sent the mail. For a good overview of how to use digital signing, go to http://www.cs.washington.edu/lab/services/email/EmailSigningHowTo/.

Encrypting Your Email

Encrypting your email adds an extra layer of security beyond a digital signature because the encrypted email appears as garbage data unless the recipient has the key necessary to decrypt the information. If you want to take a deeper dive into learning about how to encrypt your mail in Thunderbird, a tutorial available at http://www.uk-dave.com/tutorials/misc/enigmail.shtml explains how to encrypt your email with Thunderbird, Enigmail, and GnuPG. Enigmail is an extension that allows you to encrypt/sign sent mail, as well as decrypt/authenticate incoming mail. Go to http://enigmail.mozdev.org/ to learn more about this program and how it can help you with encryption.

Certificates/Security Devices

The certificate and security device management procedures are the same in Thunderbird as they are in Firefox. See Appendix F, "Security, Certificates, and Validation," for more information about using certificates and security devices.

Passwords

Note

Both Firefox and Thunderbird store their Master Passwords separately. If you happen to import from an older Netscape or Mozilla profile and set a master password in that profile, Firefox and Thunderbird both inherit that master password.

The Password Management section of Thunderbird can be accessed by going to Tools | Options | Advanced. Under the Saved Passwords section, you can manage your Stored Mail password settings as well as set a Master Password for your account. Note that the Password Manager functionality in Thunderbird is based on the same principles as those in Firefox, so there will be some overlap here between what is discussed in Chapter 2, "Protecting Your Security and Privacy." I have elected to go into a little more depth discussing the Master Password settings than what was covered in Chapter 2.

Managing Your Stored Mail Passwords

Clicking **View Saved Passwords** allows you to manage your stored passwords. See Chapter 2 for more information about the Password Manager functionality as well as some screenshots.

What Is a Master Password?

A master password is a mechanism that can be used to protect different types of devices (both software and hardware devices). Both Thunderbird and Firefox have built-in Software Security devices, so you are able to use a master password to manage the information that is stored on the device (literally, the software).

If you work in an office, someone probably has the master key to the office (and, if you are like me, you are usually trying to find that person when the alarm in the Riser Room is going off for no apparent reason…and Sparky is whining—well, that's another story…). While the Master Password is not actually the *Master Key* in this instance, it does protect the Master Key, which is the mechanism used to protect potentially sensitive data—things such as your email password or certificates, for example.

Why Would You Want to Set a Master Password?

You might be using a machine that other people have access to, and you don't want them to be able to download any new messages or send any messages from your account. If you have saved passwords and then set a Master Password, Thunderbird protects the saved passwords by prompting you for the Master Password when you click **View Saved Passwords**.

When you click **Show Password** in the Password Manager dialog box, Thunderbird prompts you for the Master Password before you are allowed to see the saved password information.

Setting a Master Password

In addition to being able to store your saved passwords, Thunderbird allows you to set a Master Password for your mail accounts. Follow these steps to set your Master Password:

1. Go to Tools | Options | Advanced.
2. Click the **Master Password** button.
3. As shown in Figure 11-6, make sure to check the box that says "Use a master password to encrypt stored passwords."
4. Click **Change Password**.
5. Make sure that "Software Security Device" shows in the dropdown menu.
6. Type your password twice and click OK.

Figure 11-6
The Master Password options screen.

An Extra Layer of Security—Encrypting Versus Obscuring

"Encrypting" data and "obscuring" data are two very different animals. If you elect to save your mail passwords by using the Password Manager functionality built into Thunderbird, this information is stored locally on your computer in a file that is fairly difficult to crack (but it can be done). If you enable the check

box in the first section that says "Use a master password to encrypt stored passwords," this file is then encrypted, making it extremely difficult for someone to open or view it.

Change Master Password

As shown in Figure 11-7, clicking **Change Master Password** launches a screen that allows you to change or set your Master Password. *Make certain to pick a password that you will remember*—if you forget your Master Password and have to reset it, you will lose all of your stored passwords. It also helps you to rely on the *password quality meter* when selecting a password—using combinations of numbers, letters (uppercase and lowercase), and symbols is always a good idea. Remember, if someone gets the master password to your account, he can easily masquerade as you in a number of ways.

Figure 11-7
The Thunderbird Change Master Password screen.

Don't Want Other People to See Your Messages?

Okay, I can't be the only one who detests people hovering over my computer and reading my mail. If you are an IMAP user, there is a way you can configure Thunderbird so that the message pane (which shows the subject, and so on, of your mail) renders as blank until you log in and enter a password. Sound cool? Head over to Appendix E, "Hacking Configuration Files," to learn how to create a `user.js` file, and then add these two lines to the file:

```
// Password protect the message list pane
   user_pref("mail.password_protect_local_cache", true);
```

The other option is to change the `about:config` line item from `false` to `true`. See Appendix E for more information on how to do this.

Master Password Timeout

You can use these settings to manage how often you want to be prompted for a Master Password. To be extra cautious, it might be wise to set the preference to "Every time it is needed."

Reset Master Password

Resetting your Master Password causes you to lose all your stored passwords as well as any certificates or keys.

Using Anti-Virus Programs with Thunderbird

Depending on which type of anti-virus program you have installed, you might want to consider performing scans on incoming email messages as well as outbound messages (to make sure that you are not transmitting a virus).

Email can be a little trickier to scan, depending on how and where your email program stores your email. Some anti-virus programs can't tell the difference between when a single email is infected or when an entire inbox or folder may be infected.

To make sure that you have a good anti-virus experience, you should make sure that you have an anti-virus program that is compatible with Thunderbird. For a list of programs that are compatible with Thunderbird, go to http://kb.mozillazine.org/Thunderbird_:_FAQs_:_Anti-virus_Software.

I have personally used the free version of AVG's Anti Virus (http://free.grisoft.com/doc/1) to scan incoming and outbound mail with Thunderbird 1.0 and experienced no problems.

TOOL KIT

Thunderbird Extension for Sender Verification: An Extension to Protect Yourself Against Phishing

The Thunderbird Extension for Sender Verification plugs into Thunderbird to help prevent the practice known as "phishing," which has become a widespread problem on the Internet. Phishing is a practice whereby you may get an email, purportedly from Citibank or AOL (these are two examples; there are countless others), that is not really sent by them and asks for your credit card number, password, or other sensitive information. These emails are often so cleverly designed that it is difficult to tell that they are fraudulent.

Note: If you are looking for the Firefox equivalent of this extension, see Chapter 7, "Customizing Firefox with Third-Party Extensions and Themes," for a discussion of *Spoofstick*.

This extension helps identify whether the sender of the email that appears in the "From" portion of the header was actually the domain sender of the email. It does this by attempting to verify the domain of the sending entity. For example, if generic@domain.com sends an email, the extension can report whether the email is coming from an @domain.com email domain. Note that this extension cannot check

whether a generic or any other @domain.com user was actually the person who sent the email. Remember, this extension is one way to help you recognize suspicious emails, but just because you get a positive verification on an email doesn't mean that it is necessarily a legitimate email.

Because this extension performs verification, the author does caution that information is sent to his web server in order to complete the verification. If you are not comfortable with this, you have a few choices of other ways that this can be done. Go to http://taubz.for.net/code/spf/ to read the FAQ that explains other information regarding the extension. As this book goes to press, the Thunderbird development team is working on integrating phishing support directly into the application, so there is a good chance there will be another alternative available to try to combat this problem down the road. Note that banks and financial institutions will never ask you to reconfirm user account data via email, so be wary anytime you receive an email like this, even if it looks legitimate.

Although Thunderbird contains features that can help protect your privacy and security, there are no magic bullets for trying to eliminate practices such as phishing. Spyware, worms, and viruses may be transmitted via email messages, but you can also unknowingly download them from a website, and when installed on your computer they can affect your email that may be stored locally. Remote image blocking and configuring your spam controls are two ways Thunderbird can help, but the onus is still on you to err on the side of caution when an email just doesn't "look right." One of the best ways to protect yourself is to make sure to use a good anti-virus program to scan your inbound and outbound email and to always keep your virus definitions up to date. Be cautious, watch your step, take your vitamins, and always remember to use real maple syrup on your pancakes.

Phishing

You probably won't get taken in by most spam. Let's face it: emails offering Vioxx, Viagra, or other meds, that low mortgage, get-rich-quick schemes, or mail-order brides waiting for you are all messages that don't pass the "Do I have 'born to pay retail' tattooed on my forehead?" test. Even the venerable "419" scam (where someone is the widow of some high official in Nigeria or some other war-ravaged country who has tens of millions of dollars to move out of the country and all she needs is your bank info and a small wire transfer fee) is getting so well known that entire websites like http://www.419eater.com are devoted to scamming the scammers.

Unfortunately, con artists are always looking for a new way to finagle money out of their victims. The latest version is known as *phishing*. Phishing is where you receive an email that's supposedly from some organization that you might be doing business with that hands you some variation on the following:

- Your account doesn't exist
- Your account has been suspended
- Someone's using your account fraudulently
- Your name/account number/credit card/other information has expired

These emails look official: they have the real company logos and everything. The underlying theme of all these is that something dire will happen unless you click the official-looking web address near the bottom of the email and

enter some account information so they can correct whatever little problem you're being informed of. On the off chance that you actually do so, you'll see an even more official-looking website (again, with company logos and graphics) that asks you for account numbers, passwords, and credit card or Social Security numbers.

Therein lies the problem: The emails are bogus. The websites you go to are bogus. These are bad people who will take your credit card and account information and do whatever they can with it, up to and including grand larceny and identity theft. You won't like any of it.

How can you avoid this kind of scam? The first few times you get a message like this, you may not know that it's really a scam, and it might raise your anxiety level to the point you go look at it. First and foremost, *never trust an email notification that ultimately requires you to give confidential information over the Internet*. Always check it out through several independent sources and, even then, if you aren't completely sure, don't give any information at all. (It's best to not even go to the website listed; if nothing else, phishers can often identify that it's you with the specific web address you went to and can target you for future scams. For the same reason, you should never click the "unsubscribe" options in email; these are fake and only serve to verify that your email address is live, which makes it more valuable to spammers.)

If you've just gotten email from someone, such as Citibank, MBNA, PayPal, SouthTrust, SunTrust, Washington Mutual, or eBay (among the dozens of companies currently popular with phishers), the first thing to do is to check on the company's website to see if there's something about phishing scams. If there's nothing on the main page, look in the website's "security" or "announcements" section, or just use the site search feature to look for "phishing," "scams," or "fraud." You can also check Snopes (http://www.snopes.com), the Internet Urban Legend websites, for information on the latest phishing scams.

If there are spelling errors in the text of the message, that's pretty suspicious. Most companies are very careful about spell checking their broadcast announcements, although once in a while things escape. Also, no matter how official the web address looks in the email, the actual address that you're routed to is something different. Sometimes the real address uses the website's IP address, sometimes it looks a bit like the real address, sometimes it is completely different, but it is never the same as what you think you're clicking.

Phishers send out emails by the millions. There's no reason not to expect that phishers will use other mechanisms to get you to fill in information, including credit card applications, "You've won a lottery!" announcements, and so on. (In the half-hour or so it took me to write this, I got three phishing emails supposedly from PayPal and another from some miscellaneous company promising me a free cell phone if I'd fill out a long web form.) Be careful.

One thing you can do when you get a phishing email is to send it to the company by using "spoof" as the username, such as `spoof@paypal.com`, `spoof@wamu.com`, or `spoof@ebay.com`. This helps the companies involved track down and stop phishers. You'll usually get an acknowledgment from the company about this that gives you a little information on what to do with future bogus emails.