Chapter 1

Spam and Spyware: The Rampant Menace

In This Chapter

- Understanding how spam and spyware affect the organization
- Fighting back
- Taking stock of your business
- Justifying a spam solution
- Choosing the right solution
- Making the solution work

You just got on the spam and spyware rollercoaster. In this chapter, you will whiz through a lot of topics at a high level. So please remain seated and keep your arms and legs inside the car at all times. Strap in and *hang on* 'cause you'll be plunging down the hills, whipping through the turns, and rolling around the loops.

In later chapters, you get a chance to slow down and soak up the details of all these topics, but this chapter's bird's-eye view is a good place to start if you're just beginning the task of blocking spam, spyware, or both.

Knowing How Spam and Spyware Affect the Organization

Because you're reading this book, you probably have a suspicion that spam and spyware are — or may be — affecting your business. If you have e-mail, chances are that spam *is* making an impact in your organization. And while employees in your business are surfing the Net, their workstations are becoming rotten with spyware that's doing who-knows-what. Knowing *how* the impact is manifesting itself is important if you want to get the upper hand.

Increasing e-mail volume

This is an understatement to be sure. Many studies conclude that the volume of spam entering most businesses hovers in the 70 to 80 percent range. Your e-mail servers are working hard to process inbound and outbound mail, and the majority of that inbound mail is putrid filth. If you're sufficiently privileged to be able to walk up to your e-mail server, that giant sucking sound you hear is the inbound spam choking the life out of your server.

Spam is consuming network resources, CPU resources, disk and network buffers, disk space — everything. If your e-mail server is sluggish, imagine how much faster it would run if you could eliminate 70 percent of the incoming traffic. On the other hand, if your e-mail server *is* able to keep up with the torrent of filth, it's because you bought a system far larger than should have been necessary, in order to manage the relevant business e-mail *and* the spam.

Everybody is in the same situation: Either they've had to invest more capital dollars in e-mail servers to keep up with the growing tide of spam, or else their mail servers are suffering under the workload.

If you are so well organized that you have statistics on inbound e-mail volume over a period of years, I'm willing to bet that you can see that the volume is increasing at a rate that significantly outpaces any increase in the number of employees in your organization.

Draining productivity

Almost all organizations have their share of employees who are drowning in spam. Three to five hundred spam messages per day for some employees is not uncommon these days. Those employees come from every level in the organization, from executives to call center employees, and everybody in between. So what is it like for these employees? I have spoken to more than just a few; here is what some of them have to say:

> "It takes me longer to get through my e-mail because I have to weed out all the spam first."
>
> "I can't stand the porn — even the subject lines are lewd and offensive!"
>
> "My spam filter at home frequently throws away messages from friends. I can't afford to have a spam program at work toss out important messages from customers or suppliers."
>
> "Yyyyyyuck!!"

These comments point to some of the key problems that result from employees dealing with spam, which include the following:

- **Extra time spent sifting through all e-mail in order to identify and delete spam messages.** This becomes increasingly difficult as spam messages look more and more like ordinary messages.
- **E-mail quota problems due to spam filling up users' mailboxes.** This is especially troublesome for those who travel, unless they are able to log in almost every day and delete all the spam from their inboxes.
- **Loss of important business e-mail messages that were accidentally overlooked and deleted.** Legitimate messages often get caught in the crossfire whether or not a spam-blocking solution is in place.
- **Phishing scam messages that look like they originated within the company or from a legitimate outside source.** Sometimes, these scams result in virus infections, security breaches, fraud, and other issues.
- **Employees who are enticed to visit Web sites waste more time and increase the risk of security issues caused by the hostile code on Web sites.**
- **Increased computer support costs.** Employees who are plagued by spam and related maladies are certain to be calling the IT helpdesk more frequently than employees who receive little or no spam. You are fortunate if your helpdesk tracking data is granular enough to capture this information.

Unless you are in the upper echelon of IT organizations that measure and categorize every electron, the spam problem is more likely one that you feel in your gut. You know it's a problem, perhaps a big problem. If you're wondering how to quantify and justify a way out of your predicament, you'll find the answers in Chapter 4.

How spam got its name

Funny names are ascribed to otherwise-mundane components in the technology world. An e-mail popup in X-Windows (a windowing system like Microsoft Windows that was invented ten years earlier) was called "biff," which was the name of the programmer's dog. Those little session- or person-identifiers that your browser stores on your computer are called "cookies."

And, of course, junk e-mail is called spam. But why "spam"?

The term "spam" was first coined in the 1980s to refer to various means of sending lots of useless information to a computer in order to overload it or be annoying to its users (or both). The Monty Python "Spam" skit was new and popular among computer science students and early (now aging) computer professionals. Reportedly, those in the Multi-User Dungeon (MUD) community originally coined the term and brought it to USENET and eventually e-mail. Legend has it that someone programmed a macro to simply post the word "spam" every few seconds (like part of the lyrics from that Monty Python skit where they simply repeat the word "spam") . . .

```
SPAM SPAM SPAM SPAM SPAM SPAM
   SPAM SPAM SPAM SPAM SPAM
   SPAM SPAM
```

. . . until someone finally kicked him off.

Exposing the business to malicious code

Through the year 2003, almost no spam carried malicious payloads such as viruses, worms, and Trojan horses. Spam was just spam. This changed in 2004 (how could you *not* have noticed?) with the apparent — uh, *obvious* — growing alliance between virus writers and spammers. Theirs is a symbiotic relationship: Spammers give virus writers the means to distribute their wares, and now spammers can do more than just send junk mail — they can control their victims' computers. I discuss this topic at length in Chapter 3.

Organizations with a sound antivirus infrastructure can take some consolation in the fact that their antivirus software will strip the malicious code from most inbound spam messages. Mail servers that are configured to strip executable attachments from incoming e-mail messages are contributing to the defense.

Worse yet, antivirus programs have been "looking the other way" when it comes to spyware. Spyware isn't stopped by most firewalls, mail servers, or antivirus programs, and often the flaws (in configuration, as well as vulnerabilities in design) let the spyware just waltz right in to end-user workstations to listen, snoop, and sometimes send data back to the hacker's home base. Spyware also raises support cost because much of it makes browsers unstable, and some spyware makes changes to Web browser configurations that users notice — like changing the default home and search pages.

But is it safe to assume that 100 percent of end-user workstations are adequately protected? You can fool yourself, but you can't fool me. Sobering lessons from the past should certainly convince IT professionals that a few viruses — and a *lot* of spyware — are getting through the defenses.

Face it: Spam is clogging the pipes and it has *attitude,* and spyware is just a little too nosey for most people to tolerate. An antivirus solution only handles one small aspect of the spam and spyware plague: It strips malicious code (*most* of the time), but does nothing about the growing volume of inbound e-mail, and it often lets spyware right through.

Creating legal liabilities

Aside from being among the unfortunate ones whose inboxes are hammered by spam every day, most legal departments have not yet addressed issues of corporate liability in connection with spam or spyware. That, however, is changing.

Subjecting employees to offensive language and images

An appreciable amount of spam is pornographic in nature, and this naturally means that employees who receive spam are going to get messages that contain content that is offensive to many people. And this is not just in the content of

messages: Spammers are becoming more brazen and are including suggestive and offensive messages right in the subject lines. This is an irritant to many, but it's insulting and distressing to others.

Some spammers have been sending messages containing *only* graphic images as one method to dodge spam filters. For spammers in the business of distributing promotional messages for porn sites, this usually means that these images contain pornographic pictures. Depending upon how an organization's choice of e-mail clients, their default configuration, as well as how employees use them, this can mean that employees who get flooded with spam will be subjected to pornography and other offensive images.

In many instances, porn spam is sending some employees "over the top," resulting in grievances and even threats of lawsuits. Organizations that are doing little or nothing to stop spam probably do not have much of a defense, I am sorry to say. Employees who are distraught because of the offensive nature of spam have a strong case for relief. They also have my sympathy — I don't like the stuff either.

Leaking corporate information via spyware

Spyware collects information as relatively harmless as a user's surfing habits, and as harmful as key logging (spyware that records your keystrokes and sends the record to someone else). A corporate user's workstation with a working key logger can create liability if it captures a user accessing sensitive information, *and* the key logger's owner subsequently compromises that data.

Downstream liability if spam originates from company computers

Figuratively and literally speaking, spam messages have no return address, so it is difficult to pin the blame on those who originate the messages. However, if a company's own e-mail server or one of its end-user workstations was being used as an e-mail relay (a system that spammers use to "originate" their hordes of messages), other individuals or companies being subjected to this spam could build a legitimate grievance against the company whose computer is being used to relay spam.

A spammer can use a company's e-mail server as a relay if the e-mail server is still using old e-mail server software. In the old days, relaying e-mail through an e-mail server was a common practice for moving legitimate mail, but now only spammers utilize this now-antiquated function in order to cover their tracks.

An organization ought to know how to prevent its computers from becoming spam relays. Any organization that fails to fulfill its due diligence in this regard can be found negligent and be subject to civil lawsuits. Organizations that forward spam (or propagate other security threats) cannot completely escape culpability.

No Silver Bullets: Looking for Ways to Fight Back

Malware (which includes spam and spyware, but also viruses, Trojan horses, and really anything that you don't want running on your computer and would prevent if you could) is a complex problem that comprises threats and issues on many levels, and no single remedy can eliminate it. Your best defense against spam and spyware is *defense in depth,* which is much like the multiple layers of defense of a medieval castle.

A castle may have a moat (a body of water surrounding the castle), with a hungry moat monster swimming around. The castle also has a drawbridge, heavy gates, high walls, and places where archers can shoot arrows at attackers and others can pour boiling liquids on would-be attackers who make it across the moat. This castle has many layers of defense. Should any one or more of these layers fail, other layers continue to provide protection.

Similarly, you can best stop (it would be more accurate to say "slow down") the harmful and annoying effects of spam by using a variety of remedies, which I introduce in the following sections. Chapter 13 is dedicated to this topic and offers even more details.

By themselves, some of the remedies I discuss will, to some degree, hinder the effectiveness or penetration rate of malware. Together, they represent a multilayered defense that provides a good level of resistance against spam and spyware.

Adding a spam blocker

A key component of your defense is a spam blocker, more often called a spam filter, which you purchase from an outside vendor. These solutions all use the same basic features to identify and weed out spam:

- **Vendor-supplied filtering rules and signatures:** Computer code and a list of known spam patterns (like fingerprints) that the spam-filtering software uses to identify messages as spam.
- **Enterprise filtering policies:** Centrally managed configurations that reflect the company's needs.
- **User preferences:** User-definable settings that tell the spam filters about spam that individuals find especially irritating, as well as options on how the product behaves on users' workstations.

- **User blacklists and whitelists:** Lists of known bad addresses (that go in the blacklist), and addresses from outsiders whose incoming messages should never be tagged as spam (whitelists).
- **Quarantines:** The holding places where spam messages are stored until individual users can look to see if any good messages were accidentally blocked by the spam filter.

Figure 1-1 shows how a typical anti-spam application works. Exactly *how* each application performs these functions varies considerably from vendor to vendor. The following steps explain what's going on in Figure 1-1 in more detail:

1. **Inbound e-mail arrives at the anti-spam application.**
2. **The anti-spam application examines the message and compares its contents with enterprise filtering policies, vendor-supplied filtering rules, end-user preferences, blacklists, and whitelists.**
3. **The application uses the comparison to decide what to do with the message:**
   - **If the message is permitted to pass,** the application forwards the message to the enterprise mail server, which will in turn route it to the recipient's mailbox.
   - **If the message is not permitted to pass,** the anti-spam application will check to see if the recipient has a quarantine. If the recipient does have a quarantine, the anti-spam application will put the message there. If the recipient does not have a quarantine, the anti-spam application will delete the message.
4. **When the end-user logs in and runs her e-mail program, she will look at messages in her inbox.**

   If there are any messages there that *should be* classified as spam, the spam application usually provides a way for the user to specify that fact so that similar messages will be rejected in the future.

   I discuss wrongly identified messages (false positives and false negatives) and how to handle them in Chapter 11.
5. **If the end-user has a quarantine, she will also have to examine it from time to time to make sure that there are not any messages there that should not have been blocked.**

   If there are any desired messages (false positives) in the quarantine, the user tells the anti-spam application that any messages from the sender should be accepted; that e-mail address will be placed in the user's whitelist. Usually the anti-spam application will also forward the message to the user's normal mailbox so that she may open, read, reply, and store it using her e-mail program.

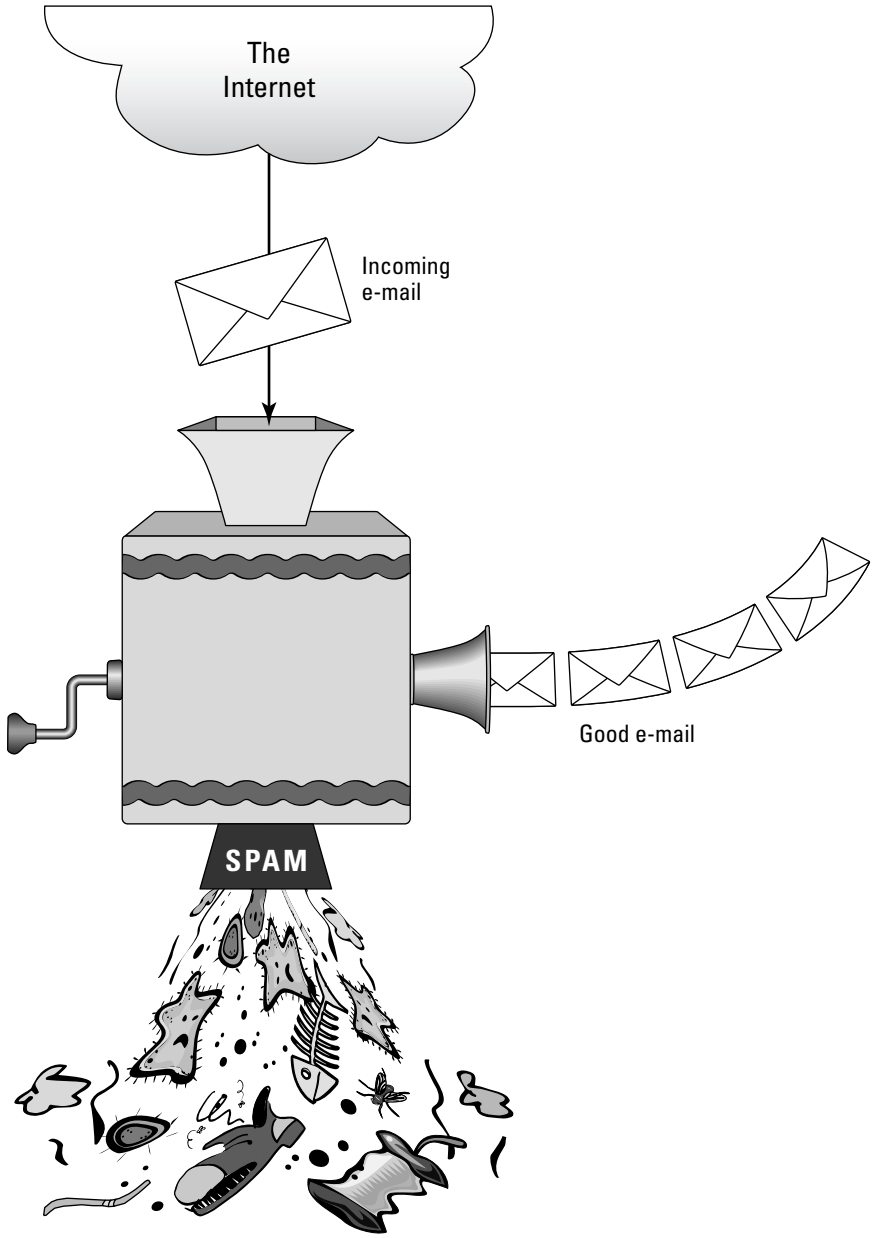

Figure 1-1: Conceptual anti-spam architecture.

Resisting the urge to counter attack

Some suggest that everyone should take up arms and form nineteenth-century style vigilante squads, or perhaps hire bounty hunters, to hunt down spammers. I'm sorry to tell you, Sheriff, but until you figure out *who* the spammers are and *where* the spammers are, you should leave your torches and axes in the back shed.

Some suggest that retaliation or counter-attack wouldn't be such a good idea anyway. The hacker and spammer crime families have recently intermarried, and so I think that any retaliation against spammers (supposing that you would be able to identify them) would be met by fierce retribution. After that, a lot of spam wouldn't seem nearly so bad.

Most anti-spam applications have several other characteristics in common:

- Anti-spam applications generally keep pretty good statistics as a way of tracking how many messages are being blocked, as well as other details.
- Many anti-spam applications permit the administrator to specify which users will have a quarantine and which will not. Inbound messages identified as spam can be "tagged" (usually by adding the word `[SPAM]` to the subject line, or they can just be deleted.
- Users can edit their whitelists, blacklists, and other preferences as often as they wish.
- Anti-spam applications will have not only simple filters containing key words, but also one or more complex algorithms that are used to differentiate spam messages from non-spam messages.

When you understand these principles and characteristics, you'll be in a position to talk with vendors (as well as people in other companies who are using anti-spam solutions), ask the right questions, and understand the answers. Then you can begin thinking about how you might block spam in *your* organization.

Because an anti-spam solution is essential to keeping as much spam as possible out of employees' inboxes, I spend a lot of time explaining them in more detail throughout this book. I explain what you need to know about your business in order to choose an anti-spam solution in the section, "Taking Stock of Your Business," later in this chapter. In the "Choosing Anti-Spam and Anti-Spyware Solutions" section, later in this chapter, and also in Chapter 5, I offer more details about the different models and features.

Keeping spyware away from workstations

There has been serious debate about the links between spyware and spam. Nonetheless, most Internet users dislike the very idea that companies are tracking their movements. At this level, spyware is an affront to privacy, and people feel better when they know that spyware is being blocked or, at least, periodically scanned for and removed.

But spyware doesn't just stop there. Some forms of spyware attempt to do more than just track users' movements: They also change Web browser settings by changing the home page, the search page, inserting bookmarks, and other intrusive pranks. Some of this spyware digs in deep: Last year I was searching for something, went to a Web site, and my PC was injected by Xupiter spyware — and it was a real pain to remove.

The most insidious spyware is the *key logger:* Software that records keystrokes and mouse clicks in the hopes that a user will type in user IDs and passwords to financial services Web sites, so that the key logger's owner can later use the captured user ID and password to vacuum out the poor user's account.

Good anti-spyware tools are available: Some for a fee, some for free. But by the time you read this, spyware blocking will be a part of most antivirus companies' portfolio of products, perhaps even built right in to antivirus software.

If you are concerned about spyware, you're already in the right place. The book that you are holding is devoted to spam *and* spyware — what they're about and how to get rid of them.

Walking through protocol holes

Spam represents one of the more recent methods used to smuggle worms and viruses into organizations. Gone are the days when a hacker could scan selected organizations (or randomly chosen ones) to look for open and vulnerable protocols that could be exploited for fun and profit. As organizations began to implement firewalls and close off all unnecessary ports, hackers had to find other ways to get inside.

Anymore, those methods include sending malicious code to millions of office workers via spam. The other popular method is to attack a Web-based application using buffer overflow or SQL injection attacks, for instance.

These attacks have been successful because they travel through ports that are left open to facilitate needed services such as e-mail and Web. They are also successful because some firewalls are not designed to perform "deep inspection" — that is, to examine the *contents* of a network packet to determine whether it contains malicious or potentially damaging code.

The methods of attack are growing more complex and difficult to stop. Despite advances in firewalls, antivirus, anti-spam, anti-spyware, anti-this, and anti-that, attackers will continue to be cunning and creative, keeping everyone ever vigilant and watchful.

Do Not Spam list

CAN-SPAM legislation in the U.S. requires that the FTC (Federal Trade Commission, the government bureau that oversees and regulates commerce) study the feasibility of creating a national Do Not Spam list that would be similar to the Do Not Call list that telemarketers are required to conform with. However, the FTC has thus far recommended against the creation of a Do Not Spam list. Unlike telemarketers, who are relatively easy to find, spammers send their spam through thousands of open relays (e-mail servers with older versions of software that permits mail to be relayed through them in order to hide spammers' tracks) and *zombified* computers (a technical term meaning home users' computers that are possessed by hacker-spammers' Trojan horse programs, permitting spam relaying). Further, spammers frequently operate — or relay their messages through — overseas connections, which is one means to distance themselves from the long arm of the law.

Thus, it is thought that a Do Not Spam list would actually become a Do Spam list, because spammers are accustomed to operating outside of the law.

Other good defense-in-depth practices

In addition to blocking spam and spyware, you need to employ the following remedies to keep your company secure (I discuss each of these in turn in Chapter 13):

- Attachment filtering at the e-mail server to remove potentially harmful executable files
- Antivirus software at the mail server *and* at users' workstations in order to stop known harmful malware
- Popup blockers on users' workstations that block this irritating and sometimes-harmful pest
- Firewalls — on laptops as well as at the enterprise perimeter — to block the entry of self-propagating worms

Understanding the role of legislation

Those of you who have been tracking the volume of spam in relation to United States regulation of CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003) can attest to the effectiveness of legislation thus far: Nil. Nada. Zilch. By now, anyone who was hoping that legislation would have any effect on spam has realized that spammers have taken no notice of the change in the law, primarily because most of them have already developed methods that make it difficult to trace any spam to them. One need only look to drug trafficking or Prohibition-era liquor smuggling to

realize that those who make their livings working on the wrong side of the law are not easily deterred or discouraged by additional legislation.

In response to citizen outrage against spyware, some U.S. state legislatures have introduced and passed anti-spyware legislation. But don't think this will make spyware go away anytime soon, either. Some spyware writers sneak in their wares with what appears to be legitimate software, and *tell* you on page 50 of the end-user license agreement — in microscopic type — that they will be spying on you. In these types of circumstances, it may be difficult to make a law that hinders their spying ways.

As I write this chapter, several known spammers have been apprehended and charged with spamming under state or federal laws. Many others have been arrested and charged with crimes, or sued by ISPs in civil court. But it's too soon to tell whether there will be enough successful prosecutions to make a dent in spam.

Taking Stock of Your Business

I'm not sure of your mindset, but I figure (shhh, I'm concentrating) it is one of these: You *know* that malware is an issue in your organization, or you *suspect* that spam or spyware may be an issue, but you aren't sure how to find out for certain — or how to find out how big an issue it may be.

I don't know very much about your organization, so I'm going to throw out a bunch of general ideas. Your job is to take those that make sense in your situation and refine them as much as you think you need to.

Before you get started, remember that you can make measuring spam as scientific as you like, but the effects of spam, such as degraded network performance or lost productivity, are about as fuzzy as you can get. Measuring the impact of spyware is a bit more difficult in that it's trying to stay well hidden, and the costs can be harder to assign because they may include public relations risks (from spyware exposing customer information) or the loss of confidential information (such as where certain researchers in your organization are browsing on a regular basis). Assigning dollars to these losses is about as much fun as taping jelly to your window. But still, you gotta start somewhere — how about here?

Talk with people

For some of you, this is painfully obvious, but I include this here anyway because of its vital importance. You cannot (and should not) assess spam or spyware's influence solely by crunching numbers your computer. There's no substitute for getting out and talking with people. Here is a list of different people you need to talk to, in no particular order:

- **PC helpdesk:** The helpdesk folks can tell you whether they get many calls about spyware or spam. Most users in an organization have the sense to call the PC helpdesk if malware is making them crazy, even if all they can do is complain. If the helpdesk tracks these calls, this would be good information to have. The more detail you can get here, the better (to a point).
- **Malware victims:** You can likely get the names of these people from the helpdesk. How long have they had the problem? How many spam messages per day do they get? Rough orders of magnitude are fine here — do they get 10, 100, or 1,000 spam messages per day? Is spyware installing when they visit Web sites or click on installers that they believe are benign?
- **Other people you work with:** I'd venture a guess that if you know ten people in the organization, one of them gets more than just a few spam messages every day. In the current IT environment, I'm certain that you know someone with spyware that he or she can't seem to get rid of.

If you're like most IT people, you don't have a lot of time to do this, and even less to spend an appreciable amount of time trying to cook up estimates on the number of spam messages that your entire organization receives on an average day. To get a broader perspective on how spam is affecting users, a survey can be a more time-efficient approach, as I explain in the next section.

Conduct a survey

A useful way to get information in a consistent format from larger numbers of users is to survey them. You can develop an online survey, or use e-mail, or even paper. But to attain statistically significant results, you need to survey more than a handful of users. Regardless of your survey medium, the following list provides some questions that you can start with. Add more of your own if you want to. Remember to ask for each respondent's name, department, extension, and e-mail address so that you can follow up if you need to.

- About how many e-mail messages do you send to Internet users per day?
- About how many e-mail messages do you receive from the Internet per day?
- How long have you worked in this organization? And (if appropriate), How long have you had e-mail in this organization?
- Have you received any spam messages in the past month? (If the answer is no, users can stop here.)
- About how many spam messages do you receive per day?
- Does your e-mail address appear on the company Web site?
- Does your e-mail address appear on other Web sites, or in newsgroups, online communities, or other locations?

You could ask more questions and get more detail, but I think you would overburden yourself making sense of the survey results. Two thoughts: First, you can always follow up with a more detailed survey for users who get a lot of spam, and second, I think you should talk with a number of the victims in person in order to better understand the spam problem as they perceive it.

If you can survey and talk to enough people, you should be able to extrapolate (guess) how many people in your entire organization get spam, and how much. Rough estimates are all that you need. Don't go overboard by asking everyone to count, unless you want to be run out of town.

Understanding your architecture

The size and makeup of your technical infrastructure will influence your approach when you begin looking at various types of spam-blocking solutions. You need to resist looking at specific solutions until you have a good understanding of your organization's architecture: size, geography, network design, and how e-mail is moved around.

Before you can begin thinking about any specific spam-blocking solutions, you must have a thorough understanding of how your present e-mail system — and by "system" I mean *everything*: Servers, clients, and every component in the enterprise that stores, processes, or transmits e-mail, from the Internet router to users' workstations, and everything in between.

Several factors contribute to the size and type of anti-spam solution that you should consider. These factors include

- **Number of e-mail users:** It is convenient to speak about the size of an organization's workforce in terms of orders of magnitude: Are there 10, 100, 1,000, 10,000, or 100,000 users in the enterprise? Solutions ideal for organizations with 10 or even 100 workers are probably infeasible for organizations with 10,000 or more people.
- **Network architecture:** This isn't so much about hubs, switches, or VLANs. Instead, focus on a few basic items such as how many Internet connections your organization has. If your company has more than one Internet connection, does e-mail enter by more than one Internet connection?
- **Geographic makeup:** Are your users and e-mail servers are located in the same building, or are they scattered all over the country or the world? Some anti-spam solutions fit best when they are very near (both physically and logically) to the e-mail servers. Other spam solutions are installed in the e-mail servers themselves, so you'd better figure out where they are.
- **E-mail architecture:** There are so many different ways that organizations can — and have — put together their e-mail environment. One organization might have one or more Microsoft Exchange servers (large organizations

can have dozens), another may use Lotus Notes, another may have open-source POP servers, and another may have its e-mail hosted by an ISP. It is also important to know — in detail — how e-mail gets into the organization in the first place. Perhaps it first hits a UNIX-based SMTP server and gets routed to the appropriate internal server, or maybe inbound SMTP sessions are terminated directly on one or more internal Exchange or Lotus Notes servers. If your organization is lacking detailed diagrams of its e-mail architecture, it's time to sharpen your pencils and get drawing.

Taking users' skills and attitudes into account

As I often say, if you need new technology in an organization to be successful, you must have not only a deep understanding of the underlying and surrounding technology, but also a keen insight into the people who will use it. Here some human factors to consider:

- **How much training will users need, and how much training can you provide?** Some anti-spam solutions incorporate changes in users' e-mail interface. In all but the smallest organizations, this means that users will need some level of training in order to understand the new controls and how they work. This can be a challenge in large, distributed organization where many users may be located in remote offices, retail locations, or even overseas. You need to find out what types of training have been successful in the past, and see if you can use those methods here. Chapter 7 covers training in detail.
- **What is the attitude toward technology?** Do the organization's e-mail users embrace new technology, or do they whine about it? This is important because any new technology project will be successful only to the extent that it is accepted and used. If the people in your organization are stubborn and resist new technology, the project may be in danger of failing. The better you know your users, the more familiar you will be with their attitudes. If you don't know many of your users (those inside IT don't count, if that's where you work), now is a good time to get out there and meet people.
- **Will you have executive support?** Closely coupled with what I call "technology attitude" is the extent to which the organization's senior management openly embraces new technology. If senior management rejects a new anti-spam tool, so too may many — or most — of the employees in the rest of the organization. You (or your manager) need to find out what executives are thinking about spam — whether they perceive it as a problem or not. In Chapter 4, I cover how to financially justify your filtering project by calculating the return on investment (ROI) for the project, which may help garner executive support.

If you are purely technocentric and don't like to deal with the human side of technology projects, then you need to find a manager, project manager, business analyst, or someone with similar project-management skills in your organization to deal with the human side of things so that your anti-spam project can be successful. Or you may need to get in touch with the right side of your brain — you never know who you might meet.

Evaluating available skills in IT

Few, if any, anti-spam solutions are truly easy to install and maintain, but instead require some level of expertise so that someone in your organization can keep the fires burning, so to speak. An effective, although complex, anti-spam solution is no bargain if no persons are available to train on it. Here are some pointers:

- **E-mail administrator:** How skilled is your e-mail admin — did this person design and build the infrastructure, or does he just manage user accounts and groups? A deep knowledge of e-mail message processing is needed, because the anti-spam solution will likely change it in some major way.
- **Network engineer:** Did the current staff build the organization's network, or have they made any significant changes to it? A spam-blocking solution may require expertise in DNS, firewalls, and DMZ architecture.
- **Helpdesk/PC support staff:** Good people and training skills are needed here, because many people will get frustrated or won't understand what is going on. Remember, success is in the eyes of the beholder: Regardless of the technical beauty of the solution, if the users don't understand how to use it, your project may be labeled a failure.

Other positions and functions in IT may also be affected, but probably less so. But you need to keep this concept in mind: Training will be needed not only for users, but also for many in IT who play a part in designing, implementing, maintaining, and supporting a spam filter.

Working within your budget

Money, of course, is always a factor in what you can do. When you start looking at anti-spam solutions, knowing your price limits can help you find the right one. I suggest you contact a few vendors (you can find a list of several in Chapter 14) and get some rough pricing for your organization. Then you will have a vague idea of product cost; next, you need to take a stab at how much, if any, professional services or consulting you will need for design, implementation, rollout, and training. If you aren't experienced at this type of resource planning, find someone who is and ask him or her to help you.

Size is everything when estimating costs. In a smallish organization (say, less than 200 users, all in one location), it will be possible to make rough estimates of consultant and contractor hours you need to complete the project. But larger organizations (hundreds or thousands of users, possibly in many locations), implementation and training will take considerably more planning before you will have even an order-of-magnitude estimate of total project cost. Again, someone with experience in such project planning and budgeting is needed to sketch out a rough total project cost.

Justifying Spam and Spyware Control

By the time you get to justifying spam control, you are pretty sure that your organization will be better off with a spam-blocking solution than without one, despite the potentially high cost (both time and money) required to put a spam-blocking solution in place. It will take a little more sleuthing to justify blocking spyware, because for most users, it is an invisible problem that you'll need to ferret out.

Justifying investment in security projects is often tricky and slippery business. Calculating a return on investment (ROI) for a solution that *prevents* an event's occurrence is especially tricky to calculate. Partially, this is because it may be difficult to estimate the impact and true cost of an occurrence — in this case, a spam message that a user receives and now must do something about.

Spam affects an organization in several ways, including

- **Productivity:** Spam wastes peoples' time — maybe a little, maybe a lot. Users have to sift through messages and delete them (and sometimes they read them, and maybe even visit the spammers' Web sites, oh my!).
- **Support costs.** Many users call the helpdesk to complain about spam and to ask that it be stopped.
- **Liability:** All the lewd material filling up employees' mailboxes may create a situation where employees feel badgered and abused, particularly if the organization is doing nothing about it. A different angle on liability may result when employees find themselves victims of phishing scams that were delivered to their inboxes.
- **Overhead:** The additional volume of spam is filling up networks, servers, and mailboxes. Much of the continued investment in the capacity to process e-mail is used to process spam, like it or not.
- **Malware:** An increasing percentage of spam contains malicious code (viruses, worms, Trojan horses), some of which might just sneak by other defenses and disrupt the business.

In some organizations, you (or someone else) will need to turn one or more of the problems in the preceding list into dollars and cents that can be measured before and after the spam filter is in place. In other organizations, a qualitative justification may be more compelling.

Spyware's effect on an organization is usually less complex than spam: It gunks up workstations and causes more helpdesk calls, usually about unstable browsers or mysterious home page and search page configuration changes. I haven't yet met a user who called the helpdesk to complain about the key logger that was installed by a Trojan horse. How is a user going to notice *that?*

If you're not sure which approach is right for your organization, you need to start talking with your managers or others to better understand what kinds of approaches for justifying projects (especially security projects) have worked best in the past. In Chapter 4, you can find more about calculating ROI and quantitative and qualitative justifications.

Choosing Anti-Spam and Anti-Spyware Solutions

After you understand how anti-spam and anti-spyware solutions work and spend time getting to know your business and its needs, you're ready to start shopping around.

If you like choices, then an enterprise anti-malware project is going to hold your interest, because several types of solutions are available for enterprises. Anti-spam solutions come in four basic setups: software, appliance, ASP, and client-only. Each setup handles the key features of an anti-spam solution a little differently. Anti-spyware is widely available for workstations, but by the time you read this, I would not be surprised if one or more anti-virus appliances or gateways also blocked spyware.

If you spend time understanding your business, you'll save time in the long run. This understanding helps you quickly rule out options that won't work. Compare the list of needs that are important to your business with the key features of a spam solution. Here, I help you understand what those features are and how the different models compare.

Types of anti-spam solutions

As I mention earlier, anti-spam solutions come in four varieties:

- **Software model:** Several software-based anti-spam solutions are available that you load on a dedicated server or right on your e-mail server.
- **Appliance model:** In anti-spam solutions, the appliance acts as sort of an e-mail firewall, in that it logically is placed between the Internet and enterprise mail server(s). The anti-spam appliance examines every incoming mail message and, using a list of filtering rules, makes a pass or block decision for each message. I'll grant you that software and ASP solutions *also* are e-mail firewalls — it's just that an appliance solution also *looks* like one.
- **ASP model:** ASP stands for Application Service Provider, meaning the application resides on a computer located elsewhere, and what you're buying is essentially a *data service,* in this case e-mail filtering. Anti-spam companies offering the ASP model perform all the spam filtering on their physical (or logical) premises, and deliver only the clean e-mail to you.
- **Client-only model:** Anti-spam software that is wholly contained on the end-user workstation is definitely worth considering if you have a small number of users (exactly how small is up to you). That's because you could install it on workstations one at a time as users complain about spam, and you can control how that spam is filtered based on individual needs. However, this solution has its downside, too. Most client-side solutions offer no centralized management or reporting capability, and these solutions don't keep the spam off your mail servers, because they don't filter messages until they reach the desktop.

If you're in a medium or large organization and are fortunate enough have only a few users with spam problems (tell me your secret!), client-only might also be for you. Just remember that it won't scale (if you change your mind and decide that all 5,000 users should have it — trust me when I tell you that you'll likely regret installing client-only spam filters on that many workstations), but that may be okay for you for now.

Chapter 6 explains the different types of solutions in more detail.

What are the key features?

All anti-spam solutions offer some of the same basic features (they block spam, of course, but you knew that). Here are some questions to ask about those features when you look at any anti-spam solution:

- **Administration of underlying operating system:** Relevant only for a software-based solution. Whether UNIX or Windows, someone will have to spend some time maintaining the operating system: installing patches, making configuration changes from time to time, and monitoring resource consumption and performance.
- **Enterprise policy administration:** Centralized spam blockers, whether software, appliance, or ASP, require some amount of company-level administration, including whitelist management, quarantine management, and adjustments to the degree of filtering, should too many or too few messages be tagged as spam.
- **Need for performance upgrades:** As the organization and/or the volume of e-mail grows, someone needs to watch resource utilization over time so that any upgrades to server hardware and network capacity is anticipated and dealt with proactively.
- **Signature and algorithm updates:** In order to stay effective, a spam filter must have the latest *signatures* (characteristics of known spam messages) and rules (ways to calculate whether a message is spam or not). Spam filters accomplish this by periodically downloading updates from the spam filter's vendor. Someone needs to watch this diligently to ensure that this always works properly.
- **How much server space does this solution require:** If you need to purchase additional hardware to run your spam-blocking solution, do you have the room (floor and/or rack space, power, cooling, and so on) required to accommodate it?
- **Directory harvesting attacks:** Spammers and hackers use some techniques to coax e-mail addresses out of an e-mail server — or at least they try.
- **Your level of control:** Only you can determine how much control you will have: Do you want the power and flexibility to be able to manage the OS that is "under" a spam filter, are you content with a "black box" appliance, or do you prefer to let an ASP filter your e-mail on its premises?

Choosing the right model

Personally, I love side-by-side comparisons and offer one for you in Table 1-1. For each of the features I cover in the preceding section, you can see how each

model measures up. For more details on choosing an anti-spam solution, see Chapter 6.

Table 1-1 Side-by-Side Comparison of Anti-Spam Solutions

Feature	*Software*	*Appliance*	*ASP*	*Client-Only*
Administration of underlying operating system:	Up to you.	Little or none.	None. This is why you out-sourced it.	Not fun, because you have dozens, hundreds, or even thousands.
Enterprise policy administration:	Centralized.	Centralized.	Centralized.	Practically impossible.
Need for performance upgrades:	Up to you.	Work with your vendor.	Hopefully, the ASP takes care of this so that it always runs fast.	Variable.
Signature and algorithm updates:	You have to make sure they work.	You should make sure they work.	Little, if any-thing, to worry about.	Difficult and out of your control.
Space in your data closet:	Depends on whether it runs on your e-mail server or a stand-alone server.	Very little.	None.	None.
Prevention of directory-harvesting attacks:	You may still be subject to this.	With the right architecture, this problem goes away.	Nothing to worry about.	Still a potential problem.
Your level of control:	You have abso-lute control. You can turn it off or remove it any time you wish.	You have a lot of control. You can turn it off, but you prob-ably cannot tinker with its its insides.	You have very little control. By-passing the ASP may take hours or or days.	Ha! Little or none.

Sizing for now and the future

In all matters of technology, you're wise to plan with not only today in mind, but also next year and the year after that. In this regard, you need to consider the following when pondering your potential anti-spam or anti-spyware solutions:

- Plan for not only the headcount growth of your organization, but also of e-mail volume in general. The volume of e-mail to and from the Internet is roughly proportional to the number of users, but the volume of e-mail *inside* the organization is more exponential. Are there any plans for expanding the role of e-mail to support business processes?
- Anti-spam applications will have to work harder to filter spam. Forklift upgrades (physically moving applications to a larger server, which you may need to bring in with a forklift, hence the name) are disruptive, so plan with extra capacity (for higher volumes of spam, as well as more complex and computation-intensive filtering algorithms) in mind, particularly if you are considering a software solution that will exist on your hardware. Think *easily upgradeable without having to replace the server.*
- Spam will likely get worse before it gets better (if it *ever* gets better). The techniques that spammers use will grow ever more sophisticated. They have a lot at stake and will continue to be creative and devious in order to reach as wide an audience as possible. The general rule is that whatever capacity you think you'll need in three years, double or triple it and buy enough hardware today to handle that future workload.
- The anti-spyware market is still an emerging market. You can expect the solution you buy in 2005, as I write this book, to be out of date in a year or two as certain solutions gain dominance and larger companies buy up smaller solutions and generally improve and consolidate the available options.

You have many other factors to consider when making a choice: If you're at or near that point, skip over to Chapters 5 and 6 for the low-down on choosing a solution.

Making the Solution Work

Stepping back a little bit, you can have a look at the factors that will determine both short-term and long-term success. In this section, I discuss the importance of planning, planning, and more planning. And, because blocking spam is a disruptive undertaking, you should seriously consider a trial prior

to pushing the solution out to the entire organization. (Although spyware blockers aren't as disruptive — you don't put them in between incoming e-mail and the end-user, like a spam filter — I suggest a trial for spyware blockers, too, in case you run into unknown interactions with some of the other software your business runs.) This section discusses other vital issues that you should be familiar with if success is important to you.

Creating a good plan

An IT project with little or no planning has little chance for success. Filtering spam is a disruptive and invasive change to make in an organization: A new and slightly unpredictable component is being placed right in the critical path of e-mail. Users' e-mail experience will grow more complicated, especially if they have quarantines. Managing a spam blocker requires constant attention to ensure that updates are flowing regularly and that users are continuing to update whitelists and marking false negatives (spam messages not marked as such) to train the spam filter.

On top of this, many different IT (and non-IT) people are needed to pull off such a project: system, network, firewall and e-mail administrators, the helpdesk staff, a project manager, and someone from the legal and human resources departments. You (or someone else) will need to figure out who needs to do what, how long each task will take, and the dependencies there are among tasks.

And that's the easy part. You'll have to make sure that all of these people will actually be *available* when you need them.

I go deep into planning in Chapters 5 and 8, and you'll find a sample project plan in Appendix A. If you need to get up to speed on project management, I recommend you get a copy of *Project Management For Dummies* by Stanley E. Portny and *Software Project Management Kit For Dummies* by Greg Mandanis (both published by Wiley).

Setting up a trial

In IT-speak, a *trial* is test run of new software, limited in some way (such as to a small number of users). Even though anti-spyware is practically invisible to end-users, an anti-spyware trial will help to shake out any installation or operational glitches that will be more difficult to solve after the solution is installed on everyone's workstations.

Something as intrusive as a spam filter needs to be carefully tested first, ideally with a small number of users. The principle reasons for this are

- **To verify that incoming e-mail still works.** Because a spam filter is directly on the critical path for inbound e-mail, you've got to know whether everything can be set up correctly so that e-mail from the Internet still reaches users' mailboxes.
- **To verify the appropriateness of the spam filter's settings.** You want to filter out all the spam, and only the spam, and allow all other messages through unscathed. Spam filters are less than 100 percent accurate, so it's important to test the spam filter in your environment to make sure it's filtering appropriately.
- **To verify capacity.** In a trial, you're only dealing with a fraction of the entire organization, but it's still important to gauge how much effort the filter takes to block spam. Then you might make some educated guesses as to whether the filter can take on the entire organization's inbound e-mail workload.
- **To verify operational procedures.** A trial is the time to get all the operational procedures such as updates, backups, restarts, and so on figured out while only a small number of users are affected.
- **To get install procedures right.** It's important to make sure that any software installs or configuration changes on user workstations are done properly so that installations are quick and trouble-free.
- **To find out how users learn and use the spam filter.** In order to train all the users in the organization, it's important to see how initial users' experiences go, so that any changes in teaching or training can be made.

Many technology implementations run into trouble because the right users weren't chosen for early testing. I can't stress enough the importance of choosing wisely. I recommend looking for test users who

- Are inquisitive and persistent. These are the people who will not balk at the first low hurdle, but will try to find their way around it.
- Are unafraid of change.
- Take responsibility and ownership of a project.
- Understand why the project is important.
- Are unafraid to offer constructive feedback, whether positive or negative. Correspondingly, you must be unafraid to receive constructive criticism.

- Have ample time to do the testing and communicate results and issues with you.
- Are articulate and able to explain the issues.
- Will help you "sell" the solution to co-workers.
- Have full appreciation for the importance of testing.
- Respect the need to refrain from "bitching and moaning" about any problems experienced in the test, but instead will be discrete with you because they understand that bad publicity isn't good for the project.

The intention of a trial is to test everything when the stakes are low, and to avoid unpleasant surprises after you've rolled it out to the entire organization. In Chapter 8, you can find more details about how to prepare for and conduct a trial for both spam filters and spyware blockers.

Training users

For something as vital as e-mail, users need to know how to operate their e-mail after you implement an anti-spam solution. You might consider putting your test users through the training first, just to make sure that the training is effective and makes sense.

You need to pull out all the stops and do whatever is needed: Schedule brown-bag sessions well in advance of implementation. Explain what you are doing and why, and what changes users can expect. Listen to their feedback, positive or negative. You need your users' backing if you are to succeed.

And as important (but similar to) training users, you need to keep them informed. Whether you're scheduling outages, changing configuration settings, or doing anything else that affects users, let them know what they need to know.

Similarly, you need to consider what — if any — training is required for users and their new anti-spyware program. If users will be required to periodically perform any tasks, then you need to train users to do those tasks. (Note that only some spyware blockers are fully automated, and there may be some reason for you not to choose one of those.)

I talk a lot more about training in Chapter 7.

Taking your solution live

After you have completed a successful trial and have trained users, you're almost ready to turn your malware filter on for the entire organization.

I say *almost,* because I don't want you using Chapter 1 as a shortcut. There are many details involved and many paths to failure if you aren't prepared. I describe as much detail as you need in Chapter 9.

Maintaining the system

Malware filters require some level of maintenance and observation. As important as malware blocking is, you've got to make sure it's working properly and do your chores. The major tasks include

- **Managing quarantines.** These are the directories that contain e-mail messages that the spam filter tagged as spam. Here you must make sure that there is sufficient disk space. At first, this will be a tuning issue, as you figure out how many days' worth of spam can be stored in the quarantine for the entire organization.
- **Manage whitelists.** A *whitelist* is the list of e-mail addresses that the spam filter will let through, no matter what. This is the company's way of making sure that e-mail from known senders won't accidentally get caught in the spam filter.
- **Manage filter rules.** Depending upon which spam- or spyware-filtering product you're using, it may be necessary to add, tweak, or remove specific rules, particularly if your organization's e-mail correspondence regularly contains keywords (such as "Viagra," if you work for a pharmaceutical company) that your filter would otherwise block. However, as products improve, this will become less and less of an issue.
- **Manage updates.** In order to be effective, the filter must download new filter rules periodically, as often as several times a day. Here, you have to make sure that these updates are working properly. In addition to rules updates, the filter software itself gets periodically updated, so you've got to be sure these updates are working too.

In order to keep your users happy, someone has to pay attention to these issues. I provide significantly more detail on maintenance in Chapter 11.