Chapter 1

How Spam Works — and Drives You Crazy!

· ••

In This Chapter

▶ How it came to be called spam

▶ The economics of the spam business

▶ Why spam is so hard to stop

▶ An overview of spam-fighting tactics

· ••

*Q*uick! It's word-association time! When you hear the word *spam,* which one do you think of:

    a. A salty, pink lunch meat that comes in a blue can?

    b. A goofy British comedy troupe's skit with singing Viking warriors?

    c. Annoying junk mail and other advertisements you never asked for that are sent to you via the Internet?

    d. All of the above.

The best answer is

    d. All of the above.

As most people know, *SPAM* (with all capital letters) is a salty, pink lunch meat that is made by Hormel and comes in a blue can.

Hormel, the makers of SPAM (the lunch meat), say that if you want to call junk e-mail by the same name, they don't object. You just can't use all capital letters, like they appear on the

can. *SPAM* is lunch meat, and *spam* is junk e-mail. Got it? We're talking about *spam* written with lowercase letters (at the request of Hormel) so that people don't confuse the spam we all hate for the SPAM that some people find tasty.

Spam, Spam, Spam, Spam, Spam, Spam, Spam, Spam

Avid fans of the British comedy team Monty Python may remember the skit where a husband and wife enter a restaurant in a seaside resort town only to find that every dish on the menu features SPAM. Unfortunately, the wife is not at all fond of SPAM and searches in vain for dishes that don't have any of the noxious substance. With SPAM appearing everywhere she turns, her frustration grows.

We're not sure why, but the skit also features a large band of Viking warriors lunching at the dinette who, every time the wife says the meat's name aloud, regularly break into a deafening song about "SPAM, SPAM, SPAM, Lovely SPAM! Wonderful SPAM!" — adding to her confusion and anger. (For true fans of Monty Python, however, singing Vikings at a seaside dinette are par for the course.)

Everyone who uses the Internet has encountered loads and loads of junk advertisements that appear when you least expect them and usually where they're least wanted — namely, in your e-mail inbox and on the message boards and newsgroups you frequent.

Legend has it that someone casting his eye over a menu of newsgroup discussion topics kept seeing the same ads posted in nearly every conversation thread. The continual appearance of these ads in every discussion group reminded this person of Monty Python's seaside café with SPAM appearing in every menu item and conversation being drowned out by the ceaseless monotony of Viking-like advertisers.

In the Monty Python sketch, the distraught SPAM-hating wife finally snaps and screams "I don't like SPAM!!!" If you're like us,

you have spent enough time sorting through the junk e-mail in your inbox that you too have found yourself screaming about spam.

Why Spam Works

Anyone who has ever sent an e-mail message knows that it's a quick, simple, and cheap process. After you have a computer and an Internet connection, your investment is finished. To send an e-mail, you don't have to worry about buying envelopes or stamps. You just have to have an e-mail address for somebody, and something to say.

This same economic reality is what spammers depend on. Sending e-mail in bulk costs the sender a tiny fraction of the cost of sending postal mail or making telemarketing phone calls. One person can generate huge volumes of mail with just a few clicks of a mouse, blanketing millions of inboxes in a matter of minutes or hours.

The economics of spam

The economics of e-mail turn all the traditional notions of advertising on their heads. No other advertising medium costs the recipient more than it costs the sender of the ad.

With television, print ads in newspapers, or advertisements via the U.S. Postal Service, the sender has to spend a bundle on printing or other preparation of the ad, delivery, and so forth. The high cost naturally forces advertisers to be a bit picky about how much advertising they send out, and to whom they send it, because each additional ad bears an incremental cost.

In the world of junk e-mail marketing, it costs no more to send the first e-mail than it does to send the ten millionth e-mail. No economic restriction keeps marketers from blasting their advertisements as widely and indiscriminately as possible. They don't even have an incentive to remove duplicate addresses from mailing lists. Why not? When advertisers pay nothing more for each additional message, any time spent on editing a mailing list is time wasted.

Why spam is a bigger problem than you think

We all get postal junk mail. That's an accepted fact of life, at least in the United States. You may wonder why spam is any different.

Spam is different from the junk mail that is mailed to your house or the telemarketing calls that interrupt your dinner, for one simple reason: The people who send you that junk mail and make those phone calls have to pay for the cost of doing so, and the price can be steep. Junk mail has to be written, designed, printed, and collated, and postage must be paid. Telemarketers must rent office space, hire staff members, install phones, and pay long-distance phone charges. We don't say this to defend them, but rather to draw a distinction between the costs that traditional marketers incur and the costs that a spammer *doesn't* incur.

When a spammer sends an ad for herbal Viagra or an XXX-rated Web site or canine harmonica lessons to millions of people over the Internet, she pays almost nothing because, as we all know, e-mail is virtually free to the party who is sending it. But someone has to bear the cost of distributing those millions of e-mails to recipients all over the globe — and therein lies the difference between online unsolicited advertising and offline unsolicited advertising.

There's no such thing as a free lunch, particularly on the Internet

If you're like most people, you pay an Internet service provider (ISP) to get access to the Internet. (Even if your company or school pays for your access, someone is paying for it.) E-mail is one of the services your ISP provides as part of its service to you. For most people, the costs of your e-mail service are simply bundled into your service package. In reality, these costs can form a significant part of your monthly bill (as much as $3 or $4 of a standard $19.95 charge).

It wasn't long ago that ISPs charged per message for Internet e-mail. In the early days (well, 1991, which was pretty early for lots of Internet users), the service provider Prodigy used to charge 25 cents per message!

Even now, users of "free" e-mail services, like Hotmail and Yahoo! Mail, "pay" by being subjected to advertisements all over their mailboxes, and the advertisers pay to run the servers at those sites. What seems to be free is really just costs factored into your service, and the costs related to e-mail don't stop there.

Suppose that you have a friend in Timbuktu whom you love to hear from by e-mail. The data that makes up the e-mail from your friend leaves her computer and begins a wondrous journey though any number of computers and networks on its way to you. Presumably, your friend owns her computer, so the resources used to create the message are largely hers. After that e-mail leaves her computer, though, the entire rest of its journey is spent bouncing around servers and careening down transmission lines that belong to anybody *other than* her — unless, of course, she happens to personally own her own international fiber-optic network!

Considering that most of us don't have a spare data network lying around, when that e-mail is sent, you and your friend are both depending on every service provider and communications network between you and Timbuktu to let that e-mail pass through their networks. In this way, virtually every e-mail is, to one extent or another, sent "postage due," with the postage being paid by everybody along the way.

Spam is a bad deal for everybody (except the spammer)

If you think about it, sending bulk e-mail to millions of people is just as cheap for a spammer as it is for a faraway friend in Timbuktu, especially when it's compared to the cost of sending junk ads by postal mail or telemarketing. After all, a spammer has no printing costs, no stamps to buy, no phones to install, no telemarketers to hire, and no long-distance calls to pay for. Instead, a spammer sends hundreds or thousands of messages per hour for just a fraction of a penny per spam.

Just because a spammer doesn't pay much for sending his spam, though, doesn't mean that someone isn't paying — and you would never guess who's at the head of the list: you.

Just like a friend you may have in Timbuktu, when a spammer decides to send the latest get-rich-quick scheme to 25 million of his closest friends, he can get an account at a local ISP and begin sending mail. After those 25 million messages leave his computer, though, the vast majority of the "postage" for delivering his mail is paid for by the 25 million recipients, their ISPs, and all the other networks, servers, and ISPs in between.

The crushing volumes of spam cost Internet service providers (ISPs) huge amounts of money for all the servers and Internet connection capacity needed to receive, process, store, and deliver unwanted e-mail. Several major ISPs estimated that by the end of 2003, spam would comprise upward of 80 percent of their entire e-mail volume. Imagine if you had to have an 80 percent larger house because your in-laws kept coming to stay. That's a lot of money, not to mention the pain and suffering!

How big of a problem is spam? A study commissioned by the European parliament in 2001 discovered that spam costs about $9.4 billion each year — a huge bill that is being footed by everyone except the spammers themselves. And much more spam is flowing this year than in 2001.

Who Hath Spammed Thee? (The Spammer Food Chain)

To understand the problem of spam, it helps to know who is doing it and what they're advertising. Surveying the Internet, you can quickly see that almost no reputable marketers use spam to advertise goods and services. That doesn't mean that reputable companies don't sometimes send out e-mail that the recipients don't want or didn't expect. But few legitimate companies engage in the kinds of complex spamming campaigns that are responsible for most of what is filling your inbox.

To the contrary, the most commonly mailed spams advertise pyramid schemes, get-rich-quick and make-money-fast scams,

phone-sex lines, pornographic Web sites, and quack medical products. Most ironically, vast quantities of spam advertise spamming software, spamming services, and lists of millions of e-mail addresses you can buy so that you too can become a spammer. We have even seen spam advertising antispam filters!

When we talk about *spammers*, we're really talking about at least three categories of people who may be responsible for putting a particular piece of spam in your inbox:

- ✔ Advertisers
- ✔ Spam service providers
- ✔ Spam support services

The first category is the advertiser. You can't have spam without somebody who wants to advertise something. They may be sophisticated technical experts who do their own spamming, or they may be computer illiterates who saw an advertisement and decided to hire a third party to send spam for them. Whoever they may be, they are generally the people responsible for whatever message is contained in the body of the spam, and generally the one to whom you make out the check when it's time to buy the miracle hair-growth and body-part enlargement product.

*Spam service provider*s are people who have built up the hardware, software, and expertise needed to pump out a bazillion spam e-mails. According to many antispam experts, the great majority of the spam you receive comes from a relative handful of professional spam service providers. They advertise their services to the latest sucker — er, "distributor" — of the latest get-rich-quick scheme and charge them a few hundred bucks to send a few million spams. Even though the distributor may never make a penny from the spamming campaign, the spam service provider has made his money, and that's all he cares about.

Spam support services can include ISPs and Web site hosting services that take any customer, no matter what kind of criminal or fraudulent activity they're engaged in. These ISPs are often in areas of the world where the laws may be either different or nonexistent. China, Russia, Brazil, Argentina, and South Korea are among the leading countries where spam service providers have found ISPs willing to provide support services, just as long as the checks keep clearing.

The first spammers

Back in 1994, the U.S. government decided to hold a lottery to give away some permanent resident visas to immigrants seeking to stay in the United States indefinitely. The lottery program gave away several thousand permanent residency visas, still called *green cards* (even though they haven't been green for many decades), to anyone who sent a postcard to a particular address before the deadline date.

Several months before the deadline, on the evening of April 12, 1994, Laurence Canter and Martha Siegel, a husband-and-wife lawyer team, decided to join the lottery frenzy by pitching their own overpriced "lottery services" to immigrant communities. But these two were not your run-of-the-mill hucksters. They were innovators with a penchant for technology. Canter and Siegel chose Usenet newsgroups, and later e-mail, as their advertising vehicles. Neither medium would ever be the same.

Within hours, the Internet service provider used by Canter and Siegel had shut off their access. But the genie was out of the bottle. The era of spam had begun. Within weeks, Canter and Siegel had branched out from newsgroups to e-mail, and in a matter of a few months they had penned the book *How to Make a Fortune on the Information Superhighway,* which detailed their spamming strategies.

Your humble co-author, Ray, had the unfortunate experience of being on the receiving end of many complaints when Canter and Siegel first burst onto the spamming scene in 1994, so the spamming duo holds a special spot in Ray's heart. At the time, he was working for the American Immigration Lawyers Association and was responsible for fielding complaints from angry spam victims who wanted to see the pair disbarred. Not surprisingly, they had already been disbarred once in the state of Florida, and would eventually lose their law licenses from other states as a result of their dishonest spam campaigns.

You can still pick up a (used) copy of their book on Amazon.com, but it's more of a historical footnote than a useful how-to guide. Indeed, you can draw a much more informative lesson from looking at where these morally bankrupt business ideas landed the pair: disbarred, dead at an early age (in the case of Ms. Siegel), and writing software manuals (in the case of Mr. Canter).

Canter and Siegel were trailblazers in another sense too: Their past legal problems seem to be a harbinger of success in the spamming business. Many of the most notorious spammers now have criminal records and convictions for fraud and drug offenses and have even spent time in jail.

The Father of the Internet speaks out about spam

"Spamming is the scourge of electronic-mail and newsgroups on the Internet. It can seriously interfere with the operation of public services, to say nothing of the effect it may have on any individual's e-mail mail system. Spammers are, in effect, taking resources away from users and service suppliers without compensation and without authorization."

— Vint Cerf, acknowledged "Father of the Internet"

Why "Just Hit the Delete Key!" Is No Answer

Although spammers love to say "Just hit the Delete key," it totally misses the point. By the time the spam hits the fan (well, when it hits all our mailboxes), so many costs have been incurred by so many people other than the spammer that it is either naïve or an utter act of denial to pretend that those costs can be undone with the pressing of one key.

Spam is about the numbers, so let's look at some numbers that show why hitting the Delete key isn't really a workable solution. The U.S. Small Business Administration estimates that the United States has approximately 25 million businesses. If only 1 percent of those 25 million decides to send you just one single unsolicited e-mail per year, you average 685 spams *per day* in your inbox. If it takes an average of 10 seconds per message to open a message, determine that it is spam, and hit Delete, you spend two hours per day disposing of e-mail you never asked to receive.

More Ways You Pay for Spam

For your Internet service provider (ISP), the costs associated with processing incoming e-mail are the same, whether or not it's e-mail that its customers want. The more e-mail your ISP processes, the higher those costs. As spam volumes increase,

it begins to clog Internet bandwidth and begins to fill up the storage disks on your ISP's servers. Whenever you're trying to surf the Web, therefore, you're competing with spam for the use of your ISP's Internet connection, slowing you down when you're surfing.

With overworked servers receiving and storing spam for hundreds of thousands of users, your access to your own e-mail can also slow down. E-mail servers are powerful machines, capable of doing thousands of tasks per second, but even those big machines can get bogged down. And when you're eager to read your e-mail, the last thing you want is to have to compete with some spammer for access to your ISP's mail servers.

Every once in a while, an ISP gets so overloaded with spam that its servers crash. This situation causes everybody who was depending on that server to be inconvenienced. It may also be more than an inconvenience if, for example, your company's e-commerce Web site was on that same server or a bunch of customers' orders were in the e-mails that got scrambled when the server gave up the ghost. Calculating the cost in terms of lost business opportunities when customers can't reach you or think that you're ignoring them is almost impossible, but those are more costs you bear, thanks to spammers.

Eventually, if the service quality gets too bad, to keep subscribers from jumping to a competitor, an ISP begins buying more Internet bandwidth and more servers. Of course, it needs to be hiring more staff members to install that equipment and to keep everything running. At some point, those costs get passed back to you — perhaps in the form of rate hikes or longer hold times when you call your ISP for customer service. While he was working on this book, co-author John, who provides mail service for a few dozen friends and web-hosting users on his tiny network, had to spend about $1,000 upgrading the mail server, just to deal with the increase in spam.

The number of unsolicited messages sent out each day is truly remarkable. The spam-filtering company Brightmail claims that its research has shown more than 25 million unsolicited messages being sent per day in 1998. By 2002, AOL and Hotmail both claimed that they were blocking nearly a billion pieces of spam each day, and still more was slipping through. According to a September 2003 survey by *InformationWeek*, spam volumes

were growing at 37 percent per month, for an annual growth rate of more than 400 percent!

Numerous court cases are under way between spammers and innocent victims who have been subjected to these types of floods. Unfortunately, although major corporations can afford to fight these cutting-edge cyberlaw battles, small mom-and-pop ISPs and their customers are left to suffer the floods.

WARNING!

Here's another cost you may not have thought of: your time. Because of the volume of spam zipping around the Internet, downloading your e-mail takes longer. Although you may call a local number to connect with the Internet, lots of other people pay by the minute for the time they spend online. Because of spam, it takes them longer to get their e-mail, and spam costs them money in connection charges every month.

Calling Erin Brockovich!

If you saw the movie *Erin Brockovich* (which was based on a true story), you know that the sassy heroine does battle with a polluting power company that has dumped nasty gunk into the groundwater, which is causing the citizens in a nearby town to become quite sick. Oddly enough, noxious floods of spam have a similar effect on the health of the Internet and all the netizens who use it.

The reason that companies dump toxic waste into lakes and rivers is that they have done the math. It may cost them many millions of dollars per year to properly dispose of the waste from one plant. Or, they can just dump it into the river for free.

Economists call the toxic waste an *externality,* which is their word for something that gets generated as a by-product of someone's moneymaking activity, the cost of which gets "paid for" by all the citizens who then have a greater risk of disease.

If the pollution levels stay relatively low, some people may never notice that they're slowly being poisoned and they may eventually die of something else. Occasionally, though, somebody does get sick, and for them, the cost of that pollution suddenly becomes great. As in the movie, companies gamble that the amount they may have to pay for an occasional illness

is less than the amount that they would have had to pay to dispose of the waste properly.

Just like polluters, spammers try to spread the costs of their spam across wider and wider populations of Internet users, knowing that as long as they don't give a "fatal" dose to any single Internet service provider (ISP), they can continue their spamming relatively unnoticed and everyone pays their little portion, never being the wiser or bothering to fight back.

Why Spam Is Hard to Stop

If you have ever spent an hour trying to coax, cajole, and threaten your computer into doing something it stubbornly refused to do, the following statement may come as a surprise: Simplicity is at the core of how the Internet works, especially when it comes to something as ubiquitous as e-mail. Part of what made it become so widely used is that it was easy for Internet service providers to implement and simple for software developers to program tools to use it.

At the heart of e-mail is a set of technical standards and Internet protocols that are so simple, they're called the Simple Mail Transport Protocol, or SMTP. You may have even seen the letters *SMTP* when you set up your e-mail software — it's the technology by which e-mail gets sent from a sending e-mail server at an Internet service provider (ISP) to a receiving e-mail server at another ISP. (Other protocols help you retrieve mail after it has been received at your ISP. Two of them, POP and IMAP, are in the spam-filtering chapters in Part II.)

As the popularity of the Internet grew, e-mail evolved from a novelty to a necessity. All e-mail now transmitted across the Internet is sent using the agreed-on industry standard, SMTP. Any server that "speaks" SMTP can send mail to, and receive mail from, any other server that speaks SMTP.

Because a server may be processing a dozen or more message connections per second, the SMTP "conversation" must be kept very brief. How brief? Well, before the entire e-mail message gets dumped onto a receiving server, only three pieces of information are received before the mail is delivered: the identity of the sending server, the From address, and the To address.

A Nobel prize in spam?

No, there isn't really a Nobel prize for spam. But a famous economist named Ronald Coase won a Nobel prize for writing, among other things, about why sometimes governments must step in when the marketplace is broken. Specifically, Coase discussed the dangers to the free market when an inefficient business — one that cannot bear the costs of its own activities — distributes its costs across a large population of victims.

The classic example is pollution: It's much cheaper for a chemical manufacturer to dump toxic waste into the local river than to treat it and dispose of it in a more environmentally sensitive manner. By creating such externalities, as economists call them, a polluter can maximize its own profit, even if it comes at another's — or everyone's — expense. Certainly those who are harmed by poisons in a river may be able to sue, but for the vast majority of victims, the cost of hiring a lawyer, assembling evidence, hiring experts, and bearing all the other costs and complexities means that most victims can never hold the polluter accountable for the harm it has done.

Much is the same when it comes to spam. Although some companies have successfully sued junk e-mailers for the damage they have caused, few ISPs can afford to fight these kinds of cutting-edge cyberlaw battles. As a result, the economics favor the abusers and disfavor the spam victims. Indeed, spammers are counting on the incremental cost of each spam, foisted on each individual member of the public at large, being ignored.

As Coase pointed out, this situation is a prescription for economic disaster. When inefficiencies are allowed to continue, the free market no longer functions properly. The "invisible hands" that would normally balance the market and keep it efficient cannot function when the market is carrying the dead weight of spammers. Unchecked, businesses that depend on stealing time, money, and resources from unwilling recipients must be stopped, or else they will continue to leech the life out of our economic system.

The price of speed: Accuracy

SMTP is fast and simple — so simple that it has no mechanism for verifying the validity of either the identity of the sending server or the accuracy of the From address. The SMTP server has no way to verify assertions such as "This message is from

your bank and concerns your account" or "This message contains the tracking number for your online order" or "Here is that newsletter about investment tips that you paid $29 per month to receive."

So why not replace SMTP with something better?

Well, Winston Churchill once said that democracy is the worst way of doing government, except for all the others. SMTP is, as Churchill may have said, the worst way of "doing" e-mail, except for all the others that have been tried. The reality is that SMTP works reliably and has been pretty much universally implemented.

To swap out SMTP for something "better" would be much like telling American automobile drivers that, starting next Thursday, we all have to start driving on the left side of the road. Not only would lots of people be completely confused, but lots of the fundamental infrastructure would need to be redesigned. And lots of people simply wouldn't be able to get stuff done for a very long time.

In short, the need for speed creates a system that has virtually no technical consequences for being a liar. That is precisely why spammers have been, and continue to be, incredibly effective in delivering unwanted e-mail. So, until somebody thinks up a better way of doing e-mail, as well as a way to implement it without bringing everything to a screeching halt, we're stuck with this simple way of doing e-mail that is also quite vulnerable to abuse.

Whitelists, blacklists, filters

Some ISPs do try to take steps to deal with spam during the e-mail delivery process. Three popular approaches are shown in this list:

- ✔ *Whitelists* are lists of servers known to be sending good, legitimate, nonspam e-mails. During the SMTP conversation, the address of the sending server can be compared to a whitelist and, if it's on the list, the mail gets delivered.

- ✔ *Blacklists*, also called *blocklists*, work just the opposite of whitelists. Blacklists are lists of servers that are known to be operated by spammers or that have been used to send

spam in the past. When a sending server attempts to connect to the receiving server, the sender's address is compared to the blacklist, and if it's there, the mail is rejected.

✔ *Filters* allow programs to look at e-mail messages and guess whether they are spam. After an e-mail message has been delivered, the filter compares it against a list of words, phrases, or other kinds of identifiers that can be used to determine whether the message is legitimate or spam. New filtering techniques, including something called Bayesian filtering technology, make filtering much more accurate than it used to be. (Look on a nearby page for the sidebar "Bayesian what?" for more information on this new filtering approach.)

Unfortunately, although whitelists, blacklists, and filters can catch lots of spam, they are not without their downsides. The kinds of powerful e-mail servers that ISPs run can send and receive hundreds or thousands of e-mails per second. But when the server has to stop and compare each message to a list, or run the message contents through a filter, that processing speed can slow to a crawl.

The maintenance of whitelists and blacklists can also be quite time consuming, and can often produce errors. For example, it may be necessary to call up somebody on a telephone to verify the identity of a sender before an ISP will add a server's address to a whitelist. Similarly, a server that may send legitimate e-mail may also send spam occasionally, and may require additional investigation before it can reliably be added to a blacklist. Even then, no guarantee exists that a whitelisted server won't start spamming tomorrow and that blacklisting a server won't result in losing legitimate e-mail.

Can You Really Fight Back Against Spam? Yes!

Before we go any further, we should apologize if this chapter is depressing. Spam is a difficult problem that causes tremendous frustration for many people, including you — otherwise, we suspect that you would be reading another, more exciting, title in the fine *For Dummies* book series.

TECHNICAL STUFF

Bayesian what?

The current cutting edge in spam-filtering technology is a category of e-mail filters built around something called *Bayesian analysis*. Named after the British-born church minister and part-time mathematician Thomas Bayes (1702-1761), the Bayesian approach is based on a theory of statistical analysis described in an essay that Bayes wrote, but that wasn't published until 1764, three years after his death.

Bayes' idea was that you could determine the probability of an event by looking at lots of similar circumstances and working out the frequency with which previous judgments about the occurrence had been accurate or inaccurate. In other words, Bayes said that a mathematical equation can be created that would not only tell you how probable a particular event is, but also automatically fine-tune the equation so that the next prediction would be a little more accurate.

If you think that this idea sounds like a mathematical theory that would allow,

for example, a computer to learn by itself automatically, you have grasped the awesome power of Bayesian analysis!

When applied to spam, *Bayesian filters* start by looking at a whole bunch of e-mails, which it asks the user to identify as good mail or bad. It then figures out on its own which characteristics are common to the good mail and which characteristics are common to the bad mail. Each new e-mail message that passes through your system is then compared against that base of knowledge, and a probability rating is assigned to it. It then reworks its calculations after looking at all the good and bad e-mail it has processed and continues over time to learn and refine its analysis methods.

As a concept, Bayesian analysis has been proving effective at identifying spam, and therefore is a frequent feature in many new antispam technologies, some of which we describe in greater detail in Part III of this book.

The purpose of this chapter isn't to make you run away screaming from all Internet technology. Rather, its purpose is to make sure that you understand that fighting spam is an ongoing and sometimes complicated project.

If somebody out there could invent a magic wand to wave over an Internet e-mail server and make spam go away, somebody would have done it long ago. No, spam has no quick solutions.

Thanks to lots of hard work by lots of clever people, though, you can indeed do many things to help make your inbox a cleaner and friendlier place. You can use a growing number of tools and technologies that, with some work, lots of patience, and a little luck, can make your e-mail experience much more pleasant.

Many technologies discussed in Parts II and III of this book fall into the three categories of whitelists, blacklists, and filters. For example, certain antispam services depend on turning your e-mail address book into a kind of whitelist, ensuring that you always get e-mail from those people you know. Others implement sophisticated filtering techniques, and still others use known sources of spam to create blacklists that block unwanted e-mail.

None of the technologies we discuss would qualify as a "silver bullet" to stop all spam forever, but they can definitely make a dent in the amount of spam you receive. All it takes is a strong distaste for spam and a willingness to give these new technologies a chance.