[**Editor's Note:** The following excerpt is from Chapter 3 of the free eBook *The Definitive Guide to Email Management and Security* (Realtimepublishers.com) written by Kevin Beaver and available at http://www.singlefin.com/ebook/.]

What's the Big Deal about Spam?

In a nutshell, spam costs organizations time, money, and overall end user productivity. In addition, if spam isn't dealt with properly, your end users may lose confidence in the usefulness of email. Although there is no simple fix for the spam problems we're having, spam cannot be ignored.

Scary Spam Statistics

Before we delve too far into this chapter, the following list highlights some of my favorite spam statistics that I think will get your attention:

- Spam comprises 55.1 percent of all emails (Source: MessageLabs' May 2003 Monthly Email Security Report)
- Microsoft claims that spam accounts for 80 percent of all Hotmail messages
- 90 percent of all spam received by Internet users in North America and Europe is sent by less than 200 spam outfits (Source: Spamhaus Project)

✎ To see a list and detailed information about these spam outfits, check out the ROKSO list at http://www.spamhaus.org/rokso.

- According to a study performed by the Federal Trade Commission, two-thirds of spam contains false claims, 96 percent of spam offering business and investment opportunities contain false claims, and 48 percent of spam promoting health services or products contains false information.
- One day in early 2003, AOL blocked 1 billion spam messages; its previous high was 780 million blocked spam messages in one day (Source: Direct Newsline)
- 4.9 trillion spam messages are projected to be sent in 2003 (Source: Radacati Group)

Example Estimated Cost of Spam

These statistics justify the war on spam. However, let's look at a real-world example of what spam could actually cost an individual organization. Say the average corporate user receives 50 emails per day (both legitimate emails and spam) Monday thru Friday and another 50 emails over each weekend for a total of 300 emails per week or 15,600 per year. These numbers are fairly conservative, and your spam numbers may vary. (Some reports state that as much as 70 percent or more of email is spam, but I've seen numbers as low as 30 percent.) Let's take a good even number of 50 percent for this example. Given that on average, half of all email is spam, we have a total of 7800 spam messages a year for the average user!

Next, consider how long each user takes to tend to individual spam messages—let's say a very conservative 2 seconds to handle each one; thus, the user consumes 4.33 hours per year dealing with spam! If you conservatively estimate that the average user costs the organization $40 per hour with salary and benefits, the company is losing $173.33 per user per year (for the average user).

This amount might seem fairly harmless for smaller organizations that have 10 or so employees, but when you start thinking about organizations that have 100, 1000, or 10,000+ employees, spam costs become a serious problem over time. These numbers add up to $173,333.33 in 1 year for a 1000-employee organization.

> Looking for a spam cost calculator? There are several on the Internet. Singlefin offers just such a calculator at http://www.singlefin.net/services/calculator_result.php.

Taking this estimate a step further, let's look at the computer hardware that's required to support these kinds of numbers. Let's assume that, based on my non-scientific research, the average spam message is around 5KB in size. Based on the average user receiving 7800 spam messages a year, spam adds up to 38MB of clutter making its way to your email server or the end user's local hard drive every year. Again, 38MB doesn't seem so bad for one or even 10 users, but scale it up to 1000 or more and these organizations now have a serious storage issue on their hands—38GB of storage space for a 1000-user network over 1 year! There's also the issue of backup media space that's required and overall network bandwidth that's being wasted.

Additional Spam Costs

Although frightening, none of these estimates take into consideration the amount of time and money IT personnel have to spend on:

- Workstation-related problems
- Spam filtering software maintenance
- Increased data management responsibilities
- Email servers running out of storage space
- Email servers having to be rebuilt after a crash
- Purchasing and upgrading workstation and/or server hardware
- Data backups having to be restored

Network administrators have to purchase spam filtering products and more storage space and possibly network bandwidth to handle all the spam. End users end up paying more for larger mailboxes for their Web-based accounts or risk losing legitimate emails. Traveling users dialing up the Internet to check email have to pay more for longer connection times because of increased spam download times. Finally, people are paying more in wireless connection charges for spam they receive via email on mobile devices such as PDAs, cell phones, and so on.

There are dozens of related issues that help justify fighting the spam problem in your organization. The point is that even with conservative estimates, the cost of spam adds up quickly! Ridding yourself of this problem will result in saved money, productivity, sweat equity, computer hardware, and network bandwidth.

Unintended Side Effects

Anti-spam solutions can actually make email less reliable than it was before. Legitimate emails that are unintentionally blocked can cost organizations money in lost business and intangibles such as reputation and customer loyalty. This unintended side effect of some anti-spam solutions is a critical issue that must be considered when selecting, implementing, and managing anti-spam technologies.

> 📖 I'll discuss the pros and cons of the various spam-filtering methods along with some tips about how you can prevent false positives later in this chapter.

Security Implications of Spam

There are obviously financial, productivity, storage space, and bandwidth losses stemming from spam. However, an often overlooked area when it comes to managing spam is that of information security. Recently, spam seems to be becoming more aggressive with messages that actually try to glean private and confidential information from our networks and computers—a far cry from the typical nuisance spam we're used to. Like in the malware world, spammers are constantly trying to find ways around existing controls.

Another security concern of spam is that of unwanted spam messages eating up a tremendous amount of storage space. Given enough time and with enough messages coming into a network, the overload can create a DoS condition leading to serious email system downtime. The obvious consequence being email system unavailability on the server and/or client, which can lead to messages not being properly sent or received—and ultimately lost business.

Other spam attacks could be considered network intrusions, especially if they come in with malware attached. Everything from viruses to Trojan horses to Web bugs can wreak havoc on networks, server, and end user systems. In many organizations, any sort of confidential information leakage is intolerable. Perhaps a broader issue related to spam attacks is one of IT and security resource utilization. When IT and security personnel must address spam attacks, they are diverted from other, more important, tasks, which can lead to even more security issues cropping up.

Some spam is actually social engineering at work. Social engineering attacks are notorious for being very malicious yet easily carried out. We can train our end users to not open emails or attachments from people they don't know, but this training can only go so far. After so much inundation with spam, users tend to end up letting their guard down allowing intrusive messages and malware take its toll.

What's in it for Spammers?

So why do spammers send spam? First and foremost, there are high potential payoffs in return for very little effort on the spammer's part. But you'd think that with the huge majority of people not responding to spam that the spammers would eventually figure out that their way of doing business is not very well received. Given the large numbers of spam messages being sent out, it only takes a very small percentage of spam recipients to reply to and purchase some spam-based offering for the spammers to succeed.

✎ Lawrence Canter and Martha Siegel are two of the original, and perhaps most notorious, spammers on the Internet. These immigration attorneys earned their 15 minutes of fame by posting green card lottery ads on thousands of Usenet groups in 1993. These ads put the Usenet world in an uproar, and the ads were later deleted by a *cancelbot*—an automated message erasing script.

Based on my research, the typical percentage of actual responders and ultimately buyers of spam products is almost always less than 10 percent and is usually much smaller. Even if the rate is only one-tenth of one percent (0.001), if the spammer has sent out a million messages and only get $2 per sale, that's still $20,000 in sales! Until the profits are diminished with the help of increased spam filtering, email-savvy users, and so on, the incentive will remain in place and spammers will continue to send spam.

Spam Laws

Currently, there are no federal laws in the United States that specifically address spam. Selling spam software or mailing lists is not illegal either. There has been legislation under consideration in the United States for years that would require commercial emailers to identify themselves to their email recipients and offer an easy way for recipients to opt-out of unwanted messages. There have been laws proposed that would establish a nationwide "do not spam" list similar to the new national "do not call" list. However, many countries, including the European Union, have already addressed the spam issue and are doing something about it.

Commercial faxes were outlawed in 1991 via the Telephone Consumer Protection Act because of the time and money losses inflicted upon recipients. Meanwhile, the spam problem keeps getting worse. The spam lobby's argument is often that it's their First Amendment right to send spam and that it's not hurting anyone. They say that consumers around the United States could be deprived of a certain product or service that they wouldn't have otherwise known about if spam isn't legal. There are spammers and lobby organizations that have been toying with the definition of spam using semantics and other justifications to say that spam really isn't spam.

📖 For an interesting insight into of the politics of spammers, check out the Spamhaus Project article "Spam Definition and Legalization Game" at http://www.spamhaus.org/newsdog.lasso?article=116.

Regardless of whether you agree that spam is free speech, it costs people and organizations time and money just like the junk faxes used to (and still do). ISPs, network administrators, and end users all suffer. ISPs have to hire technical experts to deal with spam, and, of course, these expenses are passed on the customer.

✎ ISPs are one of the biggest victims—and thus opponents—of spam.

Have you received any of the spam messages advertising great deals on antivirus software? I get a few every day. Some of these gray market outfits may be legitimate and some may not. Either way, indications show that, thanks in part to these spammers, we're headed more toward digital rights management (DRM) technologies from the vendors so that they can better protect their assets. An unfortunate side effect—and one that many of us never consider as resulting from spam—is most likely even more software registration and maintenance headaches than we're currently experiencing.

Although there are laws against fraud and other trade violations, if you order from spammers, you have no guarantee that you'll get your goods or that those goods are not counterfeit.

Conventional methods used to fight spam have not been working effectively. There are current solutions to thwart off spam, however, the global problem still exists and will for a long time to come. Right now, when spammers get caught, the most serious method of discipline that appears to occur is the cancellation of their ISP or co-location account. Solutions range from new technology, industry self-regulation, and legislation. Before the various states enacted spam laws, many lawyers and prosecutors used existing trespassing and forgery laws to fight spammers.

[**Editor's Note:** This content was excerpted from the free eBook *The Definitive Guide to Email Management and Security* (Realtimepublishers.com) written by Kevin Beaver and available at http://www.singlefin.com/ebook/.]