

5

Managing Spam

Most people consider spam to be any unsolicited e-mail that they might receive that attempts to sell them something¹. It can also include e-mails with chain letters, political statements, or messages from people who just need some attention. Although some people might think that the e-mail version of spam was named after the food SPAM,² because both are considered tasteless and a waste of time (at least to some people), nothing could be further from the truth. (As an aside, SPAM is served during breakfast at McDonald's in Hawaii, where it has the highest consumption rate per capita in the United States.²)

The origin of the use of the term *spam* for unsolicited e-mail appears to come from the Monty Python skit about SPAM³. The Vikings in the skit annoyed a waitress by repeating the word *spam* over and over again. In much the same way, unsolicited e-mail can elicit the feeling of annoyance in people who receive it. The way in which the Monty Python skit was connected to the act of unsolicited communication came from the Multi-User Dungeon (MUD)⁴ community. One member of that community, after becoming upset with his treatment by some of the other members, created a macro to repeat the word *spam* several times in the MUD environment during a sacred hatching. Later on, MUD members would refer to the event as the time they got “spammed.”

1. What is spam? Visit <http://spam.abuse.net/overview/whatisspam.shtml> and <http://www.templetons.com/brad/spamterm.html> for their answers.

2. <http://www.bizjournals.com/pacific/stories/2002/06/10/daily22.html>

3. <http://www.ironworks.com/comedy/python/spam.htm>

4. <http://www.british-legends.com/>

Spam As a Privacy Issue

In 1928, Justice Louis D. Brandeis wrote, “They conferred, as against the government, the right to be left alone—the most comprehensive of rights and the right most valued by civilized men.”⁵ *The right to be left alone* became the battle cry of many privacy advocates. Spam is considered an invasion of a right that is categorized as communication privacy.⁶ Just as you would not want a stranger knocking on your door, calling you on the phone, or following you down the street, receiving unsolicited mail is an infringement of your right to be left alone. The receipt of spam can also be considered a violation of your right to determine for yourself when, how, and to what extent information about you is used.⁷

Users should always be in charge of how and when they are contacted. Even after agreeing to be contacted, users should be able to opt out of future contacts. Continuing to contact someone after he or she has opted out of contact, or not providing a way to opt out of contact, is akin to electronic stalking. Respecting your customers’ privacy is a good way to earn their trust and their loyalty. As a consumer, demand that online services respect your privacy. This chapter provides several ways for you to fight back against spammers and discusses how to send commercial e-mail without becoming a bane of society.

The Cost of Spam

The processing of spam has become a major issue for most companies and consumers. The time it takes to process spam is not only a distraction, it is also a source of lost productivity that is affecting bottom lines. According to a recent survey, the effort being applied to managing spam will cost companies \$8.9 billion yearly, with \$650 million being spent on antispam and content-filtering products alone in 2003.⁸ Even if you are simply

5. This was written during the case *Olmstead v. United States*, <http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&navby=case&vol=277&invol=438&friend=oyez>

6. Many organizations have defined unwanted e-mail as a type of communication privacy (<http://www.caslon.com.au/privacyguide1.htm>, <http://www.privacyinternational.org/survey/Overview.html>).

7. Stefan Brands, PET Workshop, Brussels, Belgium, July 2003

8. IETF Anti-Spam Research Group

reading the subject line and the sender's name of an e-mail, it takes time to determine whether an e-mail is a legitimate message to you. Often a cursory scan of the subject line is not enough, and you are forced to open some e-mails to determine their validity. This converts to lost man hours processing unsolicited and unwanted e-mail. There is also a cost associated with processing each e-mail where it enters a company or an Internet service provider (ISP). For example, if it takes four servers to process one million e-mails per hour and half of the e-mail being received is spam, then half of your equipment costs are basically going to process e-mails that rarely benefit anyone. You also have to consider the electrical power, maintenance, administration, and storage costs for the extra equipment you have to purchase just to keep up with the additional e-mail traffic that you have to process.

Consider some numbers: Nortel Networks indicates that 70 percent to 80 percent of the e-mail that they receive each day is spam, and the rate of spam doubles every 4 to 6 weeks. This costs them about \$1,000 to \$5,000 per day. Aristotle Inc., a small ISP in Little Rock, Arkansas, indicated that spam costs the company \$5 per customer per year. The annual cost to pay for new technology and manpower to manage the spam problem comes to \$112,000 a year just for that ISP.⁹

A report by London-based security firm mi2G shows that spam caused more economic damage than hackers and viruses in October 2003. The report goes on to say that spam caused \$10.4 billion in economic losses worldwide, whereas viruses and worms caused \$8.4 billion in losses, and hackers \$1 billion in losses. Not only have spammers been filling the inboxes of corporations, they have also started attacking operators of spam block lists, which are providers that assist companies with detecting unsolicited e-mail. Spammers are flooding servers of the block list operators with spam attacks, forcing them to shut down. This is leading to increased costs to acquire more bandwidth and protection, costs that will probably have to be passed along to customers.¹⁰

9. Kris Oser, "Live from FTC Forum: What Spam Costs," *Direct Newsline*, May 1, 2003.

10. Tim Lemke, "Spam Harmed Economy More Than Hackers, Viruses," *The Washington Times*, November 10, 2003.

Spam Litigation

Many states and even foreign governments are passing antispam laws. Virginia went so far as to make sending unsolicited e-mail a felony for egregious offenses. A conviction can lead to a prison term of one to five years, a hefty fine, and a seizure of profits and income from the sale of spam advertising.

Companies have also successfully used legal action to extract damages from spammers. EarthLink was awarded \$16.4 million from Howard Carmack for using EarthLink services to send 825 million pieces of spam. EarthLink was also awarded \$25 million in damages in a suit against Kahn C. Smith. Both individuals have been banned from sending future spam.” America Online has won 25 spam-related lawsuits against more than 100 companies and individuals, including one resulting in an award of \$6.9 million from a Virginia-based spammer.

Not only does processing spam negatively affect productivity and increase IT costs, it often contains obscene images, financial scams, and malicious software that can damage a user’s computer or an enterprise’s network. A practice known as *phishing* is used by criminals to fake solicitations from online companies such as eBay and Citibank. These solicitations are sent as e-mails that are dressed up with logos and other formatting to look like an e-mail that could have been sent by the company that they are attempting to impersonate. The e-mails request personal information such as a credit card number or social security number. Brightmail, an e-mail protection vendor, indicated that 27 percent of the e-mails that they filtered in October 2003 were phishing e-mails.¹²

Malicious e-mails cause consumers to lose confidence in doing business online, which can affect every company with an online presence. It behooves all of us to support the antispam movement. Developers and researchers are working on solutions to the spam problem. As the perpetrators of spam become cleverer in their techniques for circumventing standard antispam solutions, software developers have become cleverer in their approach to antispam solutions. Several of these antispam solutions are discussed later in this chapter.

11. “EarthLink Wins Antispam Injunction,” Associated Press, May 7, 2003.

12. David Strom, “‘Phishing’ Identity Theft Is Gaining Popularity,” *Security Pipeline*, November 20, 2003.

What Can Be Done to Fight Spam

The previous sections describe various aspects of spam and how it affects individuals, companies, and developers. Based on the enormous negative impact that spam has on our lives, we all bear a responsibility to do what we can to stop spam. The following sections look at ways in which each of us can help to fight spam.

Individuals

Individuals have the biggest opportunity to affect spam.¹³ It's individuals who are running the companies, marketing departments, and data centers that send out spam. Individuals are also the terminus for spam; meaning collectively we could use tools that can make spam a bad memory. The suggestions that I am providing here for individuals applies to consumers, employees, students, and other direct users of computers:

- **Use antispam software**—ISPs often provide antispam tools as part of their service. Most e-mail applications come with antispam features. You can also obtain free tools from advocacy groups on the Internet. Turn on the antispam features of your applications. Use these features as part of your decision-making process for companies and products that you are researching. Client-side antispam software is discussed in the “Antispam Approaches” section.
- **Discourage spam**—We all face situations where we could send on a chain e-mail, pass on e-mail-based ads, or choose a company that has a less-than-reputable reputation for delivering bulk e-mail. To quote Nancy Reagan, “Just say no!” It may seem cute, or harmless, or a way to make more money, but in the end it costs us all money in lost productivity and even lost jobs due to lower profit margins.
- **Validate attachments**—Some spam can carry a piece of devious software that can cause spam and the software itself to be propagated to everyone on your contact list. Be certain of attachments before you open them, even if they come from someone you know. I even call my wife before opening an attachment from her, just in case!
- **Don't buy from spammers**—Spammers who send advertisements only continue to do it because it's profitable. Whatever they are selling, you can get from someone else. Use Google.com to find alternative suppliers of anything you might find interesting in spam.

13. The Sarasota PC User's Group also has a great list of 2004 New Year's resolutions, <http://www.davebytes.com/db010504.htm>.

Companies

Companies can be seen as bearing the greatest burden when it comes to spam. Spam causes them to lose money and productivity. Spam clogs their networks. But their advertising campaigns are also the originators of spam, either directly or indirectly. Here are some suggestions for corporations to nip spam in the bud:

- **Use antispam software**—Ensure that your e-mail servers use antispam software. Work with organizations such as Brightmail¹⁴ to deploy a spam-prevention solution for your company. Insist that your employees use antispam software on their desktops and at home. As an ISP, provide free antispam software to subscribers of your service. Both server-side and client-side antispam software is discussed in the “Antispam Approaches” section.
- **Have an anti-spam policy**—Each company should have a policy that discourages sending spam as a marketing tool or doing business with distributors of spam. All of your customers and potential customers should have a way to opt out of e-mails from your company. These opt-out preferences should be honored by all of your employees and agents.
 - As an ISP, don’t permit your members to use your resources to send spam. Use a challenge-response system to avoid the automatic creation of accounts for sending spam and other devious software.
- **Join the organized fight against spam**—Join organizations to fight spam and to pass appropriate legislation for going after spammers.¹⁵ Be a visible advocate of spam prevention. It will show your employees that you are serious about your antispam stance and enhance your corporate brand with consumers.

Developers

Developers build applications, Web services, and line-of-business applications that could potentially send e-mails to the general public. Your software could also collect contact information from consumers that could later be

14. Brightmail, Inc. is the award-winning creator of enterprise-level antispam software, <http://www.brightmail.com/>.

15. “Yahoo, Microsoft, AOL Sue Under New Anti-Spam Law,” Bloomberg News, March 10, 2004.

used to send spam to them. You have a choice to protect people like yourself and your family who are recipients of spam by doing the following:

- **Discourage bad behavior**—Many developers, including myself, run across people who are a bit extreme in their views about what constitutes fun. We are in a unique position to be part of the community of people who can create many of the applications that are reported in the news. As part of this community, we should discourage the creation of spam tools or devious software and their proliferation.
- **Write privacy-aware applications**—When creating applications that can send or collect e-mail, we should add features that permit adherence to a user's privacy preferences. When creating Web sites that send e-mail to users, provide a means for users to opt out of any e-mails that your Web site might send.
- **Expand antispam research**¹⁶—Several organizations are conducting antispam research. Typically, the work performed by researchers is rarely developed into products. It is important that product developers recognize the value in the research and incorporate it into their products. Work with research groups to see whether there is a new approach from which your product or service could benefit.

Antispam Approaches

This section looks at several approaches that have been taken to combat spam. Most of these are techniques that have been incorporated into tools and larger applications. The last two are approaches with which many of us could become more involved:

- **Accept list**—This is a list of e-mail addresses or domains that are determined to be trusted. This list is built over time as the user determines which e-mails are spam and which ones are legitimate. The drawback to the approach is that spammers often use fake e-mail addresses to evade being identified by these lists. For example, I often get e-mails that have my e-mail address as the sender. This approach also requires constant interaction from the user.

16. The Anti-Spam Research Group is the best place to get connected with researchers, <http://asrg.sp.am/>.

- **Block list**¹⁷—This is a list of e-mail addresses or domains that are determined to be responsible for sending spam. This list is built over time as the user determines which e-mails are spam and which ones are legitimate. The drawback to the approach is that spammers usually use fake e-mail addresses and domain names and often change them to evade being identified by these lists. This approach also requires constant interaction from the user.
- **Challenge-response**—This technique sends an e-mail to the originator of an e-mail asking the originator to validate the e-mail by answering a question or typing in a sequence of numbers and letters displayed in an image that cannot be easily read by a computer. This method easily catches spam sent by automated systems where no one is monitoring received e-mails. Unfortunately, this can include legitimate automated response systems from which you may receive an e-mail as the result of an online purchase or a subscription to an online newsletter. This technique can also be an annoyance because e-mails are delayed by a request being sent to the originator asking for validation.
- **Keyword-search**—This approach looks for certain words or a combination of words in the subject line or body of an e-mail. For example, an e-mail that promotes organ enlargements or Viagra would be considered spam. Using a keyword search to validate e-mails for children may be fine. However, many of the words in a keyword search could be part of legitimate e-mails. Moreover, many spammers use clever misspellings to get around these types of filters. Search rules are not case sensitive (so SEX, Sex, and sex as subject words would all be detected). Misspelling and punctuation in the middle of a spam word defeats keyword search spam detectors. Spammers also add additional white space or invisible characters between letters in a word to avoid these filters.
- **Hashing**—With hashing, the contents of a known piece of spam is hashed and stored. Each received e-mail is then hashed and if the hash matches any of the stored hash values for spam, it is rejected. Although this technique is quite accurate at rejecting known spam, it requires additional computing power to process each e-mail, and it is not very effective against most spammers. Many spammers modify their e-mails by adding a random phrase at the beginning or end of an e-mail, which renders hashing useless.

17. A directory of sites that provide block lists can be found at <http://www.spam-blockers.com/SPAM-blacklists.htm>. Although the terms *whitelist* and *blacklist* are used to discuss lists used in spam control, many people find the terms inappropriate, so I don't use them. For Carla.

- **Header analysis**—Each e-mail that is sent across the Internet has a header associated with it that contains routing information. This routing information can be analyzed to determine whether it has the wrong format, because many spammers try to hide their tracks by placing invalid information in the header. For example, the from-host field of one line may not match the by-host field of a previous line. Although this may indicate spam, it could also indicate a misconfigured e-mail server. Equally, a well-formed header doesn't necessarily mean that an e-mail is not from a spammer.
- **Reverse DNS lookup**—This approach validates the domain name of the originator of an e-mail by performing a Domain Name System (DNS) lookup using the IP address of the originator. The domain name that is returned from the lookup request is compared against the domain of the sender to see whether they match. If there is no match, this e-mail is considered spam. Although this can be effective in many cases, some companies do not have their DNS information set up properly, causing their e-mail to be interpreted as spam. This happens often enough to be a problem. That, combined with the performance hit for doing this, makes this solution less than optimum. To perform your own DNS lookup, go to <http://remote.12dt.com/rns/>.
- **Image processing**—Many advertising e-mails contain images of products or pornographic material. These images usually have a link associated with them so the recipient of the e-mail can click it to obtain more information about the product or service being advertised. Images can also contain a Web bug used to validate an e-mail address. Blocking these images can protect children from harmful images. Some spam tools flag e-mails with images, especially if they are associated with a link, and block them from the inbox. Some sophisticated tools can perform a keyword search of images and reject an e-mail based on the results.
- **Heuristics**—This technique looks at various properties of an e-mail to determine whether collectively enough evidence exists to suggest that a piece of e-mail is spam. Using this approach, several of the techniques previously mentioned, such as header analysis and reverse DNS lookup, are combined and a judgment made based on the results. Although this approach is more accurate than any of the approaches used individually, it is still not foolproof and requires a lot of tweaking to compensate for new evasion techniques that spammers deploy.

- **Bayesian filter**¹⁸—This filtering technique is one of the cleverest and most effective means for combating spam.¹⁹ It is a self-learning mechanism that can continue to outwit spammers during its lifetime. It works by taking the top tokens from legitimate e-mails and spam e-mails and placing them in a weighted list. Tokens are words, numbers, and other data that might be found in an e-mail. Fifteen tokens are considered to be the optimum number of tokens to use. Too few tokens and you get false hits because the few tokens will exist in good and bad e-mail. Selecting too many tokens results in more tokens appearing in good and bad e-mail.²⁰
 - Suppose, for example, that you are a doctor. It may be common for you to receive e-mail with the words *breast* and *Viagra* in them. However, the words *examination*, *patient*, *x-ray*, and *results* should be more common for your legitimate e-mails than spam. These words would become tokens for the legitimate list, and spam-related tokens would go in the other list.
 - You can see how this technique would be more effective on the client than at the server. Deploying this at the server will result in a more generic set of tokens than tokens that are customized for the type of e-mail that each individual would receive. Looking at the previous example, the tokens for the doctor would probably not appear in the legitimate e-mail list because the majority of the e-mails being received by the e-mail server probably won't be for a doctor, or certainly not for the same type of doctor.
- **Payment at risk**—This is an idea that was presented at the World Economic Forum in Davos.²¹ It would charge the sender of e-mail a small amount of money each time one of the sender's e-mails was rejected as spam. Although this may be worrisome for senders of legitimate bulk e-mail, it should not be a problem if they are using an opt-in model for determining who is sent e-mails.

18. CRM114, the Controllable Regex Mutilator, is considered one of the best Bayesian filter algorithms, <http://crm114.sourceforge.net/>.

19. One researcher found a way to defeat this type of filter. However, the effort involved is basically cost-prohibitive, <http://news.bbc.co.uk/1/hi/technology/3458457.stm>.

20. K9 is a software filter that works with POP3 mail servers that implement a Bayesian filter and it is absolutely free, <http://www.keir.net/k9.html>.

21. <http://news.bbc.co.uk/1/hi/business/3426367.stm>

- **Honeypots**²²—Some spammers use open relays on the Internet to send their spam on to its final destination, thus hiding their own identity. A honeypot is a service that simulates the services of an open relay to attract spammers and detect their identity. Deploying these can help fight spam, but could also make you a target. There have been cases where companies that deployed honeypots suffered denial-of-service attacks from spammers attempting to seek retribution. Operators of honeypots can also risk litigation by interfering with Internet communications.²³ Funding one may be better.²⁴
- **Legislation**—Legislation such as the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act²⁵ has made great strides in stopping U.S.-based spammers from sending out spam. The European Union's E-Privacy Directive Proposal also seeks to stop spammers.²⁶ Support of these types of legislation can do a lot for national spam control and will hopefully encourage other nations to pass similar laws.

Challenge-Response for Account Creation

Several ISPs, such as MSN, AOL, and Yahoo, have implemented challenge-response systems for the creation of new accounts to thwart spammers who use automated programs to create new e-mail accounts from which to send new spam. In typical challenge-response systems, the user is presented with a blurred image and asked to enter the characters displayed in it using the keyboard to complete the creation of a new account. This represents a major barrier to spammers who use automated account-creation systems. EarthLink has even extended this feature to force e-mail senders to respond to a challenge e-mail before their initial e-mail is delivered to the addressee.²⁷

22. <http://www.honeypots.com/about.html>

23. Kevin Poulsen, "Use a Honeypot, Go to Prison?," SecurityFocus, April 16, 2003, <http://www.securityfocus.com/news/4004>.

24. Steven J. Vaughan-Nichols, "Stopping Spam Before the Gateway: Honeypots," eSecurityPlanet.com, November 13, 2003, http://www.esecurityplanet.com/trends/article.php/11164_3108311_2.

25. <http://www.spamlaws.com/federal/108s877enrolled.pdf>

26. The European Coalition Against Unsolicited Commercial Email, <http://www.eurocauce.org/en/index.html>.

27. Jonathan Krim, "EarthLink to Offer Anti-Spam E-Mail System," *Washington Post*, May 7, 2003.

A variation of this idea proposes to send a response to each sender of an e-mail to force the sender to perform a simple operation that will use up the resources of the originating e-mail server. Although this is not of any consequence to a sender of a few e-mails, this would heavily impact a company that sends millions of e-mails.

Client-Side Antispam Solutions

Client-side e-mail solutions are features that come with an e-mail client such as Outlook, Netscape, or Eudora. ISPs such as MSN, Yahoo, and AOL also provide antispam features for their client software. These features usually consist of filters that check incoming e-mail and block it based on various criteria. Many of these filtering techniques were described in the previous section.

E-mails that are filtered may be placed into a spam folder, deleted-items folder, a specified folder, or just deleted. One of the problems with these filters is they can inadvertently filter out valid e-mails. Suppose, for example, that you have a filter that routes e-mails to a spam folder based on obscene words. After setting up the e-mail filter, you may receive an e-mail from your doctor about breast cancer. This e-mail could be filtered out of your inbox as spam. For this reason, some e-mail clients permit the user to flag e-mails that have been routed to a spam folder as legitimate e-mails. This flagging tells the filter utility to accept e-mails from specific e-mail addresses or domains. The utility remembers the user's selection and uses the information to filter successive e-mails that arrive at the client. However, this can be a bit tedious. Some more advanced filters automatically place the e-mail addresses of contacts and sent e-mails on the list of acceptable e-mails, relieving users of this burden.

Microsoft Outlook 2003 and MSN software both block images by default. Images that are embedded in e-mails may contain Web beacons that can be used by spammers to validate e-mail addresses. For users who have enabled the preview feature of their e-mail client, these Web beacons can be activated without reading the e-mail.

Peer-to-peer software such as Cloudmark permits users to mark e-mail as spam. Information about the marked e-mails goes to the other members in the peer-to-peer network to block the e-mails from other members' inboxes. This permits everyone in the peer-to-peer network to benefit from spam detection by any of the members.

The company Cobion²⁸ makes Windows, Linux, and Solaris-based e-mail filtering software. Their Web filter software controls which Web sites employees can visit based on the employee's role, the Web site's address, and the Web site's content. Their e-mail filter can control e-mail entering or leaving an enterprise. The e-mail filter makes use of acceptance and rejection lists. They also filter on domain name, subject, body content, and the content of attachments. The software is also able to scan an image file to determine whether it contains restricted text.

Spam and Infected Attachments

Undesired attachments that often accompany e-mail are not considered spam. However, when they contain viruses, they can be more harmful than the spam that delivered it. One thing that makes malicious attachments insidious is the fact that they can come from people you know who were previously infected by the same software virus. Using an antivirus application such as the ones that are made by McAfee, Symantec, or Computer Associates can help protect your computer and data from harm. Following are some guidelines that can help protect you against viruses:

- Don't open attachments from unknown e-mail addresses.
- Validate that attachments sent by friends were actually sent by them.
- Use antivirus software to scan e-mail attachments.

Server-Side Antispam Solutions

For enterprises and ISPs, the client-side filter does nothing to relieve the network traffic or reduce the resources needed to process e-mail. To positively impact a company's infrastructure costs, an antispam solution needs to stop spam before it enters the enterprise. This section looks at various types of solutions to help do this.

Block List Companies²⁹

A block list is a list used to indicate e-mail addresses or domains from which you want to block e-mail. Companies have used their own lists for years to help determine which e-mails are spam. Block list companies such as

28. Cobion was recently acquired by Internet Security Systems, <http://www.iss.net/>.

29. A selection of block list companies is at <http://www.spam-blockers.com/SPAM-blacklists.htm>.

Brightmail, Spews.com, and SpamCop make the process more efficient by combining lists from multiple companies. This is one of the easiest ways for companies to protect themselves from unwanted e-mails. The savings made from not having to process spam can easily compensate for the fee charged by these companies.

Antispam Server Software

Some companies sell software that is run on a server between the Internet and the company's e-mail server. The purpose of this software is to remove the burden of filtering e-mail from the e-mail server. This type of software can relieve companies of the expense of having to create and manage their own solution. In an effort to benefit from their investment in antispam software, for example, Boeing is commercializing its internal solution, which it is calling MessageGate Security Edition.³⁰

IronPort not only creates systems to permit companies to send bulk e-mail, they also sell servers that enable companies to filter spam.

In addition, two solutions—Spam Sleuth and SpamSquelcher—take a slightly different approach to the way that they protect companies from spam.

Enterprise from Blue Squirrel provides a solution that blocks spam from reaching a company's e-mail server. This product enables administrators to configure the many filtering options while enabling users to personalize their settings through a client application. The following list identifies some of the product's many features:

- Works with any e-mail server
- Challenge-response to force senders to validate their e-mail at a Web site
- Permits domain-level rejection or acceptance lists
- Replies to spam transmissions as undeliverable
- Validates senders by using the following criteria:
 - Checks for missing reply address
 - Validates that from address is equivalent to reply address
 - Compares the IP and DNS data against rejection lists
 - Checks subject and body text against blocked words

The product SpamSquelcher is marketed by ePrivacy Group. This product is unique in that it does not block any e-mails from reaching your company.

30. Matt Hines, "Boeing's Antispam Spinoff Takes Flight," CNET News.com, August 21, 2003.

What it does is increase the processing time for delivering spam for companies sending spam. In this manner, legitimate e-mail is not accidentally lost because of an overly sensitive filter. Decreasing the delivery bandwidth for spam has the effect of increasing the bandwidth for legitimate e-mail while increasing the costs of spammers who send e-mail to companies that deploy this technology.

Developing E-Mail-Friendly Solutions

Many companies and developers are building solutions that include a feature for sending newsletters, service updates, or marketing literature. When doing so, only collect the minimum amount of information needed to provide this service. Provide a way for your customers to opt out of these mailings. If you are bothered by the volume of e-mail that you receive on a daily basis, you can understand that customers want an easy way to manage their own e-mail. Your solution should include a way for users to manage their e-mail settings during the install process, while using the solution, and by going to your Web site.

If you provide a purely online service to customers, you should permit visitors to your site to decide whether they want to receive e-mails, including confirmation e-mails. Don't assume that your customers want to receive these e-mails. Enabling customers to look up a confirmation to an online transaction is a better long-term approach. Provide a means for customers to easily modify their e-mail settings in case they want to remove themselves from an e-mail list. Look at providing options that control how frequently customers receive e-mails. For example, consumers may only want to know about travel specials around holidays instead of every week.

Make sure that your policies on bulk e-mail are followed by agents to whom you outsource the distribution of e-mail. In addition, when you share e-mail lists with partners (with the consent of your customers only), be sure that they follow your e-mail policies.

If your company sends out bulk e-mails, be sure to register with block list companies to avoid having your e-mails flagged as spam. Although you may have a legitimate reason to send out thousands of e-mails at a time, there is no easy way for a recipient to distinguish these e-mails from spam unless you make an effort to inform the intended recipients ahead of time. Any cost associated with doing this should be offset by an increased delivery rate of your e-mails.

Protecting Legitimate Bulk E-Mail

Often companies send newsletters, monthly statements, airline specials, and security alerts using bulk e-mail to consumers who have subscribed to receive these mailings. Unfortunately, many of these mailings are blocked by spam filters and rejection lists. This has led to lost revenue, litigation, and the inconvenience of consumers who rely on the mailings.

Companies such as ePrivacy Group are creating solutions that block spam while permitting legitimate bulk e-mails to make it to their destination. ePrivacy's Trusted Sender Program requires that bulk e-mail companies register with them and adhere to certain practices in order to be accepted into the program. Subscribers to the service are able to add a trust stamp to their e-mail, informing users and e-mail servers that the e-mail can be trusted.

Bonded Sender is a similar program that is run by IronPort. Their program requires participants to pay a bond and agree to send e-mail only to users who have requested e-mail. Participants are added to an e-mail acceptance list. Companies that violate the agreement are placed on an e-mail rejection list and forfeit their bond.

Project Lumos, which is run by the E-mail Service Provider Coalition (ESPC), is an e-mail registry and authentication system that will help distinguish between valid and rogue bulk mailers. The 30 members of the ESPC represent more than 200,000 commercial marketing clients. Its success requires participation from ISPs.³¹

Participating in programs such as these will help lower costs and ensure the delivery of legitimate e-mail.

The SpamCon Foundation has gone a step further than simple participation; they are helping to fund companies running e-mail validation lists that are defendants in lawsuits. Spews.com, which was being sued by a group of spammers, was SpamCon's first client. A Florida judge eventually vindicated Spews.com's antispam tactics and dismissed the suit.³²

31. Stefanie Olsen, "Marketers Unite to Cook Spam's Goose," CNET News.com, April 23, 2003.

32. Daniel Tynan, "Antispam Activists Win (and Lose) in Court," PCWorld.com, October 14, 2003.

Conclusion

For many companies and individuals, spam is an annoyance and undesired expense. Many products and services are available to help avoid spam. Only by using these tools can we help to stem the tide of the ever-increasing unsolicited e-mails that reach our inboxes every day. If companies with which you do business send you spam, make them stop. Support programs such as the Trusted Sender Program and efforts from companies such as the SpamCon Foundation to assist antispammers.

If you are a solution provider or developer, create e-mail-friendly solutions. Make sure you give customers an easy way to manage e-mails from you. Register with companies that may mistakenly tag your e-mails as spam.

References

Spam.abuse.net is the best site on the Internet dedicated to fighting spam. It contains a wealth of content, tips, and links to help you and your organization fight spam. Help for consumers can be found at <http://spam.abuse.net/userhelp/>. Help for IT administrators can be found at <http://spam.abuse.net/adminhelp/>.

Stopspam.org is another site dedicated to stopping spam and other abuses of the Internet. They provide similar tools and content to help consumers and companies fight spam. This site provides information in other languages, such as Hungarian, and they are always looking for volunteers to translate their content into other languages.

Spamresearchcenter.com is a Web site that is dedicated to creating free antispam software for the general public.

