

Stop Spam Now!

By John Buckman

John Buckman is President of Lyris Technologies, Inc. and programming architect behind Lyris list server.

Copyright 1999 Lyris Technologies, Inc.

Introduction

In the middle of a hectic workday, you check your email box only to find it cluttered with messages ranging from get-rich schemes to advertisements for questionable products. Junk e-mail or spam is a growing problem for Internet users, whether you are an individual or a large corporation. According to varying studies, the cost of spam ranges from millions to billions of dollars worldwide. John Buckman, developer of the MailShield anti-spam/anti-relay program discusses the impact of spam, and describes 5 strategies for stopping spammers in their tracks.

What is Spam?

Spam is junk email that is sent to you by someone who has no prior or existing relationship to you. Whether one calls it unsolicited commercial email (UCE), unsolicited bulk e-mail (UBE) or junk mail, spam is defined by the fact that the recipients did not solicit the mail or divulge their email addresses for the purposes of receiving such mail. Yet, each day, thousands of spam programs scan web pages, newsgroups, and other online documents to harvest email addresses in bulk. As a result, spammers can send a high quantity of mailings to large numbers of unsuspecting users, whose mailboxes become filled with messages that may lack relevance for users.

The Impact of Spam

The problems associated with spam reach far beyond the obvious annoyance of receiving unsolicited mail. As a result of the deceptive practices that spammers use, spam can damage the reputation of companies who run mail servers, drain human energy and time, and exploit hardware resources. One of the most common techniques that spammers use is unauthorized mail relaying. Unauthorized mail relaying occurs when spammers use mail servers, owned by other people, to relay junk email. For example, after one week of setting up our own email server, we began receiving unauthorized mail relay requests. Apparently, spammers used an automated program to scan the Internet and locate our mail server. Before we installed MailShield, we discovered that spammers queued and relayed a dozen email messages per day through our server.

By engaging in unauthorized relaying, spammers make it difficult and time-consuming to trace spam back to its true source. Adding to the difficulty of tracking spam, many companies are unaware that their servers have been used to relay spam until they receive an avalanche of complaints from angry customers who received spam from these companies. Although companies can clarify to customers that they are not the "true" source of spam, it can be very difficult to regain corporate respectability after unauthorized relaying, especially if the spam contained pornography or get-rich scams.

Spammers also can damage a company's reputation by forging return email addresses. In 1998, Juno Online Services filed a \$5,000,000 dollar lawsuit against five spam companies (\$1,000,000 against each of the five companies) after their reputation was damaged by forged return email addresses. Apparently, spammers actively targeted Juno's return address for forgery. Juno President, Charles Adai, noted that their company discovered spam software for sale on the Internet that included a "forge e-mail to Juno" feature.

Spammers frequently forge return email addresses not only to prevent users from tracking the true source of spam, but also to prevent spam mail from bouncing back to their own servers. Since spam frequently contains a high number of inaccurate and outdated recipient addresses, spam mail often bounces and jams the servers spammers use to relay the mail. As a result, forged email return addresses can significantly drain hardware resources.

Fight Back!

Clearly, spammers spend a great deal of time finding ways to use other people's resources to send junk mail and conceal themselves. Given this, what can you do to fight back? The following 5 strategies can help you stop spammers in their tracks.

Stop Unauthorized Mail Relaying

One of the most effective strategies to prevent spam is to stop unauthorized mail relaying. The basic way to implement mail relay protection is to configure your mail server to allow only certain TCP/IP addresses and address ranges to relay through your server. With this technique, your mail server will reject any relay attempt from TCP/IP addresses outside of your network.

While this simple technique works fairly well, not all mail server packages support this feature. For example, version 8.6 of Sendmail, which comes with Sun Solaris systems, does not support this technique. Furthermore, many Windows NT mail systems, including Lotus Notes, CC:Mail, Microsoft Mail, and even popular firewalls (such as Gauntlet) do not provide or support basic anti-relay protection.

Third-party software, such as Lyris Technologies' MailShield, can add anti-relay security to servers that do not support filtering of TCP/IP addresses or other anti-relay techniques. You can also use some third-party software to completely replace your mail server with software that is designed to block unauthorized mail relaying and spam.

If your company has employees who travel or telecommute, you may wish to only allow specific "From:" addresses to prevent unauthorized relaying. With this technique, telecommute or employees in the field can still relay mail through your server, without interfering with your ability to block unauthorized relayers. Filtering the "From:" address is a powerful technique that specialized anti-relay and high-end mail servers support. Sendmail 8.9 examines header text to support this method, as does MailShield.

Another way to implement mail relay protection is to use a mail proxy server with anti-relay features, and a regular mail server that is protected by a firewall, internal TCP/IP address, or port-moving technique. With this implementation, the mail proxy server conceals the location of your regular server and makes it less vulnerable to unauthorized relaying. Some mail servers and anti-spam/anti-relay products support this implementation.

Ban Header Text

Many spam programs include telltale text in the headers of messages they send. For example, spam programs frequently send header text with the words, "public.com" or "friend@public."

Other examples of telltale text and tags include: savetrees.com, xadvert, and relay.comanche.denmark, email shark bulk e-mailer, extractor pro, dm pro, and dynamic mail pro.

If you ban header text, you can eliminate a significant amount of spam created by automated programs. Many mail server packages and specialized anti-spam software allow you to ban header text.

Filter Message Body Text and Subject Lines

In addition to filtering TCP/IP addresses and header text, it is also important that your server or anti-spam software filter body text. Why is it important to filter body text? If a spammer relays spam through someone else's server, the "From:" address may be a valid or acceptable address that you allow to relay. However, the email address given in the body of the text may not be the same as the "From:" address, an indicator that the mail could be spam. While many mail servers lack the ability to filter body text, specialized antispam products and some high-end servers support this ability.

Filtering body text and subject lines also allows you protection against the recent Melissa virus since "Melissa-tainted" email often includes the following telltale information:

A subject line of: Important Message From <sender's name>

A body with the following content: Here is that document you asked for ... don't show anyone else ;-)

Recently, a major telephone company used MailShield anti-spam software to block the virus. The company filtered the subject and body text of incoming mail to stop the virus from spreading through their system.

Tarpit Spammers

In general, tarpitting involves creating delays that slow down the mailsending sessions of spammers. In theory, tarpitting should discourage spammers by making it slow or difficult for them to send mail. However, there is no evidence that spammers can detect tarpitting.

On the other hand, evidence shows that when tarpitting slows down mail-sending from a server that is used for unauthorized relaying, the owner of the server may (1) become aware of the unauthorized relaying if he or she wasn't aware of it before and (2) adopt higher security measures to avoid being tarpitted. Thus, tarpitting specific domains may have an indirect result of reducing spam by encouraging the owners of mail servers at legitimate sites to use anti-relaying techniques.

Besides tarpitting specific domains, one might also tarpit users that attempt to send mail to large numbers of people. Spam software works by sending a single message, and a huge BCC (blind carbon copy) list to the server for delivery. If you know that your customers (in the case of an ISP) or employees do not need to send mail to more than 20 recipients per day, you might tarpit a mail-sending session that attempts to send mail to 50 recipients. If a person has copied 50 people, tarpitting can create a pause (such as 2 seconds) for recipients 21-50. Consequently, this delay can discourage spammers from using your server to send spam.

Last, some anti-spam software also allows you to tarpit specific TCP/IP addresses. You can define TCP/IP ranges to allow specific hosts to connect to you and to tarpit hosts known to send spam. The Real-time Blackhole List (RBL) is a blacklist of Internet TCP/IP addresses known to send spam, or sent by hosts that condone spam. The RBL is at <<http://mail-abuse.org/rbl>>. Before deciding to tarpit an address you can check the RBL to see if it is on the blacklist. However, keep in mind that the RBL also includes server addresses that are the victims of unauthorized relaying, so you may end up tarpitting servers that send legitimate mail.

Note: The RBL is an effective way to reduce the spam you receive. Yet, it is important to keep in mind that if you enable the RBL test, you may inadvertently refuse valid email from legitimate sites that may be unaware that they have been the victims of unauthorized relaying and are blacklisted.

Enforce Internet Standards

Internet mail standards basically state the following:

*All mail must have a "From:" header in it.

*All mail must have a "To:" header in it.

*All mail servers must have a reverse DNS host entry.

Spammers typically violate Internet mail standards. If you configure your mail server or anti-spam software to reject mail that does not comply with Internet standards, you can eliminate a great deal of spam. However, keep in mind that in blocking mail from servers that do not allow reverse DNS look-up, this may also result in blocking mail from legitimate sites that have improperly configured servers.

Anti-spam software like MailShield allows you to modify the rules for filtering mail and send an explanation message to users that their mail was rejected because the sending mail server does not comply with Internet standards for reverse DNS look-up. This message is particularly helpful for customers of ISPs, who can then inform their providers of the problem and encourage their ISPs to configure their mail servers appropriately and allow delivery of mail to servers that reject mail that does not comply with Internet standards.

Although not explicitly stated, valid host values for the HELO command are also encouraged by the Internet standards. Since every mail server on the Internet should have reverse DNS lookups defined, every mail server should also provide a valid hostname as a HELO value. Rejecting mail that does not have a valid hostname is another way to reduce spam.

It is also a good idea to reject mail that does not contain date headers although Internet standards do not require date headers. Many automated spam programs create messages without a "Date:" header. Checking mail for the presence of a "Date:" header will reject a fair number of spam messages. However, some automated programs that send legitimate mail also omit the "Date:" header. Before setting up your mail server or anti-spam program to block mail without date headers, you may wish to consider how important it is for you or organization to receive mail from automated programs.

Conclusion

With spam increasing steadily, it is important to take a proactive stance and arm yourself with knowledge about the methods that spammers use, so you can decide how to best implement strategies to block spam. The five strategies described here can help you reduce spam and limit exploitation of your hardware resources.

Whether you are an individual, ISP or corporation, reducing or eliminating the flow of spam plays a key role in protecting your reputation, maximizing your hardware resources, and utilizing human energy and time most efficiently.

Helpful Links

Site links to products that have anti-relay/anti-spam capabilities:

Mailshield: <http://www.mailshield.com>

NTMail: <http://www.ntmail.co.uk>

Sendmail: <http://www.sendmail.org>

Spam Resources

Coalition Against Unsolicited Commercial e-mail: <http://www.cauce.org/>
CAUCE is devoted to enacting legislation to stop spam. This site includes many helpful links and resources about spam.

spam.abuse.net: <http://spam.abuse.net/>
Scott Mueller's "Fight Spam on the Internet!" answers basic questions about spam.

Tracing the Spam: <http://ddi.digital.net/~gandalf/spamfaq.html>
This useful article explains how to trace spam back to its source and how to lodge complaints with appropriate people.

Antispam.MSExchange.org: <http://antispam.msexchange.org>
Anti-spam resource site dedicated to helping administrators fight spam on their mail servers. Updated with the latest spam news, software, related links and white papers, offering insight into the latest spam practices and the ways to combat spam with server based solutions.