# How To Deal With Spam

*Unsolicited commercial email accounted for some 10% of the 620 billion emails sent in the US in 2000. Spam represents a significant burden on networks, email servers and Internet bandwidth. Fortunately, there are many tools, services and techniques to help fight the growing flood.*

**By Andrew Ward**

Although spam causes problems to network infrastructure, perhaps the biggest nuisance it causes to an organisation is the effect on users. Spam wastes employee time, and not just because of the time taken to read the headers and then delete them. Although many spammers are extremely stupid, as evidenced by the illiterate nature of most spam, some do make a crude attempt to make messages appear to come from someone known to the recipient, and this can trap busy or unwary users into paying them more attention than they deserve.

Furthermore, users may go so far as to click on the links advertised in some spam messages, causing yet further distraction, wasted time, and even the downloading of offensive or illegal material.

## Spam And The Law

There is considerable international variation in the laws relating to spam, but it is very unlikely that any spam is ever legal. If there is no specific anti-spam law within a country or state, then spam will almost certainly fall foul both of any computer misuse (anti-hacking) legislation as well as any data protection legislation that might be in force.

Regardless of the law of the land, Internet service providers usually have a contract term that specifically prohibits the sending of spam. Any Internet user sending unsolicited commercial email therefore is in breach of contract and may have their account terminated. This does in fact happen, although some spammers will simply immediately open a new dialup account, usually using stolen credit card numbers. Fortunately, there are ways to protect against even this tactic.

## Fighting Spam

There are many ways in which an organisation can cut down the amount of spam it receives, as follows:

- Educate users to avoid actions that might encourage spam.
- Report spam so that spammers and their web sites are shut down.
- Prevent systems being used by spammers within or outside the organisation.
- Subscribe to a service that helps the organisation control the amount of spam received.
- Subscribe to a service that filters email and removes spam.
- Install filters that remove spam.

## User Actions

Most spam is generated through careless user behaviour. Users need to be educated about the various actions that can easily generate spam, and perhaps the company's acceptable use policy should be modified to include dissuasion of spam-friendly activity.

Users should not post messages in any forum that spammers might see. This includes Web bulletin boards, Usenet newsgroups, chatrooms and virtually every Internet-based communications environment except email itself. If users do need to use Usenet or similar forums for their work, they can corrupt their email address in such a way that a genuine user, but not an automated spam email address harvester, can understand and correct. For example, change andrew.ward@itp-journals.com to andrewREMO.VEward@itp-journals.com.

Alternatively and additionally, users can post messages in such environments using a different email address - for example, one from a free Web-based service such as hotmail - where the vast volumes of spam generated won't interfere with their daily work or the company's network.

It's also a good idea to keep a watch on what users are doing. How to do this depends on what monitoring capabilities there are within the elements of network infrastructure already in place. Some firewalls can monitor and log user activity, as can Novell BorderManager. Otherwise, add-on products such as eTrust from Computer Associates (**http://www.ca.com**) can do the job. It may be worth going even further and physically preventing certain activities - such as Usenet postings - using filtering tools or the capabilities within firewalls.

## *Never Reply*

One thing that users should never, ever do is to respond in any way to a spam message. Replying to the message, or replying to any address that might be listed within the message for being removed from the mailing list, simply tells the spammer that the address used is live and active. The result - a lot more spam, both from the original spammer and from anyone to whom he sells the list.

Furthermore, even clicking on a link within a spam message can tell the spammer who responded and when. People who respond are immensely valuable to spammers, since of course most people just delete these illegal messages.

How do spammers achieve this? Careful inspection of spam messages reveals that some contain hyperlinks with complex URLs. Encoded into these is the user's email address, or a reference to it within the spammer's database.

When registering on Web sites, explain to your users that they must take the utmost care to only register with legitimate, recognised businesses and to avoid any guestbooks, free memberships and other dubious sites that request email addresses. Even with legitimate sites, users should be careful to read any small print about junk mail, and either check or uncheck boxes as appropriate to opt out of any follow-up email. Often the same registration form will contain more than one checkbox, with some requiring the box to be checked and others unchecked.

Some sites don't offer these options at registration time at all, but include registrants on mailing lists automatically. It's necessary to revisit the site and amend user preferences to opt out of junk mailings.

Both the organisation itself and individual users should be wary about publishing email addresses on Web sites. If possible, publish forms that people can use to send enquiries instead, so no email address is visible to automatic address harvesters. However, recent activities by spammers have even included posting messages onto forms rather than sending email.

## *Receipt Of Spam*

Whatever procedures and systems are put in place, it's almost inevitable that some spam will get through to users, so guidelines should deal with this eventuality. Ideally, messages should be forwarded to the network administrator and then deleted but the tendency of many mail clients to remove full headers means that users need to go to some trouble to forward messages correctly, which may be unworkable. Full headers are necessary if the spam is to be reported, or the sender and / or sending domain are to be added to filtering rules.

> *"Users need to be educated about the various actions that can easily generate spam, and perhaps the company's acceptable use policy should be modified to include dissuasion of spam-friendly activity."*

## *Reporting Spam*

Any spam received should be reported to the sender's ISP, the owner of the mail relay used (which may be a different organisation), and the ISP of any web sites and email addresses referenced within the spam - unless they are spoof addresses, of course. There are many resources on the Internet that explain how to read and understand message headers in order to be able to report the spam to the appropriate authorities. One of the best is at **http://spam.abuse.net/howtocomplain.html**.

*This article will be concluded next month.*

**PCNA**

# How To Deal With Spam

*Unsolicited commercial email accounted for some 10% of the 620 billion emails sent in the US in 2001. Spam represents a significant burden on networks, email servers and Internet bandwidth. Fortunately, there are many tools, services and techniques to help fight the growing flood.*

**Concluding our two-part article.**

**By Andrew Ward**

Understanding headers can be a complex process since it involves unpicking them to find out where the mail originated - there will be false trails and unresolvable hosts. The overall objective is to identify the abuse departments of the relevant ISPs and organisations - usually, contactable via abuse@domain - and send them details of the spam and a request to disconnect the user or Web site.

Sometimes the message sent in these circumstances is (incorrectly) referred to as a LART (Luser Attitude Readjustment Tool), a fictional Unix command used to disable or kill the account of a misbehaving luser (formed from loser + user). However, reading the headers manually and then looking up the relevant hosts and their owners can be a tedious process. If the only intention is to report the spam, rather than garner the sending host and mail server information to include in filters, then there are automated tools on the Internet to complete this task. One of the best, and easiest to use, is **http://www.spamcop.net**. Alternatively, messages with full headers can be forwarded to spamcop@spamcop.net.

However the utmost care should be taken when using automated tools such as SpamCop. If an ISP receives a complaint about an entirely innocent party then abuse complaints won't be taken so seriously in future. The results that SpamCop produces should therefore be carefully inspected before issuing the complaints.

Note too that SpamCop, being an automated tool, isn't perfect. Sometimes it can fail to detect the originating mail host, and manual work will be necessary to track it down. The page at **http://spam.abuse.net** provides some information on deciphering message headers. If you require more detailed reference works, these can be found at Web sites: **http://www.stopspam.org/email/headers/headers.html**, **http://www.faqs.org/faqs/net-abuse-faq/spam-faq/** and at **http://www.claws-and-paws.com/spam-l/tracking.html.**

## Remove Spam-Friendly Features

Unfortunately, early mail servers were configured in such a way that anyone outside an organisation could use them to relay mail, thereby helping to conceal the origins of spam. Instructions for configuring sendmail to close open relays, and other measures to help prevent spam, are at **http://www.sendmail.org/m4/anti-spam.html.**

## Use External Services

At **http://mail-abuse.org** there are details of the RBL (MAPS Realtime Blackhole List), DUL (MAPS Dial-Up List) and RSS (MAPS Relay Spam Stopper). These are intended for use by ISPs and corporate network administrators to block mail from blacklisted sites, sent directly from dial-up IP addresses, and from open mail relays, respectively. The MAPS (Mail Abuse Prevention System) site contains details on how to use these tools with various different mail servers.

The RBL works by creating deliberate network outages. If spam originates from a traceable IP address, and after persistent complaints the ISP has failed to take the appropriate action, then the ISP may find some or all of its IP addresses added to the RBL. Organisations using the RBL can then choose to refuse to accept mail from those IP addresses, or to take whatever action is consistent with local site security policies. Some administrators reject all mail coming from such sites, and some will also direct any traffic destined for such hosts to a local black hole.

Note that use of the RBL (and DUL and RSS) may result in complaints from users that they can no longer receive mail from certain domains, so this rather drastic solution should be used with caution. Both the DUL and RSS are excellent means of cutting down on spam, and can be used in conjunction with the RBL or on their own.

## *Use Filtering Services*

Spam prevention services use a number of different techniques. Filtering is not totally effective because virtually all spammers except the most stupid design their messages to overcome filters, but it can bring about a noticeable reduction in the amount of spam received. Of course, the drawback of an external service is that yet another provider is inserted in the path of incoming mail, which can only increase delays and outages. One service overcomes these problems. Brightmail installs a dedicated server at the customer premises that works in conjunction with the existing mail server. The Brightmail Server houses the collection of rules that filter spam, and these are updated at frequent intervals.

There are also filtering services available for personal use, for example at **http://www.despammed.com** and at **http://stop.mail-abuse.org**. Similar sites are **http://www.spamkiller.com** and also **http://spamcop.net**. Some filtering services, such as that operated by SpamCop, optionally allow the user to reject all mail that doesn't come from a pre-approved sender.

## *Install Filtering Systems*

Filtering can be carried out in two ways - either at a point between the Internet connection router and the mail server, or within the server itself. The gateway solution prevents the spam from being transported and housed in the internal network at all, but the mail server solution doesn't require any additional hardware and provides a central point of management for mail services. Another option is to configure the Internet router itself to ignore mail from IP number blocks that appear in the RBL so the traffic never enters the network at all.

Add-on spam filters available include SpamAssassin from **http://spamassassin.taint.org**, MailMarshal from **http://www.marshalsoftware.com**, and MAILsweeper from Baltimore Technologies (**http://www.mimesweeper.com**). In addition, mail servers can themselves be configured to filter out spam. For example, Sendmail 8.9 and later versions have built-in anti-spam rules, filtering, and the ability to block known spammers and unresolvable hosts. These and other features are explained in some detail on the Sendmail Web site. Features new to versions 8.10 and 8.11 are detailed at **http://www.sendmail.org/~ca/email/chk-810.html**.

One user reported that working over 13,051 email messages, SpamAssassin - which identifies spam using text analysis - failed to correctly identify eight out of 253 spam messages, and also reported 12 false positives. Because any filtering tool might sometimes report false positives - that is, report a message as spam when it isn't - it is important that mail identified as spam is not simply deleted. Instead it should be put into a holding area where it can be manually inspected by an administrator and forwarded if appropriate. Alternatively, some schemes - such as Brightmail's - allow individual users to inspect their own "grey mail" for false positives.

*"One user reported that working over 13,051 email messages, Spam Assassin - which identifies spam using text analysis - failed to correctly identify eight out of 253 spam messages, and also reported 12 false positives."*

MailMarshal works by filtering on content, using the MAPS RBL, and domain blocking using domains specified by the network administrator. The Spam Manager and Spoof notifier within MAILsweeper work by content filtering and detection of email that originates from a source other than the apparent sender, respectively.

**PCNA**