Table of Contents

Intro

Email is a mission-critical aspect of corporate life today. Unfortunately, as email has become so useful to legitimate businesses, unscrupulous marketers have latched upon it as an easy and inexpensive way to reach potential customers. These unsolicited messages, commonly known as spam, can cause many problems.

Users are annoyed or offended, system administrators are kept busy securing their mail servers from unauthorized relays and preventing spam from using system resources, legitimate marketers' reputations suffer, and legislators create laws which have no recourse for spammers outside of their own state or country.

We need to look for solutions to prevent spam from wasting our human and system resources.

What is spam?

Spam can be simply defined as mass unsolicited commercial or promotional email. Spam is more or less equivalent to junk mail sent to "Occupant" or telemarketers asking "Is the lady of the house available?"

There is some debate about the source of the term, but the generally accepted version is that "spam" comes from the Monty Python song, "Spam spam spam spam, spam spam spam spam, lovely spam, wonderful spam…" Like the song, spam is an endless repetition of worthless text. [1]

The people who send spam (spammers, or bulk emailers as they prefer to be called) are treated with great hostility by members of the online community, and with good reason.

Most spam is sent indiscriminately to a large collection of email addresses with no verification that the recipient might even be interested in receiving it. It's simply easier for a spammer to send a message to 10,000,000 harvested email addresses and get 100 responses. ***real statistics on this???***

Spam is usually sent to mailing lists compiled by marketing services (or advertising brokers?) that harvest email addresses from newsgroups and websites, even ICQ details. These lists aren't that expensive. Spammers can buy an unsorted email list of 1.7 million email addresses for $125.00.

Spammers aren't just bad guys because they send junk mail that nobody has asked for; they are despised because of the ways they send that mail. They search for SMTP servers with open relays on the internet. Spammers can deliver mail via anonymous proxy servers directly to the SMTPserver of the addresse. They forge header information so

[1] http://www.webopedia.com/TERM/s/spam.html

their identities are hidden, leaving some hapless admin at joesappliance.com gets a bunch of nasty emails complaining about the spam received from his server.

Spammers don't give you the option to "opt-out" from receiving their messages. They may give you an opt-out link, but that only confirms to them that your email address is live and then guess what, you get more spam.

***Maybe include Brightmail's statistics for November 2002, different categories. Can we get permission to use their pie chart which details what kinds of spam advertisements are being sent, viagra, weight loss, etc. pyramid schemes, porn sites, get-rich quick.

Sidebar: What is not spam?

There is a difference between spam and legitimate permission-based email.

The Direct Marketing Association guidelines state that acceptable commercial solicitations are those sent to a marketer's own customers, or to individuals who have consented to receive solicitations online or have not opted out. Each solicitation should include a link to request removal from the mailing list, and a link to request that the email address not be shared with others for online solicitation if the marketer does provide such a service.

Some marketing services say they'll only deliver to customers who have opted in, and have anti-spam policies. If you have agreed to receive promotional email in return for a service, such as Yahoo's POP3 service, those messages are not considered spam.

Is There Really Enough Spam to Warrant All the Fuss?

Lots more details and statistics on how much spam is being sent and what's predicted for the future

Between November 2001 and November 2002, spam attacks increased almost 300% from Brightmail's probe network, from 1,956,529 to 5,503,246.

30% of the email messages received at AOL are spam.

According to Mercury News, The average user received 1470 unsolicited emails last year. (Feb 10, 2002)

$603 million was spent on direct internet marketing in 1998. This number will climb to $5.3 billion by 2003, according to the Direct Marketing Association.

Why Do We Want to Block Spam?

Spam violates corporate policies regarding non-business use of company messaging systems.

Deleting spam takes up employees' time. Even worse is the time spent reading and responding to spam.

Filtering spam increases corporate productivity through efficient email usage. Users don't need to waste time deleting spam. Ferris Research reports that the annual costs for reviewing and deleting spam is $546 per employee per year.

Average spam received per user per day:	3
Average spam received per user per year:	1095
Average time spent reviewing and deleting spam:	30 seconds
Time spent reviewing and deleting spam per year:	9.1 hours
Lost productivity cost per seat per year:	$546

Spam can violate anti-harassment and hostile environment policies. Avoid potential legal issues resulting from creating a 'hostile environment' especially when the contents are offensive to certain segments of employees.

Spam wastes system resources, bandwidth, mail server processing cycles, and storage capacity etc.***more***

Spam can overwhelm mail servers that are not secured against relaying.

Content filtering can also block viruses.

So What Anti-spam Techniques Do We Have to Work With?

Educating Email Users: Well, the easiest way to get rid of spam would be to have people never respond to it, making it an ineffective way to advertise. Unfortunately, there will always be people out there who want a bigger whatsit or a smaller waistline, and think that this "miracle product" will be the one that finally works. ***Maybe statistics on how much response marketers actually get***

Enforcing Company Policy: Guidelines for appropriate use of corporate messaging systems usually include no personal email. However, that can be difficult to enforce, and sometimes users have to provide an email address to receive a legitimate business-related service. That address can then be shared or sold.

Anti-Spam Software: There are dozens of products which filter spam on the market today, with more being developed all the time. Client-based products are not very effective for corporate use. Spam needs to be caught at the internet gateway.

The programs available to do this generally work with a variety of ways to identify spam.

Honey-pot systems set up decoy email addresses. Any mail delivered to one of these accounts is spam. Filters are created based on these messages.

Pattern recognition can be used to filter messages with inconsistencies in headers or patterns common to spam, such as a large number of recipients.

Peer to peer reporting, where programs send a copy of any message a user tags as spam to the system administrator. These messages are added to the database and pushed to the other users of the package.

Realtime Blackhole Lists are maintained by various administrators who hate spam. They serve many different purposes. Some only list open mail relays, some list sites from which the list admin has received spam. Some list ranges of IP addresses from ISPs that are known to host spammers. Unfortunately, that can also block legitimate subscribers of that ISP.

Content Filtering – search for phrases common to spam, group "like" phrases together, weight phrases. Identify by content, not patterns. Spammers will continue to find ways around content filtering. Free S*P*A*M!!!

Database of actual spam. Brightmail makes updates available every 10 minutes, but that's not quite real-time.

One huge drawback of spam filtering is false positives. How much spam is that one legitimate message worth? ***more***

Spam and the Law

From an email marketing website: Your advertising campaign will be fully legal. It will include a remove instruction, thus it will be in compliance with the new e-mail bill section 301. Under Bill S. 1618 TITLE III passed by the 105th US Congress.

HAH!!! There is no such law. It was proposed, but has not been passed. This practice is so prevalent it actually has a name, as defined in the Spam Glossary (http://www.rahul.net/falk/glossary.html#murk):

Murk

> (n.) A disclaimer at the end of an email spam assuring you that the spam complies with Bill S.1618 which makes the spam legal. Also known as a "Murkogram".
> (v.) The act of sending spam containing a Murkogram.
>
> The term comes from Frank Murkowski (R-AK), the senator who wrote S.1618 which would have made spam legal provided it followed certain rules. In particular, to be legal under S.1618, the spam must contain full contact info at the start and make no attempt at hiding its origin.

> There are three problems however: First, S.1618 was never passed. Second, S.1618 would not actually have made spam legal, it would have made certain kinds of spam *illegal*. Finally, most spam in fact, actually violates the provisions of S.1618.
>
> Thus, a Murk disclaimer serves as a sure sign that the message is spam, and that the sender knew they were doing something wrong.

Europe is quite far ahead of the US in terms of legislation regarding spam. The European Parliament requires advertisers using electronic mail to have the recipient's prior consent. The definition of electronic mail is broad enough to also cover text messaging systems such as mobile telephones.

In the US, we have no federal legislation, though some states have enacted anti-spam laws. Pending federal legislation includes:

Anti-Spamming Act of 2001 (H.R. 718) prevents unsolicited commercial electronic mail containing fraudulent transmission information and requires warning labels for electronic mail containing advertisements harmful to minors.

Anti-Spamming Act of 2001 (H.R. 1017) would amend federal computer crime laws to make it illegal to send unsolicited bulk e-mail messages containing a false sender address or header, or to distribute software designed for this purpose

Controlling the Assault of Non-Solicited Pornography and Marketing (CAN SPAM) Act of 2001/2002 (S. 630) would require unsolicited commercial e-mail messages to be labelled and to include opt-out instructions, and would prohibit deceptive subject lines and false headers in such messages. It would also prohibit the use of e-mail addresses harvested from web sites in violation of posted restrictions

U.S. laws will not have any effect on spammers who operate from other countries, and even those who operate in the U.S. won't necessarily heed the laws. About the best the government can do right now is have the Federal Trade Commission go after the senders of those email messages that are truly fraudulent.

For marketing purposes, there does have to be a way in the message for a recipient to respond to a spam message, and that is one way the legal system has recourse to track the creator of the message, if not the actual sender.

So what can you do about spam?

Make sure your servers are not open to relaying. This makes it easier to track spammers to the source, and if their ISP has anti-spam policy, you can get their account closed.

Enforce your corporate email policies. No personal mail to business email addresses.

Educate your users on how to avoid having their addresses targeted by spammers. Don’t use actual email address if posting to newsgroups. Get a hotmail account for junk and commercial mail.

Install a spam filter on your gateway that includes content-based criteria.

What is The Open Group Messaging Forum trying to do about it?

Please send comments to dale@jconsult.com