



The Manager's Guide to Coping with Spam

A Manager's Guide from
The Open Group Messaging Forum

DRAFT

Copyright © July 2003 The Open Group

All Rights Reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form, or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of the copyright owners.

All brand, company and product names are used for identification purposes only and may be trademarks that are the sole property of their respective owners.

The views expressed in this Open Group White Paper are not necessarily those of any particular member of The Open Group.

Document Number: Wxxx

All comments relating to the material contained in this document may be submitted to:

The Open Group
Apex Plaza
Forbury Road
Reading, Berkshire
RG1 1AX, England

Tel: +44 1189 508311

DRAFT

The Manager's Guide to Coping with Spam

Table of Contents

The Manager's Guide to Coping with Spam.....	1
Introduction.....	1
What Is Spam?.....	2
What Is Not Spam?.....	2
Types of Spam.....	3
Abusive Practices of Spammers.....	3
Illegal, Unethical, and Immoral Content.....	3
To Whom It Doesn't Concern.....	3
Address Harvesting.....	4
Dictionary Harvest Attacks.....	4
Opting Out Brings More Spam.....	4
Setting Web Beacons.....	4
Using Open Mail Relays.....	4
"Drive-By" Spamming.....	4
Open Proxy Servers.....	4
Forged Headers and "Joe-Jobs".....	5
"The Big Murkowski".....	5
Filter Busters.....	6
Why Should We Be Concerned with Spam?	7
Reasons to Stop Spam.....	7
Risks of Blocking Spam.....	7
The Costs of Spam.....	7
How Much Spam Is Out There?.....	8
What Can We Do To Minimize Spam?.....	10
User Education.....	10
Corporate Messaging Policies.....	10
Technology Solutions.....	11
Content Filtering.....	11
Pattern Recognition and Header Analysis.....	12
Reverse DNS and Address Verification.....	12
RealTime BlackHole Lists.....	13
Whitelists and Certification.....	13
Greylists.....	14
Do-Not-Spam Lists.....	14
Peer to Peer Reporting.....	14
Challenge/Response Systems.....	14
Technology Summary.....	15
Legal Options.....	15
European Legislation.....	15
United States Legislation.....	15
Proposed Rules for Fair Spamming.....	16
Spammers Rights Under the Law.....	16
Self-Regulation of Legitimate Marketers.....	16

Best Practices.....18
 The Ideal Spam Filter.....18

Summary.....19

References21

DRAFT

The Manager's Guide to Coping with Spam

Introduction

Email has grown from a novel communications tool to a mission-critical aspect of corporate life today. Not only does it provide a simple and efficient means for delivering personal and business messages; it is also a backbone service for electronic transactions. Marketers find email a very inexpensive way to reach potential customers. Many customers find email an effective way to learn about new products and promotions.

We've worked for years to make email messaging systems reliable as well as easy to use and administer, but unfortunately we seem to have made it a little too easy.

Unscrupulous marketers have latched upon email as an effective way to reach a huge number of people for a minimal cost. These marketing emails, and other unsolicited messages, commonly known as spam, are threatening to overwhelm the Internet and make email unusable.

To keep email as a viable communication option, we need to find ways to minimize the effects of spam, both for the spam received in our corporate messaging systems and the spam that can be sent using insecure mail relays. There is no one technology that will completely block all spam messages while allowing every legitimate message through, and legislation alone will not be able to eradicate spam.

In this paper we will discuss ways to bring the amount of spam we receive in our corporate email systems down to a level where we can cope with it.

What Is Spam?

A simple definition of spam is unsolicited email messages, generally commercial or promotional in nature, usually sent in bulk. The key word here is *unsolicited*.

Spam comes in many forms other than commercial advertisements for products or services; many non-commercial messages can also be considered spam, such as:

- chain letters
- charitable solicitations
- games
- hate mail (including racist and sexist messages)
- jokes and funny stories
- malicious code (email borne viruses)
- petitions
- political messages
- pornography
- prayers
- press releases
- promotional messages
- scams and "get rich quick" schemes (such as pyramid schemes)
- sentimental claptrap

Another factor often used to define spam is whether the message is unwanted by the mailbox owner, either by the individual user or the corporation that owns the messaging system. Depending on corporate messaging policies, personal messages may be treated as spam by the systems administrators. On the other hand, bulk commercial email of interest to the recipient may technically qualify as spam. Everyone has a different opinion of what is and isn't unwanted email; corporate messaging policies can serve here as a useful guideline.

Instant messages and wireless messages can also be defined as spam, if they are unsolicited, but that discussion is outside the scope of this document.

There is some debate about the source of the term, but the generally accepted version is that the term "spam" comes from a Monty Python's Flying Circus skit. A group of Vikings in a restaurant sings a chorus of "spam, spam, spam . . ." in an increasing crescendo, drowning out other conversation. This is comparable to unsolicited email drowning out normal Internet communications.¹

What Is Not Spam?

Spam should not be confused with permission-based email marketing messages. There are legitimate marketing services that send messages to customers who have specifically requested to be notified of promotions, contests, sales, etc. Some marketers such as MyPoints and Yahoo provide services in exchange for a user agreeing to accept promotional email. Though these messages may have the exact same content as a spam message, they are not spam, because the user has agreed to receive them.

Do note that Yahoo has reset member's marketing preferences to accept all promotional mail. We would consider those messages unsolicited and unwanted, and therefore spam.²

Types of Spam

There are, of course, different types of spam. There is nuisance spam, which is mostly harmless except for the storage space and time wasted – something like the nonsense chain letters that Aunt Marge forwards – she just can't be convinced nobody wants to read them. System administrators may also have to deal with other types of inappropriate personal email that is outside the limits of the corporate messaging policy.

Also mostly harmless are commercial or promotional messages from legitimate marketers or companies with whom the recipient may have a relationship. However, if these messages are outside corporate policy, though they technically are not spam, system administrators may still treat them like spam as they take up bandwidth and storage space.

Then we have abusive spam, usually in the form of unsolicited commercial email sent to random recipients who have no prior relationship with the sender. Many of these messages are for dubious claims or outright fraud. Others may be obscene, violating corporate anti-pornography policies.

Abusive Practices of Spammers

Additional qualifiers that cause email to be identified as spam come from the practices of unethical marketers, called spammers (and worse) by the online community. *[Spammers] are the mutant spawn of a bizarre reproductive act involving a telemarketer, Larry Flynt, a tapeworm, and an executive of the Third Class mail industry.* -- Dave Barry³

These spammers abuse email by transferring the cost of sending unsolicited messages to ISPs, open relay mail servers, corporate messaging systems, and individual recipients.

Illegal, Unethical, and Immoral Content

Many spam messages contain blatantly illegal offers, scams playing on the recipients' gullibility, and even pornographic advertisements. Some spammers insist they won't market anything illegal or anything they don't believe will work – though few of the products advertised seem to be able to live up to their claims.

To Whom It Doesn't Concern

Spammers frequently send their messages to people who have expressed no prior interest in the products or services they are advertising. Spammers often work on a commission basis. A 1% response can be enough to turn a profit for a spammer, so the more messages they send the more money they could make.⁴

From a marketing service or advertising broker, spammers can purchase lists of email addresses for very little cost, one site lists 60 million email addresses for \$150⁵. It's also not difficult for them to find other marketers to trade address lists with, and to harvest addresses on their own.

It is easier for a spammer to send a message to 1,000,000 email addresses than it is to clean up a list or target specific recipients who have expressed interest.

DRAFT

Address Harvesting

Spammers send "spiders" or agents to scour websites, mailing lists and newsgroups for addresses. Even details from ICQ and other instant messaging programs are not safe. Sometimes this does allow for a bit more selectivity, perhaps only harvesting names from websites associated with golf to target a mailing about a marvelous new golf ball that guarantees at least 400 yards for every stroke.

Dictionary Harvest Attacks

Directory harvest attacks overwhelm mail servers, as spammers send variations of email addresses to a domain mail server – any addresses that don't bounce are considered valid and are added to their mailing lists.

These attacks can be recognized as a mail server generates an unusually large number of bounces in a short period of time, however there is not much that can be done to prevent dictionary harvest attacks.

Opting Out Brings More Spam

Recipients who click on a spammer's "remove me from this mailing list" links are often only confirming that they have a monitored email address, thus inviting more spam.

Setting Web Beacons

Web beacons are another way to verify active email addresses – if an HTML message is downloaded and rendered, even in preview mode, a web beacon tells the sender that the e-mail address is being used.

Using Open Mail Relays

Spammers often use insecure mail servers without the owner's permission to redistribute their spam, in effect stealing server resources. This practice can cause delays or disruptions in mail service, also known as Denial of Service attacks – the server is too busy processing spam to deal with regular mail.

Often spammers choose backup servers pointed to by secondary MX records; backup servers usually accept and relay all mail to the primary MX host without checking it.

"Drive-By" Spamming

An interesting new tactic is called drive-by spamming.⁶ Spammers drive around and find unsecured wireless networks. Sitting in a van with a laptop, spammers can send mail from "inside" the network to the SMTP server. Any messages sent by the spammer would appear to come from within the company's network.

Open Proxy Servers

Another way spammers exploit open relays is through insecure or misconfigured proxy servers. Proxies are normally set up for users in a network for control over internet access or to cache data for frequently used websites – properly configured, they route data from a LAN to the Internet. However if they are misconfigured, they may be able to route data from the Internet into a LAN, or perhaps to another part of the Internet. Using an open

proxy, spammers can find internal mail servers and use them to route mail, or they can anonymously abuse SMTP servers elsewhere on the Internet.

Proxy servers can be installed without administrator's knowledge. In January 2003, the virus Sobig.a was released. This virus downloads a Trojan executable that, as part of its payload, installs a specially modified proxy server that is hidden, runs on non-standard ports, and does not generate a log. It is not known whether this virus was developed by a spammer for practical reasons or simply by a hacker for malicious reasons.

In June 2003 up to 70% of spam was sent from hijacked machines, according to Mark Sumner, chief technology officer of MessageLabs Inc.⁷

Forged Headers and "Joe-Jobs"

Spammers often forge or tamper with the headers of email messages to conceal their identity and location, leaving some hapless admin at joesappliance.com to get a bunch of nasty emails complaining about the spam it looks like he sent. The practice of using a fake return address is known as a "Joe-job". A spammer may do this maliciously, in order to damage another company's reputation and possibly trick their provider into revoking their Internet access, or they may do it simply to hide their own identity. Joe-jobs are named after Joes.com, which was victimized in this way by a spammer some years ago.

"The Big Murkowski"

Spammers sometimes try to give their messages an air of legitimacy with text such as the following:

This message is sent in compliance of the new email bill section 301. Per Section 301, Paragraph (a)(2)(C) of S. 1618, further transmissions to you by the sender of this email will be stopped at no cost to you. This message is not intended for residents in the State of WA, NV, CA & VA. Screening of addresses has been done to the best of our technical ability. If you are a Washington, Virginia, or California resident please remove yourself. We respect all removal requests.

Or to make themselves less likely to receive negative responses, spammers may even sound a little threatening:

Under these provisions this letter can not be dealt with as spam and no further action can be taken by the reader against this company/person. Any report of this letter as spam to any independent agency or site is a violation of U.S. Bill S.1618 TITLE III of the U.S. Congress and will be dealt with promptly.⁸

Sorry, at this point there is no such law in the U.S. If this disclaimer is actually found in an email, it is obviously spam, and the spammer is trying to avoid complaints.

This practice is so prevalent it actually has a name, "Murk," as defined in the online Spam Glossary:

(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.⁹

The term comes from Frank Murkowski (R-AK), the senator who wrote S.1618. This would have made certain types of spam illegal, unless the message included full contact info at the start and made no attempt at hiding its origin.

Filter Busters

Spammers also add "filter busters" (strings of nonsense characters) to the subjects and bodies of their messages or send HTML graphics, in the hope of confusing filters that look for known spam messages.

Many spammers actually buy filtering software to test and fine-tune their messages to get around the filters.

DRAFT

Why Should We Be Concerned with Spam?

To some companies, spam is just a fact of life, accepted as an annoyance but basically ignored. Users simply delete their spam on a regular basis and work goes on. However, companies with this attitude do leave themselves open to wasted time, money, and resources, as well as legal risks.

A Radicati Group study concluded that 94% of companies consider spam to be a very serious problem, but 43% still do not have a formal anti-spam policy in place.¹⁰

Reasons to Stop Spam

Spam attacks disrupt electronic messages and transactions, impacting corporations' ability to do business.

Spam wastes system resources, including bandwidth, mail server processing cycles, and storage capacity. Spam can overwhelm mail servers that are not secured against relaying.

Spam wastes human resources; not just the time of employees who read and respond to spam, but that of system administrators, help desk staff, and human resources personnel as well.

Spam can violate corporate policies regarding non-business use of company messaging systems. Offensive or pornographic spam can also violate corporate anti-harassment policies. Content filtering can reduce the risk of legal exposure due to a 'hostile environment' when the contents of messages are offensive to employees.

Business-related messages and solicited advertising from legitimate marketers can get lost in the proliferation of unsolicited commercial advertisements and other spam.

Risks of Blocking Spam

However spam is filtered, false positives are a risk. A false positive is a message that has the characteristics of spam, but is actually a legitimate, solicited message. Business deals and important information can be lost because of a false positive.

Other than false positives, the only major risk of blocking spam is to be sued by the message sender or recipient on the basis of censorship or violation of personal privacy. It can be argued that a corporate mailbox is owned by the corporation; therefore all messages are subject to corporate policies.

The Costs of Spam

Fighting spam does have its costs, but allowing spam to continue to grow unchecked could be disastrous. Ferris Research stated that spam cost U.S. corporations \$8.9 billion in 2002, and \$2.5 billion for European businesses. These costs are roughly split between soft costs like lost productivity vs. hard costs like equipment, system administration, and help desk personnel.¹¹

DRAFT

Is it worth the cost to fight spam, vs. just accepting it as a side effect of using email?

Prices for anti-spam solutions start at about \$15 to \$20 per user.¹²

Vendors and researchers provide greatly varying results on the cost of spam per employee per year, from Ferris Research's \$168¹³ to Nucleus Research's \$874.¹⁴

The Radicati Group's "Anti-Spam Market Trends, 2003-2007" suggests that deploying an anti-spam solution is often more than 50% less costly than living without one.¹⁵

Is it worth the cost of additional software and hardware to filter spam, vs. the cost of additional software and hardware to process and store spam?

The Radicati Group's study, Anti-Spam Market Trends, 2003-2007, reports: "A 10,000-user company, running Microsoft Exchange 2000, is deploying an average of five messaging servers just to process spam in 2003, out of a total of 21 messaging servers. By 2007, if nothing is done to stop spam, this will spiral to 25 servers processing spam, out of a total of 50 messaging servers."¹⁶

In the US, The Radicati Group estimates that a company of 10,000 users with no anti-spam protection will spend an average of \$49 per mailbox per year processing spam messages in 2003.¹⁷

Is it worth the cost of a System Administrators' time to install and manage spam filters, vs. the time it takes users to sort out legitimate mail from spam?

Osterman Research reports that spam costs for an administrator run about \$15 per user per year.¹⁸

MessageLabs estimates spam costs over \$750 per user per year in wasted time alone.¹⁹

Is it worth the risk of losing business due to false positives, vs. the cost of receiving obscene material?

12% of spam received by Brightmail for June 2003 was "adult" in nature.²⁰ Users can lose their jobs for viewing obscene material at work, or be sued for sexual harassment. Companies can also be sued for allowing the messages to be delivered to the desktop.

These are questions each company must answer in the best interests of their business, though statistics indicate that the costs of spam are growing. Radicati suggests that the \$49 per user per year figure for 2003 will grow to \$257 per year by 2007.²¹

How Much Spam Is Out There?

What makes spam such a problem is the amount of it. Even with all the developments in anti-spam technology, spam is increasing at an alarming rate. Personal and business email inboxes are flooded with spam messages, and ISPs and corporate email servers have to cope with steadily increasing traffic.

Statistics do vary, but all agree that spam will only continue to increase.

DRAFT

In June 2003, almost 7.7 million different spam messages were caught by Brightmail's Probe™ Network, which has a statistical reach of 250 million mailboxes.²² For 2002, Brightmail had blocked more than 50 million spam attacks.²³

Brightmail projects that by September 2003, over half of the messages sent via the Internet will be spam.²⁴

At any given time, 5% to 30% of the email messages received at AOL are spam.²⁵ The AOL Time Warner Internet unit is blocking almost a billion unsolicited bulk e-mail messages every day.²⁶

Research Firm Jupiter Media estimates consumers will be inundated with 206 billion junk e-mailings in 2006, double the number received in 2002.²⁷

In a December 2002 study, the Gartner Group found that the junk mail rate for corporations is approaching 50% and continuing to rise.²⁸

The Radicati Group finds that one in three corporate email messages are spam; they expect this to rise to 39% by 2006.²⁹

Medium-size companies routinely get 20,000 spam messages per day, according to the Meta Group.³⁰

Brightmail estimates the average spammer sends 250,000 messages per day.³¹

DRAFT

What Can We Do To Minimize Spam?

There is no 100% effective solution to rid the world of spam, short of doing away with email altogether. We do have some suggestions to reduce the amount of spam received. Educating users is one part of the solution, and using technology to secure messaging systems and filter spam is another. Legislation will help provide guidelines, but won't have a big effect without heavy penalties and enforcement.

User Education

Teach users what is spam, and what is not. Any unsolicited mail they receive from a company with which they have no prior relationship is spam. Any messages from a list to which they have subscribed or promotional email they have agreed to accept in return for a service are not spam.

Educate your users about what they can do to minimize the possibility of spammers getting their email addresses, both corporate and personal. Teach them not to post email addresses on websites or newsgroups, or if they must, suggest they make their addresses "human readable," like leslie at jconsult dot com.

When users sign up for any online service, remind them to examine privacy policies, terms and conditions, and watch for any check boxes which would have the user agree that the website can share their email address with other marketing partners.

Make users understand it's useless to respond to spam, that in many cases "unsubscribe" links usually just confirm a live, monitored address. If the sender is a well-known organization with a good reputation, then unsubscribing should be a valid option.

If users need to share an email address with a marketer, suggest they create a "throwaway" account, and share their legitimate business and personal email addresses to those who will not abuse them.

Make users understand that if they never respond to spam, it makes it an ineffective way to advertise. If nobody ever bought anything a spammer marketed, they would all be out of business. Unfortunately, there will always be people out there who want a bigger waistline, and think that this "miracle product" will be the one that finally works.

If users really want to order a product that was advertised in spam, it is best to go to the web site without letting the vendor know that they came from the spam, i.e. don't click on anything in the message, but type the web address into the browser manually. (But remind them that they're supporting those who hire spammers.)

Do also inform them that nobody in Nigeria is really going to share \$240,000,000 just for the use of a bank account. (Believe it or not, the Nigerian advance fee scam is actually expected to gross \$2 billion in 2003, according to MessageLabs.³²)

Corporate Messaging Policies

Develop a corporate messaging policy that includes a definition of spam. Enforce it.

A "no personal use of the corporate messaging system" policy is one way to prevent spammers from getting addresses that are shared carelessly, and personal messages can open up legal liability depending on content. Also, employees are not wasting company time and resources for personal business. However, this is extreme; email is a valuable perk that some companies want to provide to their employees.

Technology Solutions

The first technological step to help prevent spam is to secure all wireless networks, proxy servers, and mail relay servers, so that spammers must use their own resources to send mail. This makes it easier to trace spammers back to their sources and complain to their ISPs or have them prosecuted in areas where the law allows. Spammer's accounts are more often closed due to breaking their ISP's Terms of Service, rather than any laws.

There are many different types of software that can detect and filter spam. These programs can be layered to make an effective system of spam filtering to maximize the number of spam messages blocked, while minimizing the number of false positives.

Spam can be filtered at the MTA or gateway level, when it is delivered to the server, or when it reaches the desktop. The closer to the perimeter, the less work the corporate messaging system has to perform.

Ideal solutions examine messages before they are actually brought into the messaging system to save processing and storage requirements.

Server solutions can quarantine messages at the incoming SMTP server level, which prevents further processing by other servers.

By the time a spam message reaches the desktop, it invalidates most of the reasons why spam should be filtered – the message has been processed and stored by the messaging system already, and user action may still be required.

Even with a gateway or server solution, the ability to tune filters on an individual level can be useful, especially since spammers often purchase off-the-shelf spam filters to develop messages that will get through the filters.

Ben Littauer, an independent consultant from Boston, recommends the "silver shotgun" approach: "If enough people are using enough different spam filters, then the number of spam messages that get through is greatly diminished. If fewer messages get through, the response rate is reduced and thereby the total revenues for a fixed-size mailing. If the response rate drops low enough, the mailing cost (though small) will eventually exceed the return and the spammer will stop. If everyone uses the same filtering approach, however, a spammer can "tune" the mailing to that filter and still get through. Thus I recommend that organizations and individuals use more than a single spam filter, and see standardization on a single filtering approach as helpful to the spammer."

Content Filtering

Content filtering examines messages to find phrases or patterns common to spam or messages that match a spam signature database.

Heuristic filtering is a statistical process that weights common spam phrases and characteristics and assigns a token or value to each one found in a message. If the

combined weight of the tokens exceeds a set limit, the message is tagged as spam. Heuristics understand spam, even if it's a first-time spam message not in a spam database.

Messages tagged as spam through heuristics may automatically generate rules to identify future spam. These products basically learn as they are used, and can be very effective at catching most spam.

Many content filtering products use databases of spam definitions provided by the manufacturer. They may scan messages by subject lines or specific phrases. These signature files are highly useful for catching known spam.

One way spam databases are created is using "honey-pot" systems, set up using decoy email addresses posted on websites or newsgroups. Any mail delivered to one of these addresses is going to be spam. Filters are created based on these messages.

These databases are delivered as updates to the clients. Some anti-spam packages make updates available every 10 minutes, which is close to real-time.

Content filtering can also be useful to block viruses before anti-virus vendors release pattern files. It reduces the risk of data loss and data exposure, as well as lost business.

It also can eliminate pornography and hate mail, which reduces legal liability, minimizes work place harassment, and diminishes inappropriate email usage.

Of course content filtering isn't that useful for foreign-language spam.

Content filtering has one major drawback – it cannot differentiate between solicited and unsolicited mail based simply on the content of a message. Many content filtering packages include an option to allow mail from specified senders to be added to a whitelist, allowing the messages to be delivered no matter what the content.

Blocked messages should be examined, especially when a spam filter is first installed. Some programs use a quarantine folder, giving access to either an administrator or the users. This means a human must spend time scanning the filtered mail to make sure nothing legitimate has been misfiled.

Pattern Recognition and Header Analysis

Pattern recognition and header analysis can be used to filter messages with inconsistencies in headers such as forged information and envelope characteristics or patterns common to spam, such as delivery paths using multiple servers or a large number of recipients.

This type of filter is useful for poorly forged messages; however it can cause delivery failures of legitimate messages if a company uses a circuitous route to send SMTP mail, adding to the hop count and perhaps going over the limit of the spam filter.

Reverse DNS and Address Verification

Reverse DNS lookups and address verification can catch inconsistencies in messages, but they use a large amount of resources and also run a high risk for false positives.

Not all companies have their outgoing MX server listed in their DNS, which could cause legitimate mail to be filtered.

RealTime BlackHole Lists

Some spam filtering applications use realtime black-hole lists (RBLs) or blacklists, which are a fairly clumsy form of filtering, based on IP addresses. RBL's don't let spam servers connect to your mail servers.

Realtime Blackhole Lists are maintained by various administrators who hate spam. RBLs use different criteria to add IP addresses to their lists. Some go by whether a server is an open relay or open proxy, others by whether the list administrator has received reports of spam being sent by a particular server or ISP, and others just by whomever the administrator is not happy with that day. Mail system administrators who are considering using RBLs should fully understand what qualifies an entry to be added to the list before subscribing.

This type of filter runs a huge risk for false positives, as an ISP may play host to legitimate users as well as spammers. David Nelson, a senior industry analyst at Giga Information Group, says a recent study found that MAPS blocked 24% of spam with 34% false positives. This hurts all legitimate internet mail users.³³

If you have open relays in your environment and they are discovered by spammers, you may be added to a blacklist. They're not always easy to be removed from.

"Domain Name Service-delivered Blocking List" (or "DNS-delivered Blackhole List") is a type of blackhole list, using DNS rather than IP addresses.

One of the worst things about lists of servers with open relays is that spammers sometimes use them to find more servers off of which to relay their mail.

Whitelists and Certification

Whitelists work on a similar principle to blacklists, except that servers on the list are sending messages that are certified to not be spam. The lists can contain individual email addresses, or lists of domains or ISPs with "no-spam" policies.

Several consumer and marketing groups are developing whitelists based on their certification standards. They make these lists available, usually for a fee.

According to field tests of 40,000 consumers by a large consumer company, there was a 52 percent improvement in click-through rate per delivered email for messages containing a Trusted Sender trust stamp, versus the same message without a stamp.³⁴

Habeas is one company providing certification. Their Habeas Sender Warranted EmailSM program inserts a haiku and special text headers in outbound email that has been certified by Habeas as 'not spam'. Anti-spam filters can be programmed to recognize the headers and allow the message to be delivered.

X-Habeas-SWE-1: winter into spring

X-Habeas-SWE-2: brightly anticipated

X-Habeas-SWE-3: like Habeas SWE (tm)

X-Habeas-SWE-4: Copyright 2002 Habeas (tm)

X-Habeas-SWE-5: Sender Warranted Email (SWE) (tm). The sender of this

X-Habeas-SWE-6: email in exchange for a license for this Habeas

X-Habeas-SWE-7: warrant mark warrants that this is a Habeas Compliant

X-Habeas-SWE-8: Message (HCM) and not spam. Please report use of this
X-Habeas-SWE-9: mark in spam to <<http://www.habeas.com/report/>>.

Habeas also maintains a DNS-based whitelist of IP addresses of Habeas bulk mail licensees and other enterprise and individual licensees who use confirmed opt-in and meet all other standards for a Habeas Compliant Message.

Greylists

Greylisting is a recently proposed method that filters spam at the Sendmail MTA level, so there is no network traffic other than the connection. Greylisting looks at the IP address of the host attempting delivery, the envelope sender address and the envelope recipient address. If none of these three qualifiers is in the greylist database, the message is refused with a temporary failure. A properly configured SMTP server will retry after a specified time period – spamming software generally does not. Greylisting is not intended to replace other methods of spam filtering, but it is an addition that can reduce spam processing. In testing, this method blocked 97.4% of spam with no false positives.³⁵

Do-Not-Spam Lists

The FTC is developing a Do-Not-Spam-List for marketers. However, unethical spammers may not bother to take the time to clean up their lists, or even worse, use those lists as new addresses to spam. The FTC will most likely put honey-pot addresses on the list, and aggressively go after those who do spam them.

Some marketing firms such as the Direct Marketing Association (DMA) have similar lists.

Peer to Peer Reporting

In peer to peer reporting, or collaborative filtering efforts, users tag messages as spam, and the anti-spam program forwards a copy to a system administrator. These messages are added to the program's database and pushed to the other users of the package. A risk with peer to peer programs is that users may tag mail as spam when the message was something they once subscribed to. This can be a final step in the message screening process, though it is more of a community service than any type of resource or time-saving measure for the corporation.

Challenge/Response Systems

Some desktop users favor challenge/response systems, which give them much more control over their email. Any message received from a sender not listed on an "approved" list gets an automated reply requiring the sender to type a code shown in an attached graphic. This requires a human response. If the code is correct, the message is delivered.

This does put quite a bit more work on the part of the legitimate sender to get their message delivered, and it's also going to result in delayed mail if the sender doesn't see the challenge right away. Spammers don't generally even see these challenges, and for the small number of messages that will be blocked this way, they have another 999,999 addresses on their mailing list anyway.

DRAFT

Technology Summary

There is no one technology solution, but a layered approach using several of these methods can be very effective at weeding out spam.

Legal Options

The legal situation is very fluid. At this point many countries are developing enforceable financial and legal penalties for spammers, though a global standard will most likely be necessary to have a real effect.

European Legislation

The European Union's Privacy and Electronic Communications Directive comes into force on 31 October 2003, and makes sending of unsolicited email to an individual illegal unless they specifically request it. This ban does not apply to existing customer relationships, so retailers may continue to send marketing messages to consumers, as long as they provide an opt-out feature. The definition of electronic mail is broad enough to also cover text-messaging systems such as mobile telephones. The EU member states must pass this regulation individually as part of their own national laws, which could take years.

The United Kingdom government is considering exempting business email accounts from this directive, which would make it legal for spammers to continue to send spam to business addresses. "Many people feel strongly that anti-spam measures could hamper business-to-business [B2B] commerce. Others feel equally strongly that unsolicited email is just as big a problem for businesses," Timms explained at the Spam Summit at the House of Commons.³⁶

United States Legislation

In the US, there is no federal legislation, though there are nine bills pending as of July 2003.

At the present time, the only US Federal Government agency that is taking any action against spam is the Federal Trade Commission (FTC). However, the FTC is only taking action when the email messages contain evidence of fraud or illegal activity. The FTC does not take action against ordinary unsolicited commercial email. The FTC receives about 130,000 forwarded spam messages a day at uce@ftc.gov, the agency's unsolicited commercial email mailbox.³⁷

Many individual states have enacted anti-spam laws, though enforcement has been sporadic at best.

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 as long as they feel they won't be punished seriously.

However, a recent Virginia law may make them reconsider: certain types of spam can be punishable with up to five years in prison, and the forfeiture of all profits earned from the deceptive solicitations, as well as all computer equipment, computer software and all personal property used in connection with the illegal act.³⁸ This law doesn't apply only to mail originating in Virginia, but any message that passes through any server in Virginia.

Most spammers that have been prosecuted in the United States have not found themselves in trouble for sending spam, but rather for the methods they use to send spam. Howard Carmack, aka the 'Buffalo Spammer', was arrested and arraigned in New York for credit card and identity theft, not for the 825 million unsolicited e-mails he allegedly sent.³⁹

Spammers often use overseas servers in countries with no anti-spam legislation such as China and Korea, so they don't have to worry about US laws, even though it raises their costs significantly.

Proposed Rules for Fair Spamming

Common suggestions for legislation include:

- Making it illegal to falsify the routing information of the e-mail message.
- Failing to honor "opt-out" requests, or failing to include opt-out instructions.
- Failing to identify a message as an advertisement through the use of the "ADV," "ADV-ADULT" or "ADVERTISEMENT" labels at the beginning of the subject line.

Ron Scelson, aka The Cajun Spammer, brings up a valid point – if he obeys the proposed laws and uses a marker such as 'ADV:' in his subject lines, then spam filters block his messages. He proposes that if advertising messages are sent within the limits of the law, spam filters should allow them to be delivered, and that will bring more email marketers into compliance.⁴⁰

Spammers Rights Under the Law

Spammers raise the issues of censorship, claiming they have the right to send their messages under the first amendment.

A group of spammers in Florida, "E marketers America" is suing anti-spam organizations SPEWS, The Spamhaus Project, and Joker.com, claiming they are destroying spammers right to market via the Internet.

Self-Regulation of Legitimate Marketers

Marketing companies and organizations are working to develop their own guidelines and policies regarding what is and is not spam, perhaps hoping that if they regulate themselves, there will not be a need for federal legislation.

The Email Service Provider Coalition (ESPC), formed by the Network Advertising Initiative, is a coalition of e-mail service providers that plans to develop registries to certify legitimate email marketers from spammers. Marketers performance would be rated as a way to remain on the registry, which the ESPC hopes companies will adopt as a whitelist. Marketers would be evaluated and given a score somewhat like a credit rating based on customer complaints, how many times people have to unsubscribe and other factors.

There are disagreements between marketers and anti-spam activists about where the lines are to be drawn.

The Direct Marketing Association (DMA) is the oldest and largest marketing trade association in the United States. The DMA's Commercial Solicitations Online Guidelines approved in January 2002 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 when offered the chance. Each solicitation should include a link to request removal from the marketer's mailing list, and a link to request that the email address not be shared with other marketing organizations for online solicitation if the marketer does provide such a service. The DMA does provide an Email Preference Service suppression file for members to use to filter email lists.

While some anti-spam activists feel these guidelines are fair, many others do not agree that a prior business relationship is enough to justify sending marketing messages; they believe if a customer hasn't specifically agreed to accept promotional email from a company, it is spam.

Many activists believe legitimate marketers should adopt an "opt-in" policy, where users should not be contacted unless they have requested to be added to a mailing list via a company's website, a contest entry blank, or some other medium. They believe it is not appropriate to put the onus on the recipient to opt out. Lack of response does not indicate consent.

While self-regulation is one possible solution to reduce spam since legitimate marketing firms will abide by the guidelines, but spammers will continue to abuse this medium until it becomes unprofitable. The best way to get rid of spam is to discourage spammers from sending it. The bottom line here is money – if they don't earn enough from sending spam, or if they have to pay for their abuses, they'll be forced to find other ways to make money.

DRAFT

Best Practices

There are several steps we recommend all corporate messaging systems take to help eliminate possible delivery routes for spam.

- Secure SMTP servers by either disallowing any external relay, or requiring authentication.
- Verify proxy servers are configured to only route traffic from the LAN to the Internet.

Other recommendations are to minimize the amount of spam received by individual corporations.

- Use a content filter that subscribes to a regularly updated database of spam. Quarantine all filtered messages at first, and examine them to fine-tune the system to avoid false positives.
- To block directory harvests, do not post member or employee databases on corporate websites.

The Ideal Spam Filter

The ideal spam filter will have the following features:

- Easy installation and administration
- High level of flexibility and customization
- High filtering rate – 90% or higher
- Extremely low false positive rate
- Filtering at the perimeter of the messaging system
- Little impact on email delivery times or server performance
- Automatically updated database of confirmed spam
- Rules and heuristic scoring system for new spam
- Ability to teach itself what is and is not spam
- Customized white lists
- Access to quarantine folder for either administrator or users
- Integration with anti-virus filtering

Make sure you understand the filtering criteria used, and tune it to an appropriate level for your organization.

DRAFT

Summary

To continue to leverage our investment in email, we need to minimize the amount of spam that gets transmitted and received through messaging systems. The less spam delivered means the less chance for a spammer to profit, and spammers will not give up on sending spam until they stop making money.

The measures required to fight spam can be quite frustrating – there is no simple solution, but there is some relief in sight from better filtering technologies, certification systems under development, and potential legal remedies applied on a global scale

Please email questions or comments to Leslie Ogonowski of Johnson Consulting at leslie@jconsult.com.

DRAFT

DRAFT

References

-
- ¹ Hormel Foods, *Spam and the Internet*, http://www.spam.com/ci/ci_in.htm
 - ² Yahoo Resets Member Spam Preferences, <http://www.pcworld.com/news/article/0%2Caid%2C91984%2C00.asp>
 - ³ 7/14/02 Miami Herald Newspaper (Miami, Florida USA)
 - ⁴ 6/25/03 Interview with Ron Scelson and Intellireach, <http://www.intellireach.com/events/0625w.html>
 - ⁵ 60 Million Fresh Email Addresses + Opt-Ins, <http://sources.redhat.com/ml/crossgcc/2001-09/msg00015.html>
 - ⁶ "Drive-by spam hits wireless LANs" by Graeme Wearden CNET, <http://news.com.com/2100-1033-956911.html>
 - ⁷ "SoBig spam-virus still spreading" by Bob Sullivan, MSNBC, <http://www.msnbc.com/news/931205.asp>
 - ⁸ http://www.internet-tips.net/Email/SPAM_1618.htm
 - ⁹ <http://www.rahul.net/falk/glossary.html#murk>
 - ¹⁰ <http://www.radicati.com/pubs/news/03AntiSpamPressRelease.pdf>
 - ¹¹ http://www.usatoday.com/tech/news/2003-01-03-spam-costs_x.htm
 - ¹² <http://www.radicati.com/pubs/news/03AntiSpamPressRelease.pdf>
 - ¹³ http://www.postini.com/services/roi_calculator.html
 - ¹⁴ http://www.out-law.com/php/page.php?page_id=spamcostsusemploy1057164330&area=news
 - ¹⁵ <http://www.radicati.com/pubs/news/03AntiSpamPressRelease.pdf>
 - ¹⁶ <http://www.vnunet.com/lite/News/1141508>
 - ¹⁷ <http://www.radicati.com/pubs/news/03AntiSpamPressRelease.pdf>
 - ¹⁸ <http://www.serverwatch.com/tutorials/article.php/2224841>
 - ¹⁹ <http://www.theregister.co.uk/content/6/22636.html>
 - ²⁰ http://www.brightmail.com/spamstats.html#spam_categories
 - ²¹ http://www.radicati.com/cgi-local/brochure.pl?pub_id=202&subscr=&back_link=/single_report/
 - ²² <http://www.brightmail.com/spamstats.html>
 - ²³ Brightmail Reveals Annual Top 10 Spam Messages for 2002, http://www.brightmail.com/pressreleases/121202_top_spam.html
 - ²⁴ Spam On Course to Be Over Half of All Email This Summer, <http://www.brightmail.com/press-releases.html>
 - ²⁵ AOL spam dispute escalates, CNN Interactive, <http://www.cnn.com/TECH/9712/31/aol.addresses/>
 - ²⁶ AOL: Spam Problem Is Getting Worse, Internet Advertising Report, <http://www.internetnews.com/IAR/article.php/2091641>
 - ²⁷ The Anti-Spam Cookbook, Network Computing, <http://www.networkcomputing.com/1320/1319f3.html>
 - ²⁸ Study suggests spam-stopping tricks, CNET News.com, <http://news.com.com/2100-1024-993333.html>
 - ²⁹ The Anti-Spam Cookbook, Network Computing, <http://www.networkcomputing.com/1320/1319f3.html>
 - ³⁰ The Anti-Spam Cookbook, Network Computing, <http://www.networkcomputing.com/1320/1319f3.html>
 - ³¹ Living in 'Spammed' times, Internet.com. http://asia.internet.com/asia-news/article/0,3916,161_1436501,00.html

³² Spam and Virus "Blended Threats" Top E-Mail Dangers in 2002, Advisor.

<http://marketingadvisor.net/doc/11611>

³³ The Spam police, Network World.

<http://www.nwfusion.com/research/2001/0910feat.html>

³⁴ Spam by the Numbers, ePrivacy Group. <http://cobb.com/spam/numbers.html>

³⁵ The Next Step in the Spam Control War: Greylisting, by Evan Harris.

<http://projects.puremagic.com/greylisting/>

³⁶ New laws will make it 'legal' to spam your work address, Silicon News.

<http://www.silicon.com/news/165/1/4970.html>

³⁷ FTC finally realises that spammers lie, ZD Net UK News.

<http://news.zdnet.co.uk/story/0,,t269-s2134105,00.html>

³⁸ Virginia Seeks Jail for Spammers, Internet Advertising Report.

<http://www.internetnews.com/IAR/article.php/2199001>

³⁹ 'Buffalo Spammer' Arrested, InternetNews.com.

<http://www.internetnews.com/xSP/article.php/2206311>

⁴⁰ Interview with the Spammer, Intellireach Webcast.

<http://www.intellireach.com/events/index.html#0625>

DRAFT