Spam

The low cost of electronic communications has both benefits and drawbacks. Most of us take for granted, and gladly take full advantage of the ability to send a written communication delivered directly to the desktop of our correspondent thousands of miles away in a matter of seconds at negligible cost, using email software. What many of us are beginning to discover, however, is that there are hundreds of thousands of marketeers out there who want to send written communications to our desktops at a negligible cost. These unexpected, unsolicited and often intrusive emails are referred to as Spam.

This document is intended to help you understand how to stop spam email with or without the use of an email spam filter or DNS blacklist. We are presenting this information in a Q&A (Questions and Answers) format that we hope will be useful. Our knowledge of this subject relates to Internet connectivity in general, and stems from our own TCP/IP networking technology and experience. We welcome feedback and comments from any readers on the usefulness or content.

We are providing the best information available to us as of the date of this writing and intend to update it at frequent intervals as things change and/or more information becomes available. However we intend this Q&A as a guide only and recommend that users obtain specific information to determine applicability to their specific requirements. (This is another way of saying that we can't be held liable or responsible for the content.).

Questions

1. What is Spam?

The term Spam refers to unsolicited, unwanted, inappropriate bulk email, Usenet postings and MUD/IRC monologs. For the purposes of this discussion, we will use the term Spam primarily in reference to email, which is what it is generally understood to mean when used in connection with the Internet. Spam is often referred to as Unsolicited Bulk Mail (UBM), Excessive Multi-Posting (EMP), Unsolicited Commercial email (UCE), spam mail, bulk email or just junk mail.

2. When is Spam Spam?

Exactly where to draw the line between Spam and legitimate email or spam free bulk email is not as obvious as it may seem. To some, any and all email that does not come from an approved source is Spam. According to Mail Abuse Prevention System (MAPS) www.mail-abuse.org:

An electronic message is "spam" IF: (1) the recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients; AND (2) the recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be sent; AND (3) the transmission and reception of the message appears to the recipient to give a disproportionate benefit to the sender.

MAPS' definition of Spam goes on to say that whether the email is relevant, or whether the benefit to the sender is disproportionate is up to the recipient and not open to discussion. If this is the case, then Spam isn't Spam until the recipient decides it is. However, point (2) above really only makes sense when interpreted in the context of bulk email sent to subscribers. As often as not, the first email you ever send to someone has not been "authorised" since you have never exchanged emails. Further, MAPS goes to considerable length to define "strong terms and conditions prohibiting [email users] from engaging in abusive email practices". These terms and conditions deal exclusively with bulk email sent to lists of addressees. In other words, they want their users to send spam free bulk email. This underlines the generally accepted principle that for Spam to really be Spam, it has to be bulk email. This definition is reinforced by Henry Neeman's "Why Spam is Bad" - a thoroughly enlightening read. Mr Neeman explains to a particularly dense group of spammers, entirely in single syllable words that "Spam is the same thing lots and lots of times."

To learn more about how to stop spam mail and block junk email with a junk email filter or anti spam program, read on.

3. Where does the term "Spam" come from?

The prevailing theory is that the term refers to a classic skit by Monty Python's Flying Circus. In the skit a couple in a restaurant tries in vain to order something that does not have SPAM in it. As the waitress lists endless dishes, all of them containing increasing amounts of SPAM, a group of Vikings in the corner begin to sing "spam, spam, spam, spam…" until all useful information is drowned out. But where did the connection between unwanted SPAM and unwanted Spam come from?

It did not start with email. The term has it roots, in relation to the Internet, in the late 1980s or early 1990s in Multi-User Dungeons (MUD) and Multi-User Shared Hallucinations (MUSH). MUDs and MUSHes are online, real-time, interactive, text-based virtual environments. According to one source, a MUSH user programmed a macro key to type "spam spam spam…" in a MUSH until his connection was terminated by a SysAdmin. He was subsequently referred to as “the !*%@ who spammed us” by other members. From MUDs and MUSHes the term Spam began to be used to describe Excessive Multi-Posting (EMP) on Usenet groups. Usenet “news” groups are forums where “authors” can “publish articles” to be read by other users and subsequently discussed. Not much of what gets “published” could ever be considered “news” by any reasonable standard of measure, but the original term is still used today. Under normal circumstances a user would post a message to one or to a small number of relevant newsgroups, asking questions or airing opinions. By using software to automate the process of posting, it became possible to post the same message to thousands of newsgroups ensuring a readership in the hundreds of thousands or even millions.

The very first Spam email was sent on 1 May 1978 by a Digital Equipment Corp. sales rep advertising a computer equipment demonstration. An attempt was made to send this email to all of the Arpanet users on the west coast of the US. The reaction on the part of the recipients was not unlike what you may expect today. Remember that Arpanet was a military project and commercial use was not acceptable. At the time, there was no such thing as an email Spam filter to stop Spam mail because there was no Spam. In April 1994, the Phoenix law firm, Canter and Siegel, advertised their services by posting a message to several thousand newsgroups. This was probably the first automated large scale commercial use of Spam, and was the incident that popularised the term, which up until then had been exclusively part of the arcane vocabulary of Multi-User Dungeons.

4. Why do people send spam?
Spam is the electronic equivalent of junk mail. People send Spam in order to sell products and services or to promote an email scam. Some Spam is purely ideological, sent by purveyors of thought. The bulk of Spam is intended, however, to draw traffic to web sites or to sell sex and money making schemes. Unlike junk mail in your physical mailbox, Spam does not abait if it is unsuccessful. When marketing departments send junk mail at considerable expense, without success, they generally cease, or try a different sales pitch. Spam on the other hand can be entirely unsuccessful, but the large number of wannabe spammers waiting in the wings ensures that we will continue to receive lots of it.

Spammers go to considerable effort to thwart recipients’ attempts to stop spam email. They specifically design their emails to bypass your email spam filter.

5. How can I tell who the spam is from?
Normally you cannot. Spam control can become very sophisticated. More experienced users can look at the email “headers” to find the origin of the message but frequently the spammer will set up a one-time email account purely to initiate the spam email shot. When the email shot is finished, the account is closed. At other times, the spammer will forge headers making it difficult or impossible to trace the origin of the Spam, so finding the original sender will very often prove fruitless. Spam protection and junk email prevention require more subtle measures than just finding the culprit.

6. How do spammers get my email address?
Through many means. Some companies you may have had dealings with sell their mailing lists to third parties, spammers included. Spammers also use “robots” to scour the Internet and

harvest any email addresses that they find. If you post to newsgroups you are also at risk of spammers picking up your email address and sending you junk email. To get adequate spam protection and get rid of Spam, you really need more than one email address. This is an essential element of proper Spam control.

7. If I unsubscribe won't it get rid of spam?
If you didn't have to subscribe to get it, there is little chance that unsubscribing will get rid of Spam. Professional spammers (something about those two words in the same phrase doesn't seem right, but I digress…) use this trick to validate their email address list. They buy or steal lists sometimes containing millions of email addresses. Large percentages of these addresses may be invalid. By unsubscribing to the list, you are informing the spammer that your email address is a good one, and may be sold on to other spammers. Be prepared for more Spam, from many more sources. A better alternative would be to try blocking Spam, or to bounce Spam email using specialized email software.

8. Isn't Spam illegal?
Clearly Spam is illegal if it promotes an illegal product or service. However, spam legislation is pending in the US and in Europe that would make the mere act of sending unsolicited commercial email illegal in the absence of an existing business relationship. The Coalition Against Unsolicited Commercial email (CAUCE) applauds the tough proposed European legislation, but opposes the proposed US anti spam legislation which it considers weak and ineffective at stopping spam. Bill S 630 would establish UCE as a legitimate practice. The onus would be upon the recipient to "opt out" of the mailing list by unsubscribing. In the event of non-compliance on the part of the spammer, it would be up to the ISP to trace them and take action (most end-users lack the sophistication to trace an email back to a physical real-world company or individual). Fines of up to $10 per illegal Spam would be levied. The CAUCE argues that since the Federal Trade Commission (FTC) is the only enforcing body, given the large number of Spam emails it is unlikely that any serious enforcement would ever take place. CAUCE takes the position that the recipient's email resources are private property and likens UCE to placing advertising billboards on their property at no charge.

Proposed European legislation is much tougher and many believe it would help get rid of Spam. It will require prior consent from the recipient before receiving unsolicited commercial electronic communications including SMS, fax and email. The directive has already been published in the Official Journal of the Economic and Monetary Union and is expected to be implemented in member states by 31 October 2003.

9. How big of a problem is spam?
Big. Spam is a big problem first of all because it is symptomatic of inefficient, parasitical businesses. The Nobel Prize winning economist Ronald Coace in what is now known as the Coace Theorem postulated that an inefficient business (one that cannot bear the cost of its own activities) is dangerous to the economy, because to function, it must spread the cost of its activities across a large number of victims. The Coace Theorem cuts close to home where Spam is concerned. Any business that needs to send Spam emails to survive is not a viable business. The benefit to the spammer is disproportionate to the cost borne by the spammer,

which is next to nil. More importantly, the cost of Spam removal to the victims is totally disproportionate to the benefit to the spammer. In a free market economy such a grossly inefficient process should cease when property rights are enforced (i.e. the cost is borne by the the party who incurs them).

Spam is a big problem because property rights are difficult or impossible to enforce which makes it hard to get rid of Spam. From the 1800s through the mid 1960s industrials considered it their right to produce and pollute with impunity. The economy could not run without their products. They could not afford to not pollute. It took over two decades of lobbying to move government and industry to another point of view. Yet these were reasonable businesses, with physical assets in the countries of their victims and subject to their legal systems. Consider the spammers in contrast. Any physical assets they may have are irrelevant to their activity, which incidentally, has no borders. They are not subject to the legal systems of their victims. If they become subject to legislation attempting to stop Spam they can find a more favourable environment in another country. The immediate effect of the new European legislation will be to force the spammers offshore rather than to stop junk email. There will be less Spam coming from European countries, but there will not necessarily be any less Spam.

Spam is a big problem because of the shared resources it consumes. Internet Service Providers (ISPs) allow you to surf the Internet, and deliver your email to your email software usually for a flat monthly fee. They must, in turn, purchase bandwidth (the technical term for their own connection to the Internet). The more users they have, the more bandwidth they need. If they have very large numbers of users they may need to purchase additional servers to manage email. These costs are offset by the added revenues of a larger user base. Spam however, increases their need for bandwidth, and increases the load on their email servers with no added revenue to compensate. The added cost must be passed on to the customers, the victims of spammers trespassing on their private cyberproperty. Some very large email servers have been shut down due to Spam overload for extended periods depriving hundreds of thousands of paying customers of their emails. One leading ISP processes about 30 million email messages a day, 30% of which are Spam. The problem of Spam has reached proportions where it threatens the viability of email and of the Internet itself.

Spam is a big problem because of the private resources it consumes. Many business people spend up to fifteen minutes per day reading and deleting their Spam emails. A company with 100 knowledge workers earning an average of $40,000 per year each spending ten minutes per day deleting Spam would experience an added burden of $80,000 per year. This cost would be passed on to Internet users and non-users alike as they purchase products from this company at their local department store.

Spam is a big problem because of number of victims it involves. According to META Group, 5-15% of corporate email is Spam. This is expected to grow to to 15-30% in the near term. This means that the average medium-sized company receives 20,000 Spam emails per day. Taking the above example a little further, if 10 million people each lose 5 minutes a day deleting Spam, in terms of productivity, this could cost the global economy over $4 billion annually, not counting wasted bandwidth, CPU time and network administration time and tools. Based on these assumptions, the global cost of Spam may well be over $5 billion annually.

10. What are DNS blacklists?
DNS blacklists are lists of domains that are known to originate Spam. Many anti-spam software programs use these lists to control Spam by refusing any email that originates from one of these domains. DNS blacklists are usually maintained by anti-spam organizations or by individuals with an intense dislike for Spam. The difficulty with DNS blacklists is the need for objectivity in deciding when to blacklist a domain. In order to know that a domain is producing Spam, the offence must be reported. Reporting Spam without any anti-abuse mechanism in place, however, leaves nothing to stop people from getting servers added to a DNS blacklist out of malice. The obvious solution would be to require a minimum number of reported incidents before blacklisting a server. This proves equally unsatisfactory however as a measure to stop Spam mail. Anyone who manages large mailing lists knows that a small percentage of people who subscribe subsequently accuse the sender of spamming them when they receive their email. Naturally, a company that sends out millions of legitimate commercial emails will receive more accusations of Spam than one that sends out a smaller amount of spam free bulk email.

The real solution lies in good management. A system administrator that knows about Spam, that knows who the large legitimate bulk mailers are and responds rapidly to complaints from unjustly blacklisted domains will ultimately provide a useful service to the Internet community at large. There are some well-managed DNS blacklists on the Internet and these can be a useful addition to the feature set of anti spam software. Below is a short list of the better known sites:
Realtime Blackhole List
Spam Cop
Spews.org
Open Relay Data Base
Monkeys.com
Rfc-ignorant.org

11. What is an open relay?
Anyone who has travelled a lot has experienced the following: You check into your hotel. You connect to the Internet using the Ethernet socket in your hotel room. You try to send an email to the office, and your email client refuses saying “relaying denied”. What happened? Suppose your email address is you@foo.bar. Your regular email server, which may be named mail.foo.bar, knows all of the IP addresses of all of the machines connected to the Internet via the foo.bar domain. Should the mail.foo.bar forward email coming from another domain than foo.bar, this is referred to as “relaying”. Most ISPs do not allow relaying of email from untrusted domains, indeed from any domains but their own. Your laptop computer was using an IP address allocated by your hotel’s DHCP server. Mail.foo.bar did not recognize this IP address, and refused to relay. There are a lot of poorly configured email servers however, that will let anyone use them to send email. An open mail relay becomes a channel for Spam, virtually “hijacked” by unscrupulous spammers who send large numbers of emails through them until they are discovered and banned, and move on to another open relay. Early versions of certain email servers did not stop spam email , but defaulted to open relaying when set up, so that there are many open relays available to spammers today. Recent versions of most email server products default to denying relaying in order to block junk email.

12. How can I stop Spam email?

There are a number of things you can do to stop Spam email. Which ones suit you best will depend upon your needs, the type of email you generally receive, whether you have complete control over your email account, the number of legitimate correspondents you may have and how long you tend to keep them.

Scenario A.

Joe runs a small business. He regularly exchanges emails with about 50 business contacts. He also uses the Internet extensively to order goods or information, to book events and travel and to make new business contacts on newsgroups. Currently, over one half of his email is Spam. He can delete it fairly quickly, but it gets on his nerves. The first thing Joe can do to get rid of Spam is change his email address and inform his regular colleagues. Next, he can get a second, web-based email address at no charge from one of the many providers of this type of service. He can use his web email address when entering information into online forms or when dealing with any untrusted third party, knowing that this is the address that will be likely to get more Spam. When it starts to get too much Spam, he can simply change it without having to inform anyone. Lastly, Joe can use the Spam filters in his email client software to filter out any obvious Spam that manages to get through. Optionally he can use dedicated anti Spam software to block Spam.

Scenario B.

Annette works in the customer service department of a large organization. Unlike Joe, Annette receives large numbers of legitimate emails from people with whom she has had no previous contact. It would not be feasible for Annette to change her email address and inform all of her correspondents. Furthermore, all of the email addresses in Annette's organization have the same format: firstname.lastname@organization.tld. Annette receives over one hundred emails per day, of which typically sixty are Spam. Annette needs to talk to her email administrator to discuss the problem, which plagues many of her co-workers as well. The ideal long-term solution for Annette's organization would be to install a server based anti Spam software with rules that can be modified for users and groups of users. Email users in Annette's service may have slightly different needs than users in human resources or in the legal department. In the meantime, Annette can probably lower her Spam workload substantially without filtering out legitimate customer email. By using the filters in her email client to examine the sender email addresses and subject fields of the Spam she receives, she can quickly identify keywords that will enable her to filter out most of the obnoxious Spam messages. This is not a good long-term solution, but will help her to cope until her email administrator implements something better.

Scenario C.

Jean is head of IT in a middle school. She wants her students to use the Internet for research, become fluent in IT and be able to receive emails from legitimate sources. She already has a web content filtering system in place, but has no means to ensure that students do not receive inappropriate emails. Unlike Annette's organization, which would rather let the odd Spam message get through than accidentally prevent legitimate customer emails from reaching their destination, Jean's school cannot allow any inappropriate email to reach the students, even if this means blocking the odd legitimate message. Jean needs a server based solution that meets the following requirements: a) it must filter all email regardless of what email server it came from, b) it must quarantine suspect emails, allowing authorised personnel to flag individual mails as legitimate and c) it must have a variable threshold allowing the administrator to increase the level of severity in the event that marginal but bad emails actually reach their recipients.

There are many ways to stop Spam. One or several may be right for you. This will depend on a variety of factors as the above scenarios suggest.

13. How does an email Spam filter work?
For most email users, using an email Spam filter to get rid of Spam is the only viable alternative to manually sifting through large numbers of junk email every day.

There are different kinds of filters:
User defined filters are included in most email clients today. With these filters you can forward email to different mailboxes depending on headers or contents. For example, you would put email from each of your friends into a mailbox named after them. You can also use these same filters to forward email to the trash if the origin or contents are suspicious. To do this you need to carefully look at any Spam emails you receive. Try to notice common characteristics, recurring patterns in senders' email addresses, dubious claims in the subject line and so on. You will soon find that Spam filtering using a small number of rules can eliminate a large number of Spam emails.

Header filters are more sophisticated. They look at the email headers to see if they are forged. Email headers contain information in addition to the recipient, sender and subject fields displayed on your screen. They also contain information regarding the servers that were used in delivering your email (the relay chain). Many spammers do not want to be traced. They put false information in the email headers to prevent people from contacting them directly. Some anti spam programs can detect forged headers which are a sure indication that the email is Spam. Not all Spam has forged headers though, so this filter by itself is not sufficient.

Language filters simply filter out any email that is not in your native tongue. It only filters out foreign language Spam, which is not a major problem today, unless the foreign language in question is English. In future, languages other than English are expected to make up an increasingly large percentage of Internet communications. If you do not expect to get emails in another language, this may be a quick and easy way to eliminate some portion of your Spam.

Content filters scan the text of an email and use fuzzy logic to give a weighted opinion as to whether the email is Spam. They can be highly effective, but can also occasionally filter out newsletters and other bulk email that may appear to be Spam. This can usually be overridden by explicitly authorizing email from domains you subscribe to.

Permission filters block all email that does not come from an authorized source. Typically the first time you send an email to a person using a permission filter you will receive an auto-response inviting you to visit a web page and enter some information. Your email then becomes authorized and any future emails you send will be accepted. This is not suitable for all users, but very effective for those that choose to use it, as long as the auto-response email is not blocked by the Spam filter of the initial sender!

14. I want to send Spam free bulk email. How can I be sure my recipients won't think I'm sending Spam?

Not all bulk email is Spam. Many responsible organizations send Spam free bulk email regularly to their customers, and subscribers. In efforts to stop Spam email, many recipients use specialised email software to block junk email, which has the undesired effect of filtering out legitimate Spam free bulk email. What is more frustrating to the email sender is to receive Spam reports from DNS blacklist holders stating that they are sending Spam when in fact they are sending legitimate Spam free bulk email. Many people subscribe to so many lists, they cannot remember what they subscribed to. If an email looks like Spam, they report it without taking a closer look to determine what it is.

In order to avoid this sort of occurrence, which at best is a nuisance and at worst can get you blacklisted causing thousands of your legitimate emails to bounce, it is necessary to look at your emails to see whether the look like Spam. If they are full of CAPITAL LETTERS AND EXCLAMATION MARKS!!!!! and they REPEAT THE SAME THING and they REPEAT THE SAME THING, then they will likely be considered Spam. If the recipient is using anti Spam software, they may never receive your email. The best test is to send yourself the email using anti Spam software first. If your anti Spam software thinks it is Spam, then don't send it. Fix whatever is wrong with it before sending it out. You will be doing yourself and your subscribers a big favor.