

Can E-mail Marketing survive SPAM?

Written: April 2004

A complete list of all articles written for the E-marketing Insights column of What's New in Marketing is available at: <http://www.marketing-insights.co.uk/wnimall.htm>.

About the author – Dave Chaffey, BSc, PhD, MCIM	
E-marketing trainer and consultant	Clients include 3M, Barbican, Britvic, The British Council, Computer 2000, HSBC, Intel, Siebel, NCH and Tektronix
Author of 6 best-selling business books	<ul style="list-style-type: none"> • <i>Internet Marketing: Strategy, Implementation and Practice</i> • <i>E-business and E-commerce Management</i> • <i>Total E-mail Marketing</i>
A marketing 'guru'	Recognised by the CIM as one of 50 gurus who have 'shaped the future of marketing'
Visiting lecturer at leading UK business schools	<ul style="list-style-type: none"> • University of Cranfield • University of Leeds • University of Warwick

Table of contents

Introduction

The tide of SPAM – unsolicited commercial e-mail messages – doesn't show any sign of turning. According to MessageLabs, who track the volume of e-mail SPAM and viruses, in 2003, SPAM increased from 40 to 60% of global e-mail traffic. That's a lot of SPAM when you consider that 30 billion e-mails are sent each day. Of course, you don't need the statistics to show you this – unless you are well protected, you can see from your own inbox.

Initially this would appear to be unwelcome news for legitimate, permission-based e-mail marketers and we would expect to see e-mail marketing response rates plummet.

However, I believe that E-mail Marketing can survive SPAM since it is still thriving - or is that surviving? This is based on long-term tracking studies from US and EU data published by e-mail broadcasters such as Doubleclick. Looking at the latest US report from Doubleclick (http://www.doubleclick.com/us/knowledge_central/documents/trend_reports/dc_q403emailtrends_0402.pdf) shows that Delivery, View and Click rates have held up well over the last year - we fortunately don't seem to be seeing the dramatic decline we saw in online ad response from the early days.

We might have expected response rates to fall over the year since we would expect that legitimate marketing messages become lost in the clutter of SPAM messages in the inbox together with the time spent by e-mail recipients in deleting SPAM. But it seems that e-mail recipients are generally good at distinguishing between SPAM and permission-based e-mails they have agreed to receive. It also seems that although some permission-based e-mails will get caught blocked or get caught in SPAM filters, many are still getting through.

Stable response rates not lead to complacency since there are many individual campaigns that have failed since its messages has been mis-identified as SPAM. In this article we review why legitimate permission-based e-mails may be identified as SPAM and consider actions e-mail marketers need to take to counter SPAM.

What is SPAM?

Everyone who uses e-mail knows what SPAM is. It is unsolicited commercial e-mail offering the recipient to get rich quick, get large quick or get high quick. In another words, it is e-mail sent without the recipient agreeing or opting in to it. SPAM is usually sent in bulk – batches of millions of e-mails using servers hijacked around the world. Because there is always that 0.0001 percent response, spammers and their suppliers work hard to collect e-mail addresses through developing software spiders to crawl the web to harvest e-mail addresses published on web pages or through writing worm-viruses that find e-mails from the infected PC's address list or documents.

Originally SPAM was best known as a tinned meat (a contraction of 'spiced ham') and the myth is that the negative connotation arose during the second world war when it was a staple in the ration packs of US soldiers. Its reputation wasn't improved by the Monty Python sketch. A modern acronym that has been devised is 'Sending Persistent Annoying e-Mail'.

A permission-based marketing e-mail is one that is solicited by the user; they have consented to receive it by proactively ticking a box. Any other indication that is taken as indication of consent is at risk of being perceived as SPAM by the recipient, although it may still be legal in some countries. Non-permission-based approaches to e-mail list building which although they may not break the law in a country, that run the risk of being considered SPAM include adding previous customers who have not opted-in to an e-mail list, adding people to the list who have failed to notice that a box on a web form has been pre-ticked; or failed to tick a box saying they don't want to receive e-mail; or if they are an existing customers of a company. This means that under some national laws many legitimate companies are still legally sending out what recipients consider SPAM. It is not the intention of this article to review the latest laws in different countries, I am making the point that you may be legally compliant according to the laws of some countries, but still sending SPAM.

The difficulty for the marketer is that whatever definition you use, SPAM is SPAM in the eye of the beholder, whether the beholder is the person receiving the message or the software that is used to identify e-mail on its journey from the sender to the recipient.

For the legitimate marketer, the problem is the so-called 'false positives', which is where a legitimate permission-based e-mail from a well-established brand is wrongly identified as a SPAM.

We will see that it vital for the e-mail marketer to ensure that the e-mail is not interpreted as SPAM on any stage of its journey.

Where is SPAM identified?

Spammers work hard to understand why their messages are not read and find methods to avoid being blocked. Here, the legitimate e-mail marketer is much like the spammer, since they and their suppliers also need to understand what is stopping their messages getting through and identify solutions to this. There are three general places where SPAM, or legitimate permission-based e-mail is identified which will stop it being read by the recipient.

1. **In-box identification** – the simplest way that SPAM is identified, is by the recipient if it looks like SPAM from the header it will be quickly removed using the delete button.
2. **Software filtering** – E-mail can be identified as having the characteristics of SPAM using anti-spam software which may run at a variety of locations; at the ISP, a third-party mail-scanning service, at a company firewall or mail server, at a web-based e-mail service server or on the end-users computer.
3. **Domain blocking** – where the domain from which the e-mails are broadcast is blocked since its IP address is deemed to be a known source of source of SPAM.

How is SPAM identified?

What makes your campaign smell of SPAM and how can you avoid it smelling of SPAM

I refer to a campaign smelling of SPAM since categorizing an e-mail as SPAM is inexact – your e-mail may have some characteristics of SPAM, i.e. it may smell of SPAM without being SPAM. We will review the characteristics that make an e-mail smell of SPAM for each of the three places where e-mail is identified as described above.

1. **For in-box identification.** An e-mail will look like SPAM if the recipient doesn't recognise the sender, i.e. it is not a company or product known to them in the From or Subject line. If it is not clear from the subject line, a preview of the text in the e-mail will usually show that it is irrelevant.

So, for an in-house e-mail list you must use the company or brand name in the From address, or in some cases, like an e-newsletter where the name of the e-newsletter is in the From address, use the name of the company or brand in the subject line.

For campaigns using rented lists or co-branded with a partner it is more tricky. Many companies concatenate both list owner and the brand being promoted in the From as in 'Freeserve-Accucard', but since this may get truncated it may be better to put the brand in the subject line.

Another vital step to avoid being identified as SPAM by the recipient is to use copy within the message that explains that the message is not SPAM. This is commonly headed as a '**Statement of Origination**' or more informally '**Why am I receiving this e-mail?**'. This should explain either that the recipient has opted in, ideally with the place and time of opt-in, or that they are receiving it since they are an existing customer. You should also explain that the message is within the law of the country.

For e-mail campaigns using rented or shared lists, it is essential that the statement of origination is clear, typically at or near the top of the message. For house-list campaigns, it is still useful to have, but is probably best at the footer of the message.

2. **Software filtering** – There are now many techniques that are used to identify SPAM by different types of anti-spam software. We will now review eight of the most common ones which are often combined in a single anti-spam tool and describe the type of steps that marketers can take to avoid being wrongly identified as SPAM.

A. **Keyword and key phrase filters.** First generation anti-spam software used a simple look-up table of words that are commonly used by spammers such as 'Viagra', 'Sex', 'Over 18' or 'Free'. If these words are contained either in the message header or body then it is deleted or assigned to a Junk Mail folder.

Such words do not present a problem to most companies, but what if your company is in 'Sussex' or you are a bank, that by law has to say that your product is only available to those who are 'over 18'? Or maybe you are offering a Free-trial. In these cases, one alternative may be to use these 'naughty words' as part of graphics embedded within the e-mail which will not be recognised by most filters. Of course the spammers, use variants of words such as 'v'igra' or 'vlagra'.

Do not be overly concerned by using words such as 'Free' in the subject line – I have seen tests where such e-mails pull a higher response than more subtle approaches. The reason is that many SPAM filters now use a more sophisticated approach.

B. **Message rating filters.** Second-generation anti-spam software uses a scoring system where different keywords and different phrases score different points. So 'Free' might score 2 points and 'Sex' 10 points. If the e-mail is rated over 15 points it will be classified as SPAM. Some programs now use Bayesian filters which use a mathematical model to learn the characteristics of SPAM and to watch for patterns characteristic of SPAM. You

may have noticed gobbledy-gook phrases at the bottom of some SPAM messages, these are used to overcome such an approach.

One practical step e-mail marketers can use to check their messages for spam rating is to use the Lyris Content checker. <http://www.lyris.com/contentchecker>.

Messages are also blocked if the original From address has been masked, so it is important for legitimate marketers not to do this.

C. Blacklists. Blacklists are lists of known Spammers such as those reported to Spamhaus Project (www.spamhaus.com) or SpamCop (www.spamcop.net). If a recipient is on the blacklist it is deleted or put in the Junk Mail folder. Blacklists are often used in conjunction with filters to block e-mails. One of the most widely used systems is developed by Brightmail (www.brightmail.com) uses a global network of e-mail addresses set up to trap and identify SPAM. Brightmail is increasingly used by ISPs such as BT to block SPAM.

Blacklists are also used by many types of anti-spam software such as the two most popular; McAfee SpamKiller and Norton AntiSpam.

It is unlikely legitimate marketers will be placed on these, but it may be worth checking. However, there is an argument for companies who send out a lot of consumer e-mail to test whether messages pass through the main filters. Filtering used by major ISPs such as BT, AOL, Freeserve and also web-based e-mail services such as Hotmail and Yahoo!Mail should also be tested.

Using seed addresses at some of these accounts can help, but you may be missing some. E-mail monitor (www.emailmonitor.co.uk) estimates that 99% of e-mails in the UK are ultimately delivered through 20 ISPs. It offers a tool known as MailBox Monitor which is configured with addresses at these 20 ISPs in order to test for blocking due to blacklists or the different filters described above. It also has a tool known as Message Check which tests an e-mail address before sending against the main filters.

D. Whitelists. An organisation whitelist is a list of bona-fide e-mail addresses that are likely to want to contact people within an organisation. It will include all employees, partners, customers and suppliers who have obtained opt-in from employees to receive e-mail. A personal whitelist is one created by the user of e-mail software of message senders they are happy to receive e-mail from.

The organisation whitelist approach has not been adopted widely since it is difficult to set up, but it probably offers the best opportunity for the future. The personal whitelist feature is becoming more common in anti-spam software and is now built into Outlook or the popular Qurb (www.qurb.com) service which guarantees to 'block 100% of Spam'!

But there is little action the marketer can use other than recommending that they are put on the whitelist. Some e-mail recipients may use such tools rather than opting out.

E. Challenge/response authentication. In this approach, if an e-mail is sent from someone who is not on your whitelist, or possibly on your blacklist, a message is automatically sent, asking the sender to manually confirm or authenticate their identity by following a link from a challenge e-mail that requires a response. This approach is available as part of antispam solutions from companies such as Spam Interceptor (<http://si20.com>) and SpamBully for Outlook (www.spambully.com). The theory is that spammers are not going to be able to respond. The problem is that permission marketers will not be able to either. Fortunately, it seems that this approach is not widespread...yet.

F. Sender Warranted E-mail.

Sender warranted e-mail use some type of watermark to identify legitimate e-mail. Habeas (www.habeas.com) has been one company that has successfully promoted this approach. This is a great example of lateral thinking. The e-mail message contains a defined signature which is based on a small haiku poem. For example, the footer might contain 'X-HABEAS-SWE1-Winter Into Spring'. E-mail marketers who use the Habeas service have the right to include these identifiers in the foot of their message. Since Habeas has an

agreement with the major ISPs such as AOL and anti-spam services such as Message Labs, such messages are never classified as SPAM since they are from a trusted sender.

Of course some spammers have started using the Habeas codes within their e-mails, but two prosecutions have been brought against them.

A similar approach is the concept of a 'bonded sender' developed by Ironport (www.bondedsender.com) Senders of opt-in e-mail post a financial bond to prove they are a reputable company. Senders of SPAM would not be able to afford to pay the bond. Recipients who feel they have received an unsolicited email from a Bonded Sender can complain to their ISP, IT manager, or IronPort and a financial charge is debited from the bond.

G. **'Peer-to-Peer' blocking services.** These take advantage of the fact that humans are good at identifying SPAM and they then notify a central server which keeps an index of all SPAM. SPAMNet from CloudMark (www.cloudmark.com) requires users to identify SPAM by pressing a 'Block' button in Microsoft Outlook which then updates a central server, so when others download the same message at a later time, it is automatically identified as SPAM. I have used this service and it works effectively, but I have noticed a problem where legitimate e-mails I have opted-in to are classified by SPAM as other users. You can mark them as legitimate, however.

3. **Domain-level blocking.** ISPs or firewalls can block individual domains or web IP addresses which are known sources of SPAM or the pattern of sending suggests spamming. This approach is intended to trap known spammers who hijack servers and send out a large number of e-mails. However, it can lead to legitimate e-mail marketers being blocked, particularly if their e-mail platform is co-hosted with a machine that has been hijacked. This may also be a problem if you send out a large number of e-mails in a short-period.

This may be a problem for marketers that broadcast a large number of e-mails. One solution is to send out the e-mails over a longer period or 'throttle back' the rate at which e-mails are sent. However, it is difficult to know which ISPs are blocking your domain. One tool that could help here is IP block alert also from IPT Limited's E-mail Monitor (www.emailmonitor.co.uk). We can expect to see more such tools introduced by e-mail broadcasters and they will become part of the service.

Future anti-spam initiatives

Earlier in 2004, there was an announcement of intent for international co-operation by governments to encourage ISPs to create an effective infrastructure to limit SPAM. Initially this was to focus on reducing the ease with which spammers can spoof or mask their real address in e-mail headers by replacing it with another domain name. This would prevent spammers using common domain names such as Yahoo.com or Hotmail.com, but some believe it will not prevent spoofing of less well known names. Providers such as Sendmail (www.sendmail.com) are developing 'sender authentication technology' which allows organizations to verify the source of a message before accepting it by automatically checking if an email came from where it claims it did. Also earlier this year, Bill Gates announced at the annual Davos meeting of business leaders that Microsoft would develop technology that would help rid the world of SPAM within two years! Draw your own conclusions. Proposals have followed such as the Microsoft Caller ID E-mail specification and Yahoo! Domain Keys aim to combat domain spoofing which is not conducted by legitimate e-mail marketers.

An additional component of future approaches could be charging a small amount for each e-mail sent, particularly where multiple messages are sent. This would eliminate the economic incentive for spammers, particularly if they could not hide the source address. What will be of more concern is proposals to charge large volume e-mail broadcasters. Although companies using third party broadcasting services are already paying between 0.5p and 10p per message, companies broadcasting their own e-mails would also see an increase in costs. However, any small increase in price per message may be able to borne

by companies if current response rates prevail. Indeed one argument is that with less SPAM, response rates will increase.

All of the developments covered in this article and the increasing number of court cases brought against serial spammers give some cause for optimism. But eradicated in 2 years – I don't think so! I will be looking for the percentage of SPAM sent to start decreasing first.

Dave Chaffey – Contact details

Dr Dave Chaffey, Director Marketing Insights Limited
>> Improving Performance through eMarketing Intelligence >>
E-mail: dave.chaffey@marketing-insights.co.uk
Phone: +44 (0)7740 181 590
Web: www.marketing-insights.co.uk
eResources and Books: www.marketing-online.co.uk