

A spammer in the works

Everything you need to know about protecting yourself and your business from the rising tide of unsolicited "spam" email

A MessageLabs white paper by Paul Wood, Chief Information Security Analyst



Contents

The threat of spam to business systems	2
The damage that spam does to profitability	3
What explains this sudden explosion of spam ?	4
Baiting the hook	5
Who are the spammers? What's in it for them?	6
How come they know your address?	7
The channels through which this menace proliferates	8
Spam and the law	9
So what can be done to combat the problem of spam?	10
The MessageLabs anti-spam solution	12
Measuring the return on investment	13
So what conclusions can be drawn?	14

Introduction

Like most people, you've probably encountered the menace of spam first hand. You'll know all about that infuriating avalanche of junk email which somehow worms its way uninvited into your inbox, fouling up the efficiency of your email system, taking up precious bandwidth and generally wasting your valuable time.

How come some unknown fraudster has got hold of your email address and is badgering you with a dubious get-rich-quick scam, you want to know? What possible use might you have for growth hormones, herbal remedies, miracle diets, dodgy loans, hair restorer, cheap trinkets, unsavoury website subscriptions and the myriad of other junk-mail offers which you never requested?

More significantly, you may also ask yourself: if your business colleagues are being swamped with a similar tide of this time-wasting rubbish, what collective impact is the menace of spam having on the efficiency of corporate activity?

This paper provides everything you need to know about spam — where it comes from, how it works, the problems that come with it, who the spammers are, the tricks they use, the different types of spam and the legal issues.

Most vitally of all, we explain how you can prevent this pestilence from wasting your time, clogging up your email system and damaging the profitability of your business.

The threat of spam to business systems

It began as little more than a "nuisance" around a decade ago, initially frowned upon as being somewhat unethical but nobody felt the need to do anything about it. Since then spam has grown exponentially to become a serious threat to email security for businesses globally.

By 1999, the proportion of spam turning up in corporate mailboxes was already becoming a concern. By early-2003, the time of writing, the sheer volume of spam has become so damaging that more and more businesses are waking up to the problem and searching for ways by which this growing menace can be contained.

Some figures for the first three months of 2003 alone put the escalation of spam volumes into an alarming perspective. In January 2003 MessageLabs statistics were showing that one in every 4.1 emails was identifiable as spam. That's 24.5 per cent. By the following month this had increased to one in 3.9 (25.6 per cent). And by March the ratio of spam to legitimate email had rocketed to one in 2.8 (36.3 per cent).

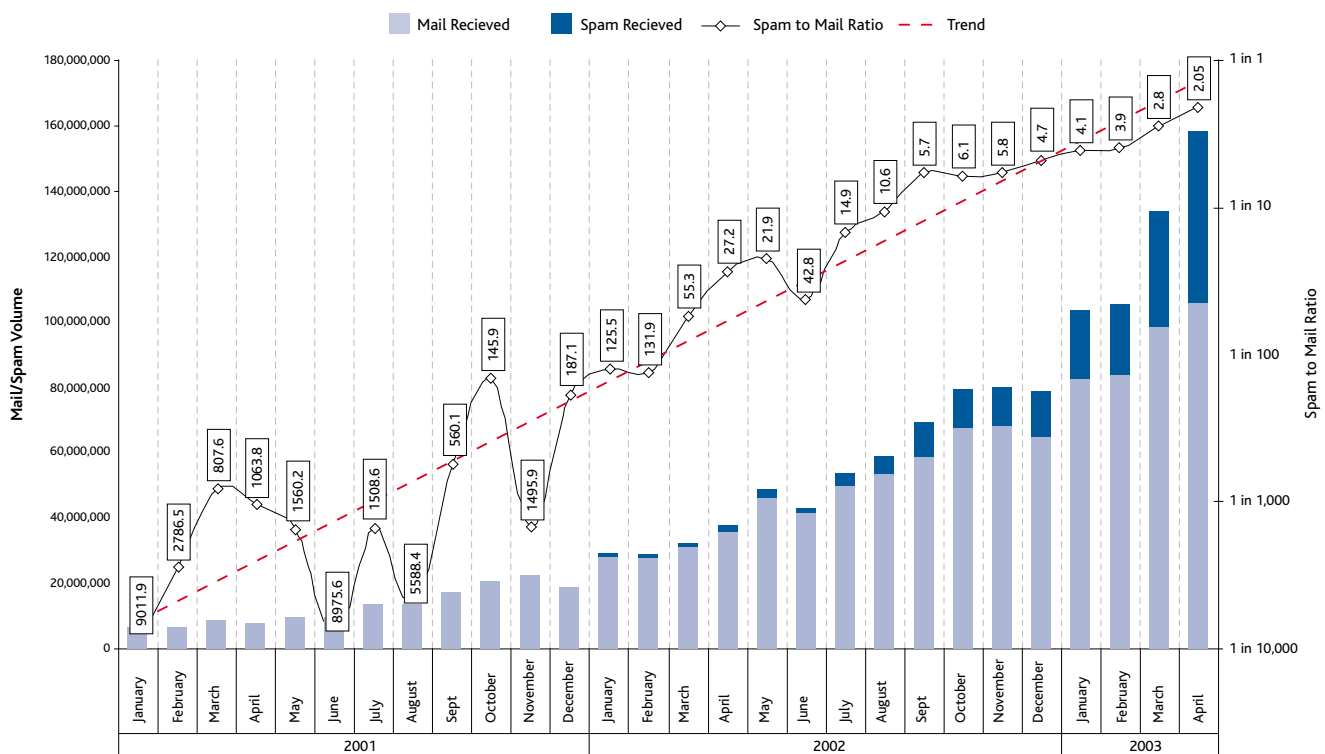
European Commission figures for 2001 estimate that the cost of spam globally is around £6.4bn a year in connection charges alone. With in excess of 544 million Internet subscribers worldwide, that's an average of nearly £12 per user per year.

The threat to ISPs (Internet Service Providers), businesses and consumers is particularly severe in the US. One large ISP reported receiving nearly two million spams each day from a promotions company until an injunction was obtained to prevent it. If you assume that each user spends only ten seconds identifying and deleting spam messages, the amount of connection time being squandered through that single ISP was in the order of 5,000 hours every day.

As part of a six-month investigation of spam by the Center for Democracy and Technology, a US not-for profit Internet privacy group, 250 email addresses were set up. These attracted 10,000 emails, of which 8,842 were unsolicited.

It's bad, and it's getting worse. That is the clear message. Researchers at Gartner have predicted that spam will account for around 50 per cent of all email by 2004. However, uniquely-placed as we are at MessageLabs to quantify the rising tide of spam, our projections show that the ratio is likely to break through the 50 per cent mark by as early as July 2003.

Spam to Mail Ratio - Global Trends



The damage that spam does to profitability

Productivity

The first casualty of the spam epidemic is employee productivity. Staff who have to wade through their email inboxes to differentiate the relevant email from the rubbish are at an immediate time-management disadvantage. And who knows how much more time they might be persuaded to waste if they were to be drawn in by a particular spam offer? They would lose concentration and be distracted from their work, resulting in a considerable break in productivity.

Bandwidth

A Gartner survey in 2002 revealed that staff were already spending an average 49 minutes a day (that's 10 per cent of their time) just managing their email — and that 34 per cent of business email being received was spam. Given the massive escalation of spam since then, it may be assumed that email management has become an even more time-consuming activity at work.

By March the ratio of spam to legitimate email had rocketed to one in 2.8 (36.3 per cent)

Pressure on the IT team

It has to be paid for; and selection of bandwidth from your ISP is a business decision tailored to your anticipated business usage. If just a quarter of your incoming mail is unsolicited spam, the unexpected volume will already be throttling your Internet connection. That slow-up in email delivery can soon start to impact on your hard-won competitive edge. You can increase bandwidth to maintain speed, of course — but do you really want to pay more, just so that spammers can get faster access to your people?

Exposure to legal hazards

Volumes of pornographic spam are increasing. So is the pressure on employers to protect their people from exposure to offensive or disturbing email-borne material. There have already been well-publicised instances where employees have successfully brought legal cases against their employers, principally in the area of sexual harassment stemming from the abuse of email. However, given the continuing growth in pornographic spam, the hazard is already beginning to extend worryingly into the realms of unsolicited email.

Though complaints about spamming can now be investigated by the ASA for the first time.

What explains this sudden explosion of spam?

User complaints and queries relating to unsolicited emails have increased in direct proportion to the growth in spam – an additional support task that IT teams could do without. Having to deal with the disruption and user disgruntlement caused by spam deflects IT professionals from more productive work. So here's another cost impact, in addition to the negative effect on the morale of IT staff who would rather be working on creative projects.

In the early days of the Internet, the term "spamming" was initially coined to describe the activity of indiscriminately posting the same messages to lots of different newsgroups, often provoking outrage as a result. The term itself was thought to have come from the well-known Monty Python sketch where everything on the menu included Spam – whether you wanted it or not.

Nowadays, what actually constitutes spam, or "unsolicited email" remains a matter for debate. The nature of the communication being delivered is one issue; and the question of what "unsolicited" means is another. It's important to be able to differentiate email that has been targeted indiscriminately at thousands of individuals from legitimate email that nonetheless carries some kind of commercial message.

However, in broadest terms, spam can perhaps be defined as unsolicited bulk email dedicated to electronic advertising – the Internet equivalent of the conventional junk mail which lands on your doormat most days of the week. Essentially, it can be delineated by these overriding characteristics:

1. It is almost always targeted arbitrarily in huge volumes at a large number of users.
2. The motive behind this avalanche of junk email is invariably to leverage some benefit to the spammer, whether it be financial, political or some other benefit.
3. A less prevalent motivator among some spammers is the malicious desire to disrupt business internationally. What has become known as a "denial of service" (DoS) attack is designed to flood mail systems and bring down servers with sheer volumes of electronic trash. A notable side effect of a DoS attack can be to disrupt the performance of the company website, which may be sharing the same bandwidth connection as the mail server.

As email has rapidly become the most widespread global communications medium, so it has come to be an obvious channel for those who wish to sell products and services – or relieve unsuspecting customers' of their money by overtly fraudulent means.

Email is surely too great an opportunity for the junk-mailer to resist. On one hand it offers a truly global marketplace that's instantly and constantly accessible. On the other, the ability to work from "off-shore", away from the jurisdictions of more civilised authorities, also enables the spammer to indulge with impunity in all kinds of questionable marketing techniques – and downright criminal behaviour in some cases. Moreover the ease with which millions of spam emails can be transmitted, extremely cheaply, is a further attraction for the spammers.

In 2002, in excess of 64 million spam emails were identified and intercepted by the MessageLabs anti-spam service.

Baiting the hook

Most spam presents either some kind of financial offer, chiefly loans and credit, or is product/service-related. Much of it can be pretty naive and innocent enough in itself, though a growing proportion of spam (currently around 10 per cent) is pornographic in content.

However, spamming is now becoming a more sophisticated business. Unlike the more regulated legitimate marketing industry, the sources through which spam is delivered are often specious. Because a spam is usually easily spotted and deleted without opening, the spammers are resorting to more elaborate tricks to attract attention. A variety of social engineering methods are exploited to induce the recipient to open and read the content of the message being sent.

More often than not, spam originates from an email address that is spoofed or forged, concealing the identity of the sender. The spammers will, for example, appear to be sending their mail from an address that you'll recognise – from someone else's address book which they have previously accessed and are now spoofing.

You may also receive emails with subject lines and intro texts that have more insidious appeal, making it more difficult to identify the communication as spam. Lines such as "why haven't you replied?" or "shame you missed the party, here are some pictures" are common deceptions used in this way.

Another example of the smart spammer at work is the greetings card scam. An intriguing email alights on your inbox, explaining that there's a personal message waiting for you at a linked web site. There you are instructed to download some software, in order to read the message. What you don't realise is that the licence agreement, which most people just click with a "yes" without reading the small print, includes your explicit permission for the program to send a copy of the original email to every single person in your Microsoft Outlook address book.

Top offenders in the swindle category are known as "four-one-nine" or "advance fee fraud" scams which seem to have originated in Nigeria, with growing numbers now coming in from Iraq.

It's called 419 because advance fee fraud is defined and punishable under section 419 of the Nigerian criminal code. The 419 takes various forms, but here's a typical one: you get a flattering email from some unknown person in a foreign country. He has come across x-million dollars lying dormant in a bank account, but he needs funds to spring the cash and get it out of the country. If you send an appropriate sum to help, he'll cut you in for a proportionate percentage of the x-million.

Who'd fall for a thing like that, you might wonder. Well, there have been more than 150 cases reported in the UK alone over last 12 months in which gullible people have handed over an average £50,000 each. That's around £7.5 million for the fraudsters, while the "investor" suddenly finds that his emails don't get answered any more.

Interestingly, recent statistics releases from the UK's National Criminal Intelligence Service estimate that up to five agents are waiting in London hotel lobbies every day to meet people connected with a 419 scam.

European Commission figures for 2001 estimate that the cost of spam globally is around £6.4bn a year in connection charges alone.

Who are the spammers? What's in it for them?

The underground nature of the spamming industry makes it difficult to profile the typical spammer. Certainly they have access to sophisticated software engineering, even if they don't have the capability themselves.

There are known to be currently around 180 well-known serious spammers at work out there, in addition to many more who operate on their own account, for profit, malevolence or propaganda. Some more organised outfits function, or at least mail, their wares from off-shore or criminally-acquired locations, taking precautions to remain as anonymous and hard-to-track as possible.

Profits for spammers vary. Those selling a product or service directly stand to make a fortune from sales, in return for an attractively small outlay. Even a tiny percentage in uptake can generate substantial income, given the sheer volume of emails that are sent out soliciting business. Meanwhile the most common type of operator — the spammer-for-hire — is less well rewarded, tending to make around US\$250 per every million emails sent. As one self-confessed and unapologetic American spammer says: "It's a numbers game."

How come they know your address?

Just as in the conventional paper junk mailing business, names and addresses are an extremely collectable commodity. Email addresses find their way on to mass mailing lists through a variety of channels. Most are acquired by spammers who can automatically harvest email addresses from publicly accessible web sites or newsgroups, while people who use the Internet a lot for financial transactions or even for general surfing are also potentially vulnerable.

Spammers target large business organisations with what are known as directory harvesting attacks (or DHA), using software to generate random user-names at that specific domain. The perpetrators use a dictionary of common names and some software to generate large batches of potential addresses for a given domain. This software can even look for SMTP error codes returned by the server, to establish whether or not the address is valid. Some more sophisticated servers, in common with the MessageLabs anti-spam service, can detect a DHA and automatically blacklist the sender's address.

Free Internet email accounts such as Hotmail are targeted in this way too. Online marketing operators are known to be developing engines capable of serving 100 million messages per day. Hotmail itself has tried to counter the problem by reducing the number of messages that users can send each day. The limit is now 100 in any 24-hour period — down from 500 a day.

Of course their overheads are minimal. It costs so little to mass-mail in millions over the Internet. One million email addresses can cost as little as 63p and one million spams take about four hours to send by dial-up at a cost of only £2.40. With just a one per cent success rate in terms of sales, economics are such that the spammers can afford to continue unrelentingly.

There are now many "ratware" products doing the rounds of the spamming operations, designed to enable the transmission of millions of emails in a very short time and to make subtle changes to each email before it is sent. Ratware cannot be bought through legitimate outlets; it is usually written by spammers and sold to others. Although ratware tends not to be sophisticated by the standards of most commercial software engineering, it is already sufficiently advanced to produce the desired results.

Software is also available to those who assemble mailing lists for spammers. This enables them to enter a web site and to harvest every email address quoted therein. One way and another, mailing lists — often containing useful demographic information about the addressee as well — are not difficult for the spammers to come by.

There are programs called "spiders" and "crawlers" that enter websites and gather information for building entries for search engine indexes. The big search engines on the Internet deploy these programs, quite legitimately, but of course the technique is also open to abuse by spammers. The spider is so called because its legs can encompass a whole lot of sites simultaneously, while the crawler gets its name from its more methodical examination of sites, one page at a time, following links to other pages as it goes.

Some spam can carry hidden links to websites (known as "spyware") that are used for tracking how many of their emails have been opened, and who has opened them, further validating the email addresses they have used. These encoded links are triggered when the email is opened, but can only work when the recipient is connected to the Internet at the time, and assuming they are able to view HTML emails.

Ironically, if you click the "unsubscribe" box (or link) on an unsolicited email, hoping that they will leave you alone in future, you are merely confirming the validity of your email address – which thus becomes all the more valuable to the spammers. The "unsubscribe" issue has proved to be a problem for legitimate bulk-mailing operations too, since the presence of such a device in an email can often result in the mail being filtered out by some anti-spam software.

It also raises the question: how do you unsubscribe to that otherwise perfectly legitimate newsletter that you subscribed to long ago, but may have forgotten about?

When completing an online form, sometimes you may find an option is pre-selected by default with the anticipation that you won't notice it. Once the form has been submitted with the option still selected, you may have unwittingly given the company permission to send what you may consider to be spam. These "spam traps" assume that most people don't read all of the form, and will fail to spot the spam trap, with a comparable success rate to the greeting card scams.

Similarly, if you should fall for it and buy spam-advertised products, you will most likely be asked for further personally identifiable information such as your name, address, phone number and credit card numbers. This guarantees that you will get even more spam – and that the spammers know more about you.

To try and keep pace with the spammers, the anti-spam community make use of what are known as honeypots, where particular email addresses are consciously circulated on the Internet, so that they find their way into the spammers databases. This attracts a huge amount of spam in return, which can then be further analysed so that the appropriate measures are assembled in advance to defeat them quickly.

Gartner have predicted that spam will account for around 50 per cent of all email by 2004.

The channels through which this menace proliferates

Almost all spam gets to you from one of three possible sources.

1. There is the dedicated "spam house", usually an offshore ISP that specialises in bulk mailing.
2. Unsolicited mail can arrive from a fraudulent dial-up account. The spammers will create a new account (often DSL) with stolen credit card details and use it to spam freely for a month or so, before moving on to another dial-up service provider.
3. You might be the victim of the insidious bulk-mailing software, designed to seek out insecure email systems on the Internet, known as open relays and open proxies, through which spam can be sent. Among its growing array of features, this software enables junk email to be disguised as regular email by the social engineering techniques discussed earlier, and also to pass undetected by many conventional anti-spam filters.

Our projections show that the ratio is likely to break through the 50 per cent mark by as early as July 2003.

Spam and the law

From the autumn of 2003, the sending of unsolicited communications via email, SMS or phone will become more rigidly regulated across all EU member states. Proposed new legislation relating to email under the European Directive on Privacy and Electronic Communications are likely to:

- Require businesses to gain prior consent before sending unsolicited advertising emails. This consent must be explicitly given on an "opt-in" basis, except where there is an existing customer relationship.
- Require that the use of "cookies" or other tracking devices (including "spyware") is clearly indicated and that the recipient is given the opportunity to reject them.

Spam has become a particular scourge to business (and individuals) in the US, where volumes of unsolicited email have been a major problem for much longer than in Europe. It was the States which pioneered the large .com domains, attracting early spammers to target them, while tending to pass over the less prominent top-level country domains, such as .uk, .de or .au, for example.

Since the more recent .com boom, there has been a huge increase in the numbers of .com addresses outside the USA – and the explosion in spamming has thus become a worldwide curse.

Meanwhile, the UK's advertising watchdog, the Advertising Standards Authority (ASA), has established tough new rules governing the use of email and text messages for marketing purposes.

Revised codes of practice state that "explicit consent" of consumers is required before marketing via email or text messages. Marketers may however "market their similar products to existing customers without explicit consent" providing recipients are given the opportunity to decline to receive further messages. Also marketing messages are required to be clearly identified as such.

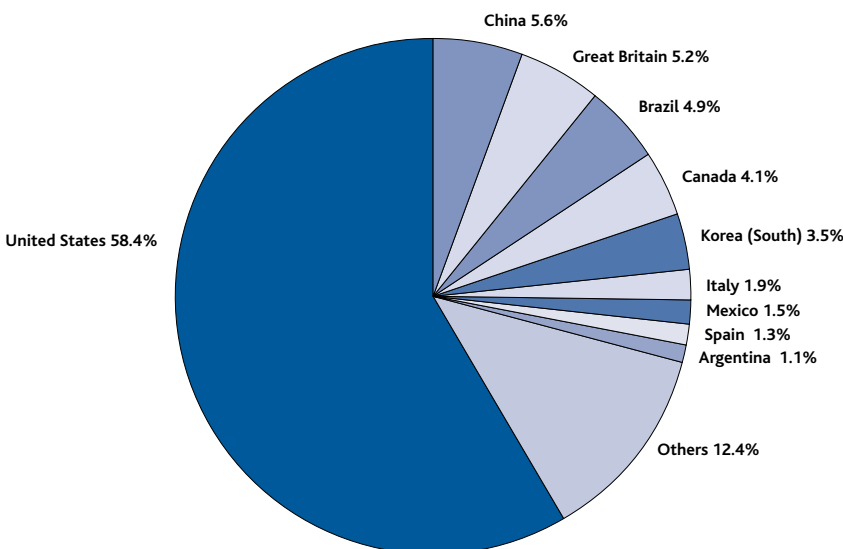
Though complaints about spamming can now be investigated by the ASA for the first time, many industry experts believe that the real strength of the new ASA rulings will be in making a clearer distinction between legitimate permission-based marketing and spam.

MessageLabs works closely with the Anti Spam Research Group (ASRG) set up by the Internet Engineering Task Force (IETF). Though the ASRG's brief specifically excludes pursuit of research into the legal issues of spam, the group's purpose is to understand the problems it poses and to come up with thoroughly evaluated solutions.

The plain fact is that laws in themselves will never defeat the determined criminal or shady operator. The "locks" need tightening up too. The only way to be certain of combating the growing menace of junk email is to put in place an intelligent security system which can identify spam accurately and stop it at the Internet – before it can get anywhere near your network boundaries and start clogging up your email system.

A Gartner survey in 2002 revealed that staff were already spending an average 49 minutes a day (that's 10 per cent of their time) just managing their email.

Spam activity by country of origin



So what can be done to combat the problem of spam?

There are a number of methods that can be employed to fight off spam, some more effective than others. Broadly speaking they are as follows:

A further source of spam, notably in the USA, is accounted for by the increase in the number of more permissive, cash-strapped ISPs who allow spammers to use their servers in return for a slice of their profits.

DNS blacklisting

This was the first spam prevention mechanism to be deployed. It is simply the blacklisting of known spammers, enabling any communication coming from a blacklisted IP address to be blocked. Its weakness is that, once the spammer knows the address he's using is blacklisted, he simply moves on to a new one. Additionally, blacklisting only filters on the basis of IP address, without analysing the textual content of the email itself.

Historically, blacklisting tended to result in a high degree of false-positives, where legitimate email is wrongly identified as spam. However, as the technique has matured, this problem is thankfully no longer on the same scale.

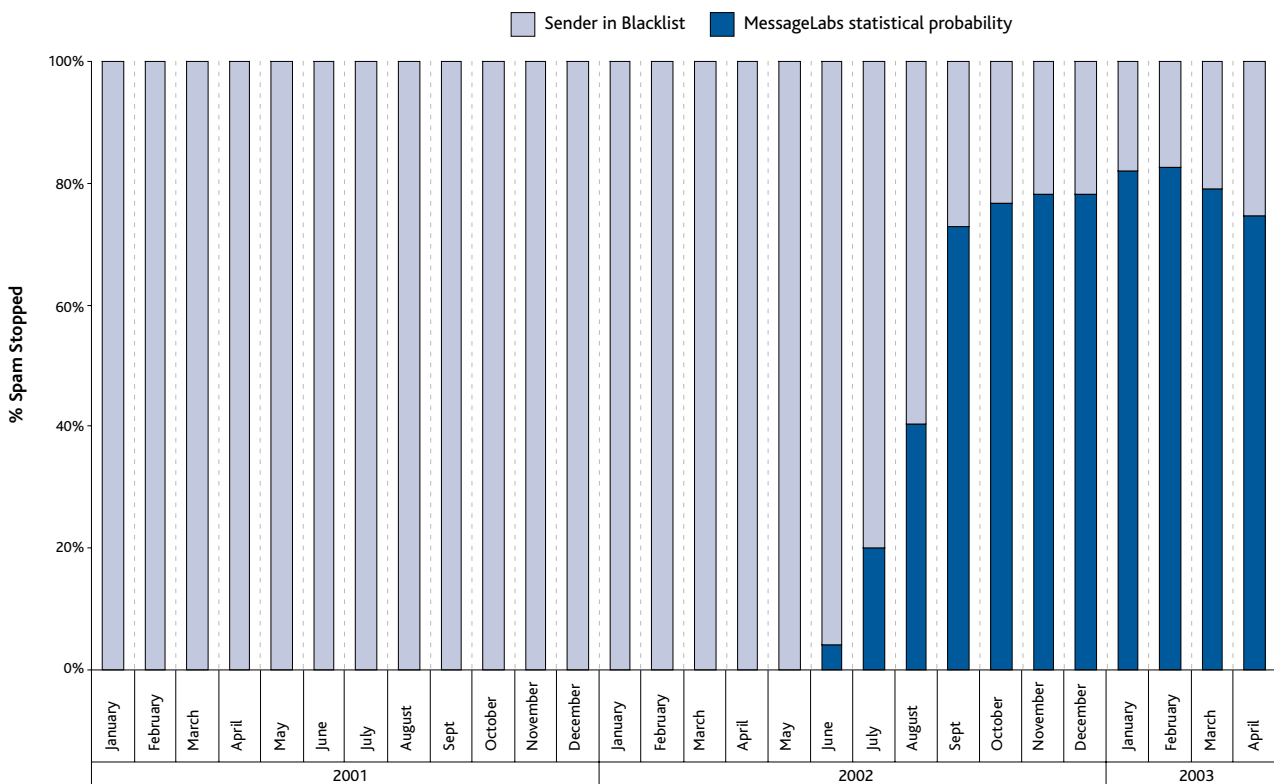
Fingerprints or signatures

As in the case of viruses, it is possible to generate what are known as signatures, or fingerprints, of any particular bulk-mailed spam outbreak. The signature can then be loaded on to an elementary spam filtering system, which will then stop all email bearing that signature. The technique results in practically zero false positives, but it suffers from the "sacrificial lamb" problem. In other words, somebody has to get hit by the particular spam before it can be analysed, its signature created and the fix distributed to all users.

Whitelisting

This is like blacklisting in reverse. The idea is that only mail which is sent to you by someone who has already contacted you by email can be delivered into your inbox. Any first-time correspondent who is not on your whitelist must identify himself before the mail can be accepted. This can create irritating problems, however. For example, if you buy some product or service from an online store, how does the automated confirmation of receipt get through your whitelisting system?

% Spam stopped by reason



Collaborative filtering

This method relies on the goodwill of anonymous Internet users who upload details of spams which they've identified — and may well have been hit by — to a central web site. A number of anti-spam services use this databank of user submissions as the basis for spam detection, but unfortunately the method is beset by high numbers of false positives.

Heuristics

Essentially heuristical analysis revolves around a complex set of rules that can be combined to identify what is and what is not spam. It's a technique that MessageLabs developed with enormous success in identifying email-borne viruses and has further exploited in its anti-spam technology. Heuristical methods alone are no longer a complete safeguard in combating spam, however, since the spammers are improving their technique in making spam look more like genuine email.

Currently the MessageLabs combined approach is more than 96 per cent accurate.

Bayesian probability

At MessageLabs we have pioneered the use of mathematical machine learning techniques in identifying spam. Bayesian probability assesses the likelihood of an email being spam by learning to recognise the difference between bona fide emails and spam. Simply, the more email that the engine sees, the better it becomes at spotting the spam. Bayesian probability models have proved to be extremely powerful and effective — reducing the false-positive rate to an almost negligible one in 1,000 incorrectly identified emails.

Haiku

A more recent method that is also becoming more widely used is where a proprietary "Haiku" tag is included in the email headers. The Haiku, which consists of a small poem, can be used to indicate a pre-existing relationship, for example.

The aim of this is to make mail filtering much simpler by further eliminating the numbers of false-positives. It is also intended that should a spammer misappropriate the Haiku tag, copyright laws can be used against them. However, it remains to be seen how successful this approach may be, since it has its many proponents as well as its critics.

The MessageLabs anti-spam solution

Before too long, the explosion of spam filling our mailboxes will significantly reduce the effectiveness and efficiency of email as the most widely used Internet application; damaging the credibility of the medium as one of the most powerful business applications we have come to know and rely on. The most prominent irony of the spam epidemic is that, in the longer term, the spammers are simply killing off the very medium on which their activities depend. By flooding the marketplace with their wares in such vast volumes, they are rapidly throttling the email system — like a parasitic ivy plant, which eventually smothers the tree it invades.

The only way that we can preserve email as the otherwise vitally useful communications medium it has become is to prevent the "ivy" from taking hold in the first place. The fact is, the menace of

spam can only be contained by protecting your email system from the damaging effects of unsolicited mail — and that means putting in place the most comprehensive defence system.

At MessageLabs we believe that the only way to combat spam comprehensively is by combining the best of all anti-spam techniques into an intelligent whole.

The power of the MessageLabs solution lies in its dynamic amalgamation of Bayesian probability, heuristics and artificial intelligence techniques with the best features of white and blacklisting.

This is what enables our anti-spam service to stop unsolicited email before it can get through our customers' gateways and into their vital networks.

The MessageLabs anti-spam solution

As a highly focused, specialist managed service provider, MessageLabs is a world leader in all aspects of email security. Our anti-virus service, which stops all known and unknown viruses before reaching our customers' networks, is already protecting thousands of corporate users from the ravages of email-borne infection. We also provide an anti-porn service, which spares our customers from many of the problems that pornographic email attachments can cause.

At the core of our anti-spam service is a learning engine containing more than 1,000 rules, overlaid by artificial intelligence techniques based on statistical probability, similar to those already used for determining the probability of certain illnesses in patients. MessageLabs have pioneered using these established techniques in combating spam by searching for particular patterns

and characteristics within large volumes of junk email, and we have found this to be very successful in almost eliminating the numbers of false-positives. Currently the MessageLabs combined approach is more than 96 per cent accurate, only seldom mistaking legitimate email for spam.

The MessageLabs service is unique in that it allows you to set up and fine-tune your own filtering criteria, using a combination of public and internal white and blacklists. It also enables you to specify how all spam and suspect email is to be handled – whether quarantined in a designated safe inbox or disposed of on receipt at MessageLabs. This helps to free up your employees' time, as well as alleviating bandwidth issues and reducing the demands on your internal email systems for storage space.

Measuring the return on investment

The IT manager at one MessageLabs anti-spam customer, a major player in the aerospace industry with around 1,000 email addresses on its system, tells us that before signing up for our service his company was receiving around 15,000 unsolicited emails a month. That figure represented nearly 20 per cent of the company's incoming email traffic.

Now that they have the MessageLabs anti-spam service, the problem has completely gone away. Although what pleases the IT manager most is the obvious return on investment that this represents – fully validating the decision to invest in the service. His estimation of ROI went like this: if it takes an average of a minute, conservatively, to open an email, look at it and discard it, then 15,000 minutes of business time was being wasted each

month. At £20 per hour, that adds up to a cost of nearly £5,000 a month, so the ROI is plain to see in time saved alone.

Savings also follow if you are not having your bandwidth taken up by incoming spam. Similarly, pressure on storage space including backup media is markedly reduced. An increase in productive time spent by IT personnel is also a quantifiable improvement, when staff no longer have to waste time on firefighting the spam menace. Less easily measured, but nonetheless invaluable in terms of corporate peace of mind, is the enhanced protection from the possibility of legal action by employees who claim they are harassed by pornographic email content.

Potential cost of spam

<u>Number of Users</u>	<u>Lost Productivity (minutes per month)</u>	<u>Lost Productivity (per month)</u>
25	492	£164
100	1,966	£655
250	4,916	£1,639
500	9,831	£3,277
1000	19,663	£6,554
2000	39,325	£13,108
5000	98,313	£32,771

N.B. Using the March 03 figures for spam of 36.3%, for a company with the above numbers of email users (hourly cost approx. £20), each receiving on average 30 mails per day, taking an average of 5 seconds to read and delete spam emails.

So what conclusions can be drawn?

In 2002, in excess of 64 million spam emails were identified and intercepted by the MessageLabs anti-spam service on behalf of our customers. The evidence is all around that the spam menace is becoming ever more of a problem for business email systems.

Indeed, whether you measure the problem by your own experience of mounting spam incursions in your own inbox or by global statistics that track the massive rise in spam volumes, the picture is clear: the spam problem is getting worse almost by the day; and it's certainly not going to go away in the short term.

The determination of spammers to continue plying their dubious trade can be seen from the increasingly devious methods they are employing in order to defy anti-spam measures. Meanwhile, systems which deploy only one or another anti-spam technique have already been discredited as the spammers find their way round them.

Spammers aren't yet able to circumvent the newer statistical filtering methods, but as we have already seen, spammers are becoming more sophisticated, and as this level of sophistication improves, the only way to combat the problem will be to employ a combined approach to combating spam.

MessageLabs have found using a mix of the most advanced filtering methods, spam traps and honeypots, to be the best way to ensure that anti-spam technology stays one step ahead of the spammers. We've pioneered this approach in all our email security services at MessageLabs.

We believe that our anti-spam solution – filtering spam at the Internet level and keeping it well away from your business – is the only certain way to ensure the integrity, efficiency and reliability of your email system.

In 2002, in excess of 64 million spam emails were identified and intercepted by the MessageLabs anti-spam service.

Europe 1270 Lansdowne Court, Gloucester Business Park, Gloucester, GL3 4AB, UK
T +44 (0)1452 627627 F +44 (0)1452 627628

Americas 512 Seventh Avenue, 6th Floor New York, NY 10018, USA
T (646) 519 8100 F (646) 452 6570

Asia Pacific 1601, Tower 2, Lippo Centre, 89 Queensway, Hong Kong
T +852 2111 3650 F +852 2111 9061

Freephone UK 0800 917 7733
TollFree US 1-866-460-0000
info@messagelabs.com
www.messagelabs.com