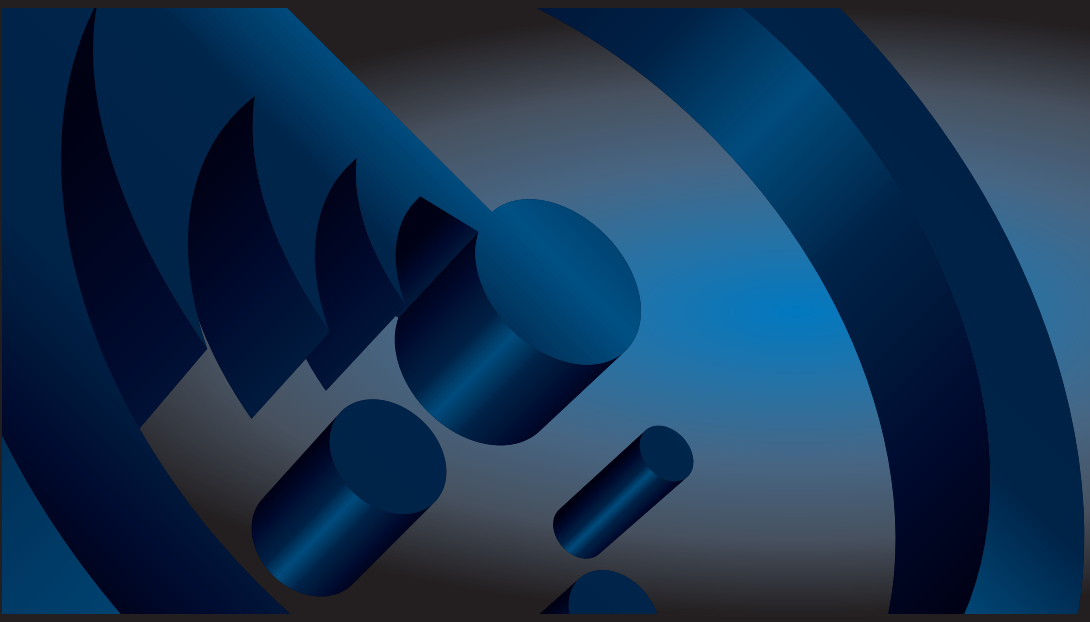
Spam Monitor Survey
Volume II

March 2004



CLEARSWIFT™

The MIMEsweeper™ Company

CONTENTS

PART 1 - SCOPE AND AIMS OF THE SURVEY 3

PART 2 - FINDINGS SUMMARY 4

PART 3 - DEFINITIONS & ABSTRACT 6

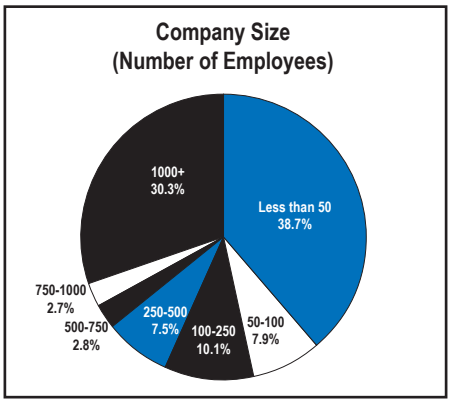
- Introduction 6
- What is spam? 6
- The cost of spam 7
- Anti-spam Technology 8
- Is legislation the answer to the spam problem? 8
- Is user education also part of the answer? 9

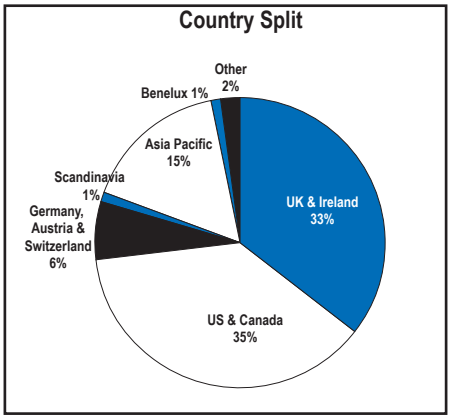
PART 4 - RESEARCH FINDINGS 10

- 1: The Changing Nature of Spam Messages 10
- 2: The New Techniques used by the Spammers 11
- 3: Anti-spam Techniques and Technologies 13
- 4: End-User Education 18
- 5: Anti-spam and the law 20

PART 1 - SCOPE AND AIMS OF THE SURVEY

This survey report is based on the input of 1,260 professionals at middle to senior IT management level who participated in an online study commissioned by Clearswift in October 2003.





The survey is representative of a cross-section of industry sectors and geographies. The largest groups of respondents were based in the USA (421), UK (398), Australia (148), France (92) and Germany (66). Responses were received from 45 countries in all. Respondents worked in small, medium and large organisations. 38.7 per cent worked in organisations of fewer than 50 people, 18 per cent in organisations of between 50 and 250 people and 30.3 per cent worked in organisations with over 1,000 people. The survey was made up of a total of 50 questions which were put into 3 specific areas: Technology, Education and Legislation.

The survey was hosted on the following web sites - clearswift.com, computerworld.com, computerweekly.com, cbronline.com, computerwoche.de and weblmi.com.

The survey was carried out by Clearswift. Clearswift, the MIMEsweeper company, has been developing content security solutions for over 20 years. Its world leading MIMEsweeper software is used by over 20 million people in more than 15,000 customer sites. IDC ranks Clearswift as the world's number one supplier of email filtering solutions (IDC report #29635R).

The research is sponsored by TRUSTe, an independent, non-profit privacy initiative dedicated to building users' trust and confidence on the Internet and accelerating growth of the Internet industry. It has developed a third-party oversight 'seal' programme that alleviates users' concerns about online privacy, while meeting the specific business needs of each of its licensed web sites.

Clearswift commissioned this survey in order to provide input to the company's strategic planning and its research and development programmes. The company wanted to gain in-depth understanding of email users' concerns about spam, how they were deploying technology, email education levels and best practice initiatives in order to combat the problem.

The spam market is growing and constantly changing. Spammers are becoming more sophisticated and despite legislative efforts aimed at curbing their activities, the volume of spam continues to grow. The US researchers The Radicati Group projects that the percentage of email classified as spam will grow from 45 per cent in 2003 to 52 per cent in 2004 - and will hit 70 per cent by 2007.

PART 2 - FINDINGS SUMMARY

The results of the survey provide compelling, detailed evidence that the spam problem has not been solved - both in terms of end-user best practice and vendor anti-spam solutions. There is still a long way to go in technology, legislation and education terms to tame spam completely.

Spammers v IT Departments - Who is Winning?
The nature of spam attacks is becoming more and more varied. The survey identified over 50 different types of spam attack - most of them aimed at harvesting email addresses. The most popular spam attacks were siphoning from the Website, Denial of Service and Open Relay.

The survey also highlighted inadequate email traffic monitoring by organisations. Almost a fifth of all respondents did not know whether or not they had been the victims of any kind of spam attack. Forty per cent did not know whether a third party had used their organisation as an Open Relay to send spam.

As to whether technology is deployed to stop spam, and whether it is effective - the answer to both questions is 'could do better'.

Twenty per cent of those surveyed had no spam defences whatsoever. Of those who did, only 32 per cent felt that such defences were adequate. The majority (55 per cent) felt that they were inadequate. An alarming 36 per cent of respondents never refined or reconfigured their spam filters. Only 14 per cent of those surveyed were involved in any of the anti-spam initiatives. The vast majority of these do not contribute to any anti-spam blacklist (or block list).

Web access appears to be an Achilles heel for many organisations, with 63 per cent of respondents not deploying any Web filtering software to stop spam.

End-User Education
The survey results strongly suggest that more productive efforts must be made to educate end-users in how to combat spam. The astonishing statistic that 84 per cent of respondents admit that their company has been blacklisted for sending spam clearly indicates that there is an urgent need for such education.

Over one third of those surveyed reported that their organisation did not have an anti-spam policy in place. Of those organisations who did have a policy, less than half communicated it to their employees. Few employees seem to report spam to the IT department - and even fewer organisations take action against staff who have responded to a spam offer.

The level of knowledge of the legal implications of email marketing is inadequate - with just below half of respondents describing it as 'poor'. The communication of these obligations to marketing departments is being carried out in only half of the organisations surveyed.

Anti-spam and the Law
Most people seem completely unaware of legislation enacted to prevent spam. Of those who are aware of anti-spam laws, the vast majority felt that these laws were inadequate. Some people clearly feel a desire to take legal action against spammers, but there is little evidence of such legal action actually being taken.

Respondents were quizzed on the details of the US CAN-SPAM Act of 2003. Most people felt that adult/pornographic spam should be labelled 'adult advertisement' and that all other spam should be labelled 'advertisement'. Two-thirds of respondents supported the 'safe harbour' protection for standards-compliant commercial emailers. 89 per cent of those surveyed supported a 'do not email' registry - but were divided on whether emailers who spammed those on the registry should be criminally prosecuted.

PART 3 - DEFINITIONS & ABSTRACT

Introduction

Over the last two years the prevalence of spam and the emergence of new virus strains have highlighted the growing burden on IT as a means of managing electronic communications. Email has become the essence of work, and ensuring it is continually working is now mission critical.

Content security and content filtering are key components of a layered security model. Email, by design, passes through firewalls and intrusion detection, but as recent events - such as the MyDoom virus outbreak - have shown, this is not enough to guarantee safety. Organisations need to rely on strong content security and filtering mechanisms to provide vital additional safeguards.

The problem of spam, virus infiltration and other individual email-borne threats are not mutually exclusive. They all fall under the umbrella of content filtering and content security, which means that only a holistic solution can really help business to negate the threat in its entirety.

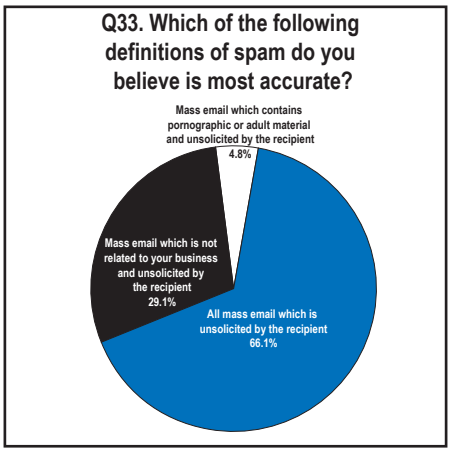
Spam is becoming more dangerous, with two new trends raising the stakes. Firstly, virus authors are using spam email techniques - in a recent example, a spam email containing a Trojan horse program was used to help spread the latest version of the Mimail email worm. Consequently, companies are realising they have to protect themselves from spam just as much as from viruses.

Secondly, 'phishing' is growing rapidly. Phisher scams tend to use spam email to drive unwitting Internet users to fake web sites where their information is captured. In July 2003, the FBI warned there had been a rise in such scams since the beginning of the year. Critically, with phishing it is difficult to tell that the email is a fraud. As with spam, email from phishers usually contains spoofed FROM and REPLY TO addresses to make the email look as though it came from a legitimate organisation. The email is usually HTML based, so to the undiscerning eye the email bears the authentic trademarks, logos, graphics and URLs of the spoofed organisation. Within hours, or even minutes, of account number and related password information being supplied by the unsuspecting Internet user, unauthorised transactions will begin to appear on the compromised account. Phishing is basically spam - yet another reason why corporates are realising they need a very good content security solution that doubles as a top-flight anti-spam solution.

Spam email is at best a nuisance and at worst an insidious first step in corporate and personal theft. Refining and applying best practice email management procedures, along with the deployment of effective anti-spam technology is now becoming mandatory for all organisations.

What is spam?

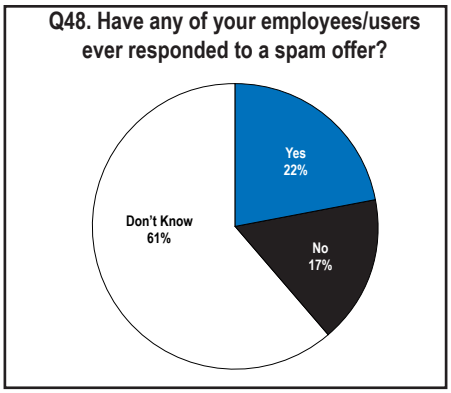
More than 66 per cent of our respondents agreed that the definition of spam they believe to be the most accurate is: 'All mass email which is unsolicited by the recipient'. Twenty-nine per cent were happier with this definition: 'Mass email which is not related to your business and unsolicited by the recipient'.



The fact that not everyone agrees on the best definition for spam has contributed to the difficulties facing legislators around the world. It is true that much spam is universally recognised as such, but defining exactly what is spam and what isn't can be problematic. For example, a blanket ban on emails containing the word 'Viagra', would not be helpful to a pharmaceutical research and development department working on a new version of the drug. A 'one-size-fits-all' anti-spam solution can never be totally successful. The only efficient way to deal with spam is to use a solution that allows companies themselves to determine what is or isn't spam to them.

The cost of spam

The cost of spam to those who transmit spam is very small. The costs to the recipients can be large and multi-faceted. The ever increasing volume of spam email increases network, storage and bandwidth costs. Managing spam at the desktop takes time and reduces employee productivity. Offensive spam email can result in litigation, fines and the financial consequences of loss of reputation. Finally, spam can lead to individual and corporate theft.



The fact that spam is cheap to send out means that it is here to stay. Spammers need only a very few people to answer their emails in order for it to be worth their while. In our survey, 22 per cent admitted they had responded to a spam offer. In reality, where spammers are mass mailing out millions of emails, very small response rates net them significant profits. In addition, with the new techniques they are now using (i.e. sending viruses to infect machines, so they can send spam from other people's machines without their knowing about it), it is becoming increasingly cheaper for spammers to continue their activities.

While costs such as the consumption of bandwidth, network and computing resources to deal with spam seem obvious, the major cost of spam to companies is the huge burden it places on IT administration. Spam is responsible for vastly increased numbers of emails coming through the gateway, and IT administrators have to manage much higher traffic rates than they would otherwise have to. They also have to manage the extra storage being employed. Hours and hours are eaten up looking through quarantined emails and deciding which to let in and which to block. In addition, there is the time spent in investigating emails that have been blocked which may perhaps be legitimate.

Dealing with spam attacks also takes up considerable IT administration. Our survey revealed over 50 different categories of spam attacks - each requiring its own time consuming remedial activities.

In 2003, The Radicati Group estimated that by the year end the worldwide financial loss resulting from spam would be over $20.5 billion. Radicati estimates this annual cost will reach over $198 billion in 2007. The European Union estimates that spam currently costs Internet users up to £5.5 billion per year.

Anti-spam technology

The anti-spam market is swamped by vendors, with new products appearing almost daily. This presents a number of problems for those looking for an anti-spam solution. First of all, it makes it very difficult to find the one that is right for your individual business. Secondly, it is too easy to be lured into buying a really cheap solution - only to then discover it is absolutely useless. There is a real need for customers to buy solutions from reputable companies that are here to stay. All the analysts agree that the anti-spam market is going to see a huge amount of consolidation, meaning that several companies will be acquired and the majority of the others will just go broke. The Radicati Group recently identified Clearswift as one of the top five anti-spam vendors in the world. It has the number one email filtering product in the world and, with its history of being the pioneer that created content filtering, Clearswift understands the spam problem better than anyone else.

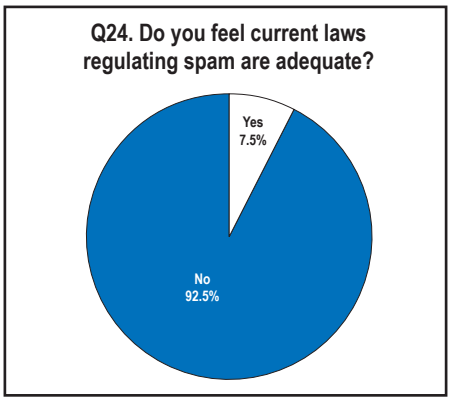
As far as anti-spam technology is concerned, many suppliers are making outlandish claims about their products - most of which cannot be verified. It is not enough to claim that a product blocks all spam, because these products may well be blocking significant quantities of legitimate emails as well.

Some companies (17 per cent in our survey) rely on their ISP to stop spam. This is not a good approach as 'one-size-fits-all' does not work. What organisations need to realise is that spam is a content filtering problem. It can no longer be considered in isolation from other content filtering threats. Virus writers are using spam and spammers are using viruses to help each other. This is truly a content filtering problem and we need to make sure anti-spam defences are considered in the overall context of a layered security strategy. What's more, anti-spam defences cannot rely on one technique alone - to be efficient you need to adopt a number of complementary techniques, allied to a regularly updated datafeed of new spam to be blocked.

Vendors have been applying new anti-spam technology to their products since our last spam survey in July 2003. Some of this showed up in the survey, with a fifth of email users adopting a heuristic-based approach. Clearswift, and others, have introduced probabilistic analysis using a Bayesian classifier into their products. Clearswift has also introduced an automatic three hourly spam update service. (These approaches are expected to show up in next year's survey of email users).

Is legislation the answer to the spam problem?

Email users are unequivocal about whether current laws regulating spam are adequate. More than 92 per cent felt that they were not, and the recent AOL spam lawsuit dismissed in the US shows email users have good reason to be sceptical. A US Federal Judge in the Eastern District of Virginia ruled that AOL had failed to show Virginia had jurisdiction over the Florida-based defendants simply because AOL's business is located in Virginia and the alleged bulk emails had gone through that state. The AOL case failed on a legal technicality between one US state and another! Clearswift believes that only through consistent enactment and enforcement of legislation by governments throughout the world can spam legislation can be effective.



At the OECD spam workshop in Brussels in February this year however, it was clear there was no consensus on whether spam should be fought by an opt-in or opt-out approach. For example, the US CAN-SPAM Act is based on the opt-out principle, whereas the European Data Protection Directive prescribes an opt-in approach.

In November 2003, Microsoft offered a $250,000 reward for information leading to the arrest of the writer of the SoBig virus. In January, Microsoft offered a similar $250,000 bounty for the arrest of the author of MyDoom. These 'Wild West' tactics hardly amount to a vote of confidence that legislation will deter creators of spam, viruses, worms, and other malicious code.

Is user education also part of the answer?

A general need for organisation-level education of email users and specific education for marketing teams clearly exists. Any marketing person is potentially a spammer. If such staff are not educated in how to use email marketing in an acceptable way, they will simply add to the problem. With 84 per cent of email users in the survey admitting that their company had been blacklisted for sending spam, it is obvious that considerable education is still required.

Legislation, such as the US CAN-SPAM Act of 2003, codifies the practices that all legitimate US marketeers must now follow. It mandates that unsolicited commercial emails are labelled and that opt-out instructions must be included in the message. All US marketing staff will have to be educated to ensure that they comply with the CAN-SPAM Act, which took effect on 1 January, 2004.

PART 4 - RESEARCH FINDINGS

1: The Changing Nature of Spam Messages

The survey we conducted last year showed up the reality that spam was a huge, multi-faceted problem impacting on employee productivity, network bandwidth, storage requirements, processing cycles, virus infections and legal liabilities. The survey also confirmed that spam affected every company, and that spam costs money.

The content of spam is ever changing and Clearswift has tracked this in its monthly 'Spam Index'. Between June 2003 and January 2004, spam content changed substantially (for example, healthcare spam grew from 18 per cent to 43 per cent during this period).

The nature of spam has also been changing. In October 2003 Clearswift reported that it had identified a new entrant into the spammed products range - spy software or spyware. Spyware, which is both easy to deploy and readily available, also brings another potential threat - corporate espionage.

Following the announcement of chatroom closures by Microsoft, Clearswift's research department picked up on a blatant attempt to increase the vulnerability of minors to Internet stalkers. About 15 per cent of spam email blocked overnight by Clearswift's spamActive™ software contained the subject line: 'MONITOR your Kids on the Internet with Spy Software', advertising a product which allows users to spy on anyone just by sending them an e-greeting card.

Clearswift believes that the large increase in spam volumes in 2003 is, in no small part, due to the installation of proxies by the mass-mailing worm SoBig. SoBig's intent is to steal usernames and passwords. Phishing spam increased enormously in the last quarter of 2003. In its simplest form the email itself may have an HTML form that requests verification of bank account details.

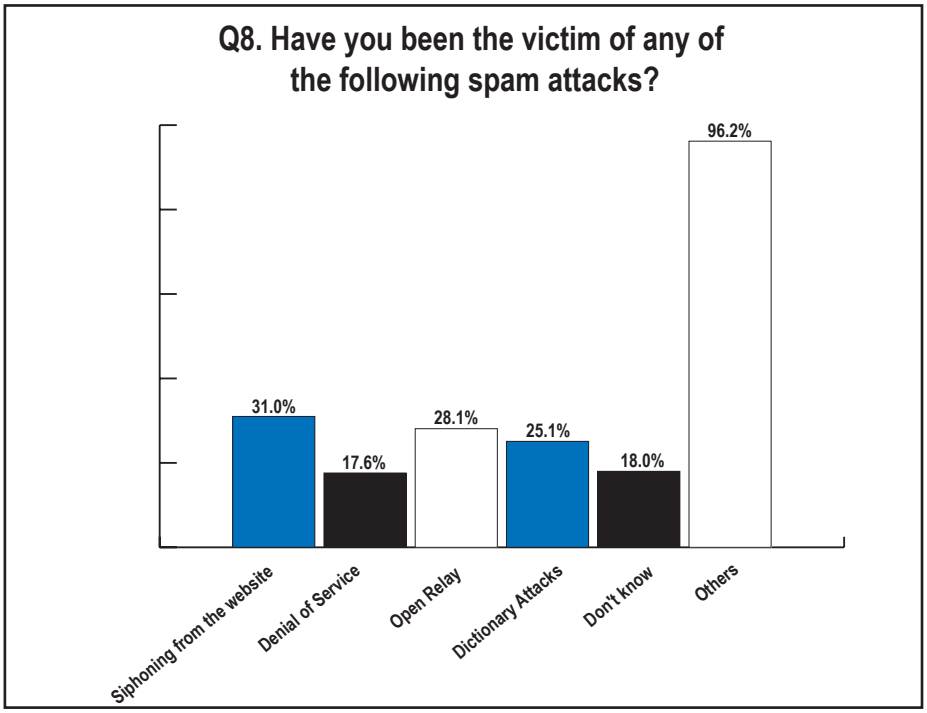
In January 2004, the mass-marketing worm MyDoom generated even more email volumes than SoBig. MyDoom's intent was to steal passwords and to enter people's PCs via a 'back door' in order to control the machines remotely.

Spyware, SoBig, MyDoom and phishing move the spam phenomenon even deeper into the criminal world.

Spam has also developed a seasonal element. For example, during the run-up to Christmas 2003 there were volumes of spam detailing financial packages to help people pay for presents. This is called social engineering and is a technique also widely used in the run-up to Valentine's Day, Mother's Day, Thanksgiving, and so on.

2: The New Techniques used by the Spammers

This section of our new survey reviews the new techniques used by spammers to get around anti-spam software and trick people into opening messages and attachments.



Email users were given a list of spam attack types and asked to say whether they had been victims. The more common forms of spam attacks were siphoning from the website, denial of service and open relay. The nature of spam attacks is becoming more and more varied. For example, the 96 per cent of 'others' included more than 50 different further types of attack mentioned by respondents. Most of these techniques were aimed at harvesting email addresses. This demonstrates the level of commitment by spammers to penetrate email users' defences. It also demonstrates just how difficult it is to keep up with the spammers and to maintain adequate defences. Spam management is just one of hundreds of tasks that the IT manager has to deal with, and consequently it is a major challenge to combat spam's dynamic nature.

The most effective way to stop spam is by using a layered approach, and it is encouraging to see that the majority of respondents have recognised this necessity with 21 per cent using heuristics and 19 per cent using statistical filtering to block spam. This shows that people realise they need to use more sophisticated techniques which will allow them to decide what is and isn't spam. 'One-size-fits-all', static anti-spam solutions will not give users the results they want.

Siphoning from the Website

This involves a range of techniques which are used maliciously to steal another website's traffic - very often for the purpose of acquiring email addresses. Nearly a third of respondents admit to being aware that they have been victims of siphoning. There is almost no way of preventing spammers from getting email addresses from company websites, especially as more and more software is developed to help spammers to siphon addresses from various sources. Techniques used include the wholesale copying of web pages (with the copied page altered slightly to direct visitors to a different site, and then registered with the search engines) and the use of keywords or keyword phrases 'belonging' to other organisations, companies or web sites.

In fact, more and more spam is being received which is about spam itself. In Clearswift's monthly Spam Index for August 2003 spam about spam rose to 4 per cent of the total of all spam received.

Denial of Service
A denial of service (DoS) attack, is an incident in which the user organisation is deprived of email and/or website access because of malicious and deliberate actions by a third party.

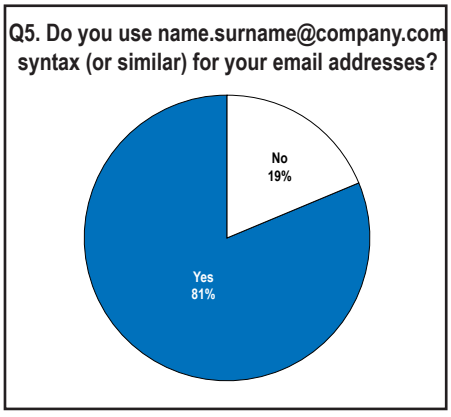
The figure of DoS attacks (18 per cent) demonstrates that the nature of spam is changing (e.g. more and more spam is now used to propagate viruses). Indeed, virus writers and 'script kiddies' are now using spam to infect machines with all sorts of viruses. Spam is also used to trick people into divulging personal and financial information.

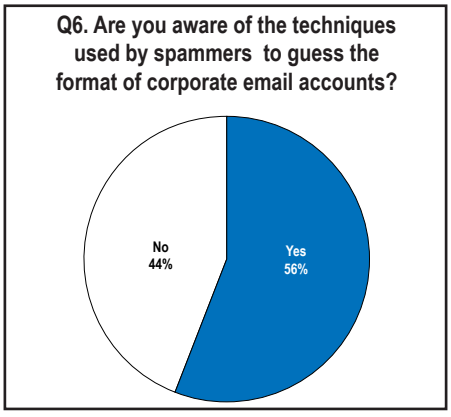
Open Relay
An open relay is an SMTP email server which allows third party relay of email messages. It allows an unscrupulous sender to route spam through someone else's system without their knowledge - and at no cost to the sender.

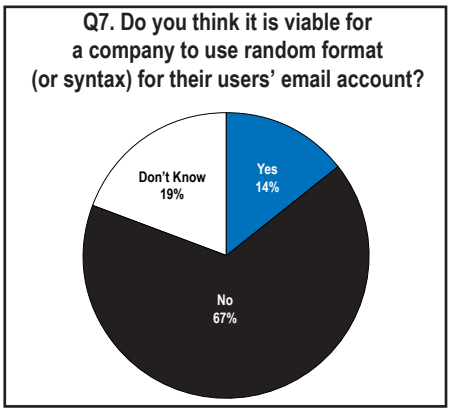
The 28 per cent of respondents who suffered from open relay attacks illustrates how spammers are using increasingly sophisticated techniques to make sure they can send their emails and to make them extremely difficult to trace. It also questions the effectiveness of legislation, as spammers use more and more advanced techniques to hide their traces.

An incredible 18 per cent of respondents did not know whether they had been victims of any kind of attacks or not. This is a worrying figure and suggests that not all IT managers and administrators have grasped the problem and the serious consequences it can have.

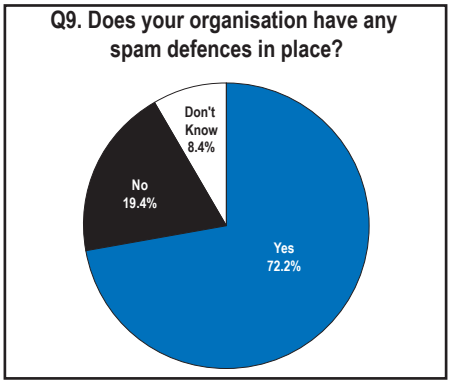
The following three charts demonstrate how vulnerable companies are to techniques used by spammers. While many people have suggested using non-standard syntax for email addresses, it is clear this is not really a practical option for most businesses as it would be far too time consuming and costly to change them.

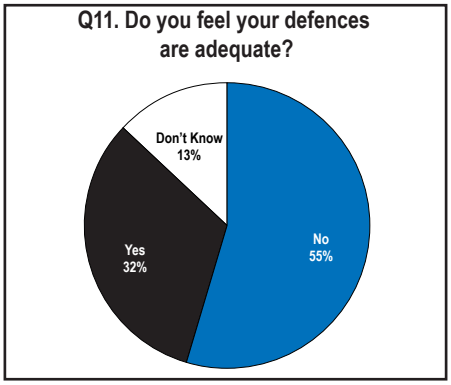






3: Anti-spam Techniques and Technologies

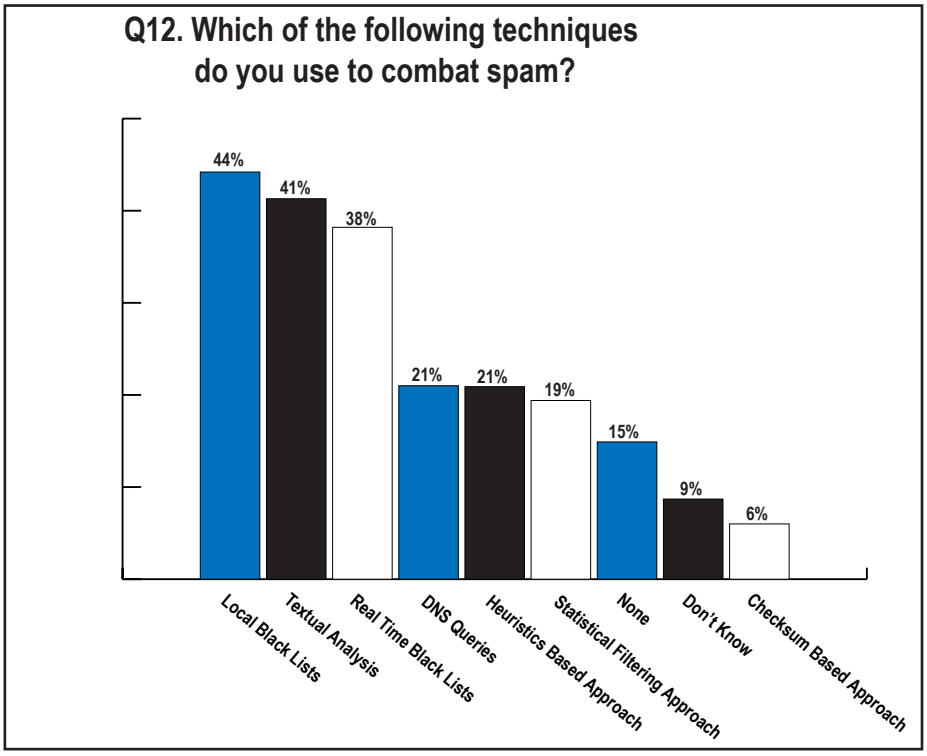


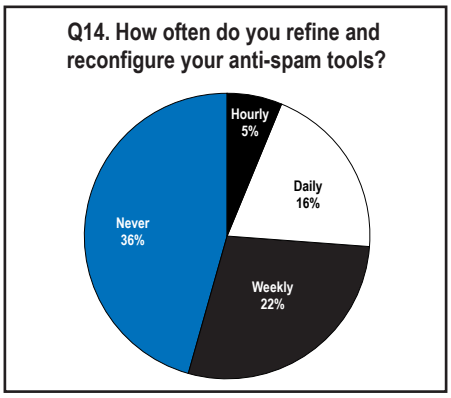


Despite abundant media coverage on spam, almost 20 per cent of respondents still do not have any kind of spam defences. Goodness only knows what impact this has on their IT resources. For those with spam defences in place, 55 per cent of respondents say their defences are inadequate.

It shows again that the one-size-fits-all solutions proposed by most anti-spam vendors simply do not work. These static anti-spam products lure IT managers into thinking they can solve their spam problems overnight, when this is actually not the case. To be effective, anti-spam defences need to be tailored to each company. Otherwise, they will end up being just another burden on the IT manager's time (with lots of quarantined emails and false positives).

These figures are consistent with those of Clearswift's Spam Monitor Report published in June 2003. They show that users need to upgrade their thinking on spam and look to more sophisticated anti-spam technologies for an answer to their problems.





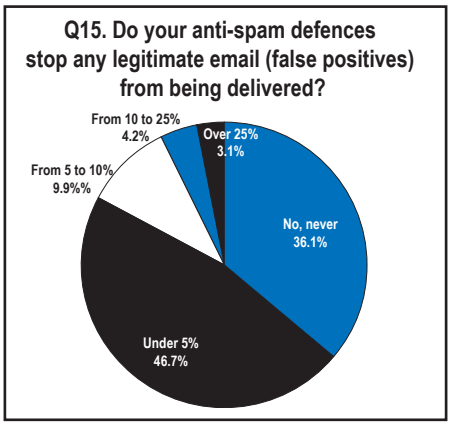
The most popular techniques being used to combat spam are real time black lists (38 per cent), local black lists (44 per cent) and textual analysis (41 per cent). These techniques are the hardest to implement as they are very time consuming and require regular updating. Clearswift spamActive's automatic three hour blacklist updating removes much of the burden on its customers of keeping the blacklist current.

Over the last year, we have seen a series of subtle changes in the nature of spam. We have also seen a number of big changes - such as the fact that virus writers are now using spam as the vehicle to infect machines.

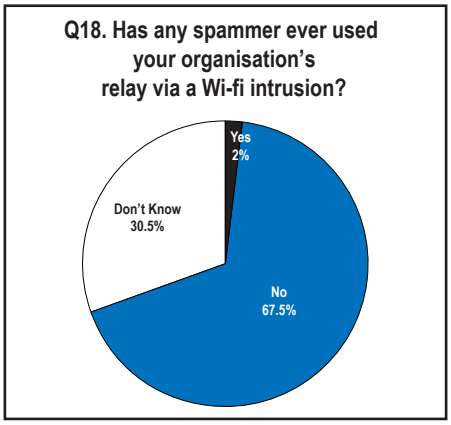
For anti-spam tools to be effective, they must be capable of being refined and reconfigured, and users must make use of the dynamic capabilities that such tools possess. Having a service feed component to a solution is essential when it comes to spam, as the tool must be updated with new spam information on a regular basis. The Clearswift 3-hourly updated spamActive datafeed is a good example of this.

However, only just over 20 per cent of email users refine/reconfigure their anti-spam tools on at least a daily basis. A worrying 36 per cent NEVER do this.

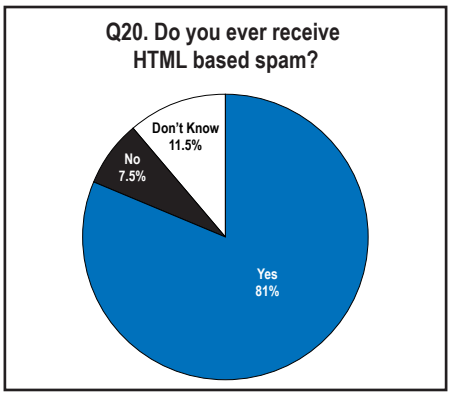
Static anti-spam solutions can never be very effective in an environment where the nature and content of spam changes every day. In 2003, Clearswift introduced a "learning" anti-spam software solution. The out-of-the-box spam detection rate of 92 per cent improves over time, as the software 'learns' about the organisation's email.



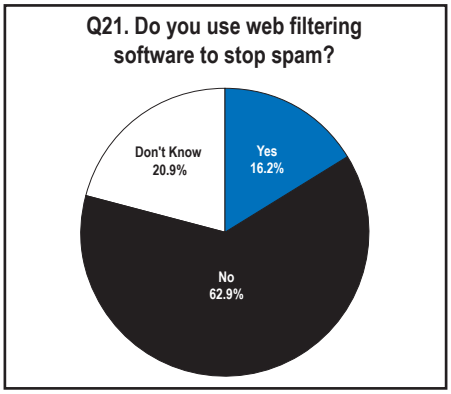
The problem of blocking legitimate emails (false positives) is clearly not going to be solved with a one-size-fits-all anti-spam solution. Just over four per cent of email users report a false positive rate of between 10 per cent and 25 per cent, while 3.1 per cent suffer an incredible rate of over 25 per cent! The administrative burden of trying to sort out such high rates of false positives is clearly unacceptable. What is needed is a solution which can be tailored and constantly refined to each organisation's specific needs. Clearswift's technology offers a customer-proven 0.01 per cent false positive rate.



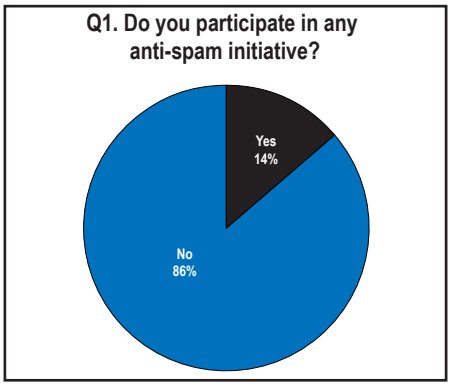
Just over two-thirds of email users reported that no spammers had ever used their organisation's relay via a Wi-Fi intrusion. However, a worrying 30.5 per cent did not know whether they had been attacked in this way or not. This is another example of where organisations could be unknowingly propagating spam because they are not adequately monitoring what is happening within their IT systems. This ignorance makes it easy for a spammer to use the organisation's relay via a Wi-Fi intrusion.



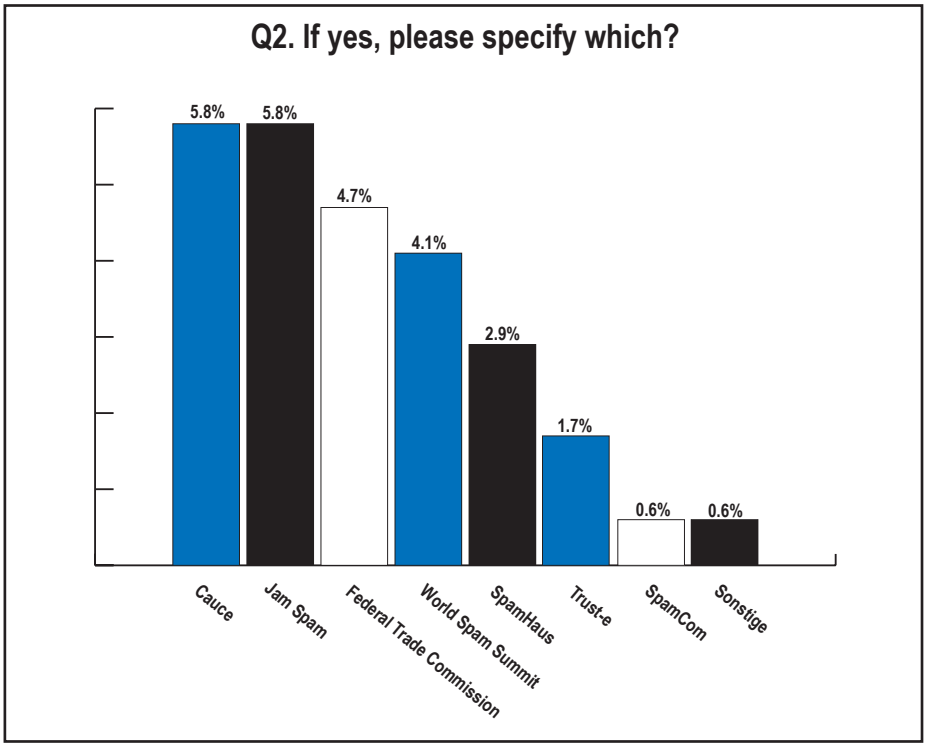
A very high proportion of users (81 per cent) admitted they had received HTML-based spam. These messages typically include graphics, and it is the HTML portion that generates a return message from the user to a web site to retrieve the graphics. This is what is called the 'web Beacon' phenomenon. With the use of preview panes, the user unwittingly lets the spammer verify the validity of the email address without opening the email message. These email messages are larger than normal and use up even more IT storage and bandwidth. Spammers also use HTML email because graphics help them sell more goods and services.



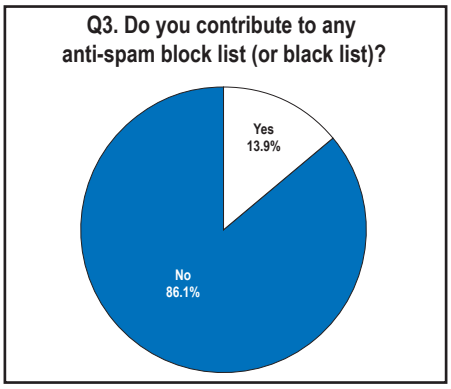
There appears to be a real gap in email users' anti-spam armoury when it comes to web usage. Almost 63 per cent of respondents do not use web filtering software to stop spam. There is clearly an education gap concerning this issue.



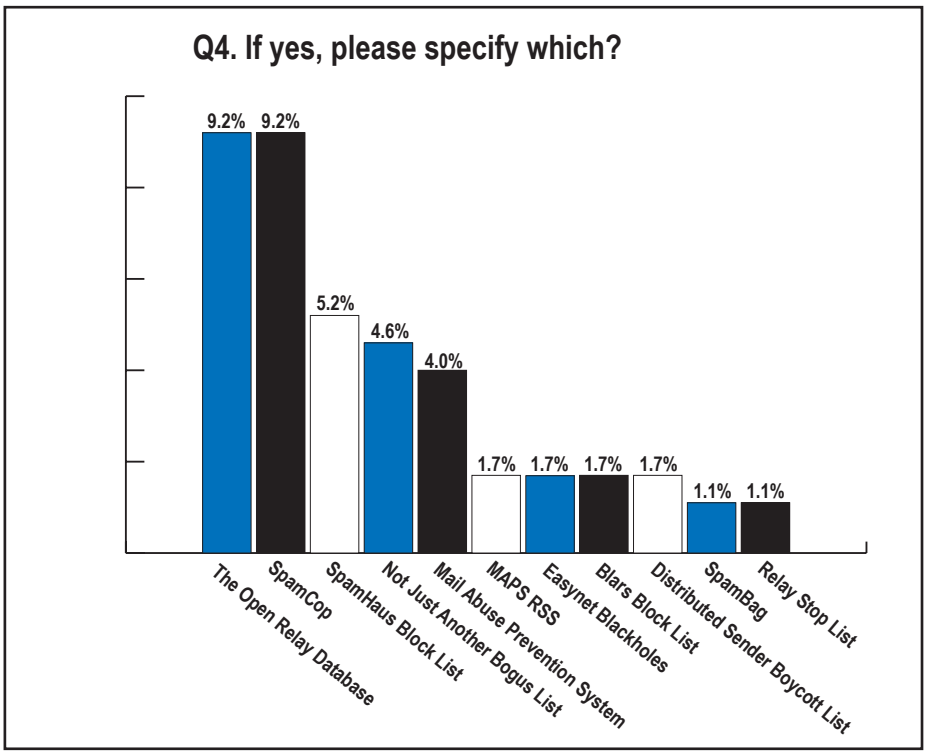
The small number of respondents (14 per cent) who are participating in anti-spam initiatives is a cause for concern. One could presume this low take-up is because these anti-spam initiatives are perceived as ineffective or because users are not aware of them. Of those respondents who do participate, there is a fairly even spread across nine different initiatives.

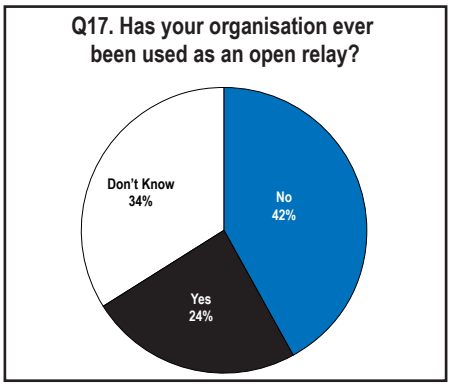


Taking part in these initiatives is key to IT Managers understanding the spam problem, especially as several vendors are making wild claims about their anti-spam capabilities. Clearswift takes the role of education and participation in anti-spam initiatives very seriously and is involved in many industry and government debates.

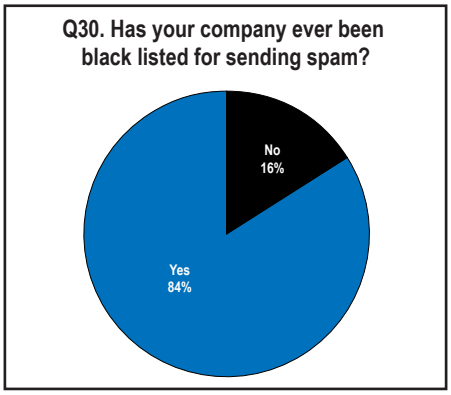


More than 86 per cent of respondents said their organisation does not contribute to any anti-spam blacklist (or block list). This highlights the lack of commitment of some IT managers to really solve the spam problem. Almost half of them admitted to using blacklists to stop spam, but very few of them contributed to them. This means that they rely on others to do the job. They should be more proactive. Clearswift's spamActive approach encourages user blacklist submissions which Clearswift verifies and shares with the MIMEsweeper user community.

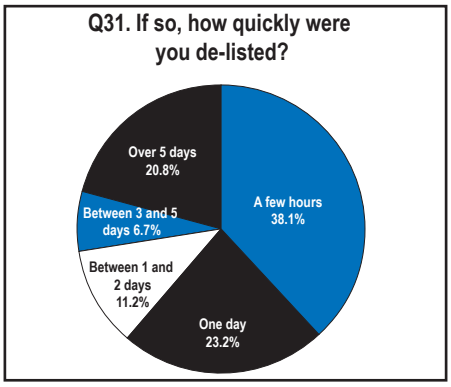




The fact that 40 per cent of respondents are not aware of whether their organisation had been used as an Open Relay, could help to explain why so many companies have been blacklisted for sending spam (see below). This suggests that IT managers are not aware of the techniques being used by spammers to send spam. It also shows they are not actually studying their email traffic flow. Close monitoring of outgoing email traffic would spot a third party's use of open relay at an early stage, and a good reporting tool - such as that in MAILsweeper Business Suite - would monitor and document this email flow.

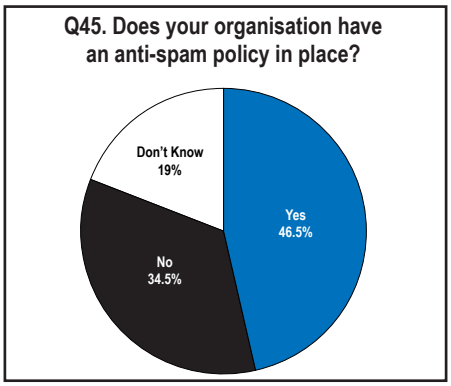


Being blacklisted for sending spam can cause major disruption. Email is mission critical and being without the ability to send email has serious and expensive consequences for any business. There are two main reasons why companies get blacklisted. The first is that spammers are using the company's open relay, which means that the IT manager has a mis-configured system. It also means the organisation is unaware of the nature of its email traffic flow. The second reason is that it could be due to excessive email marketing. Education is needed here, but IT managers could also prevent this if they regularly studied email traffic flow.

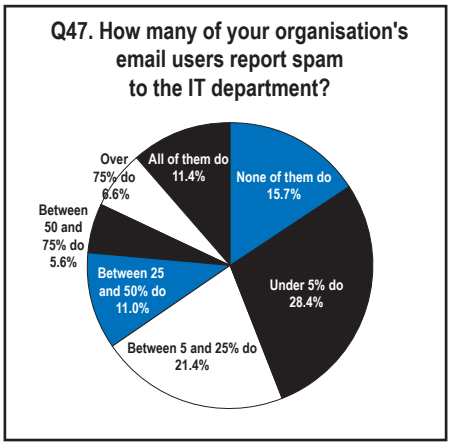


It took a day or more for 61.9 per cent of the organisations affected to be removed from the blacklist and 21 per cent of the blacklisted organisations stayed on the list for over five days. This is clearly unacceptable in an world that depends on electronic communications.

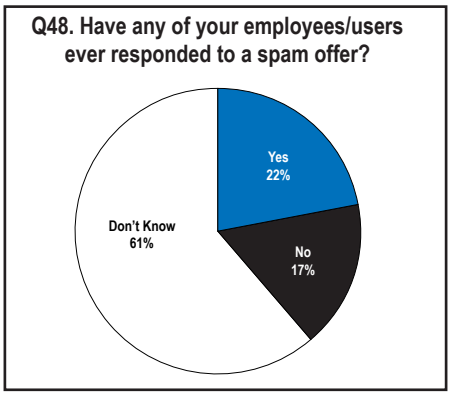
4: End-User Education

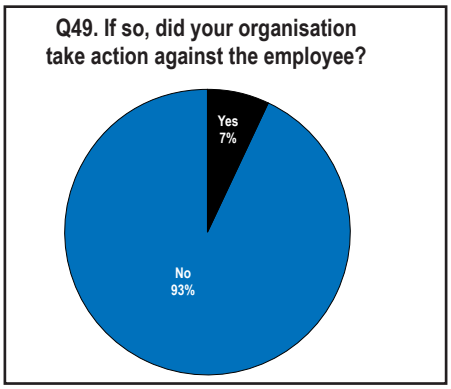


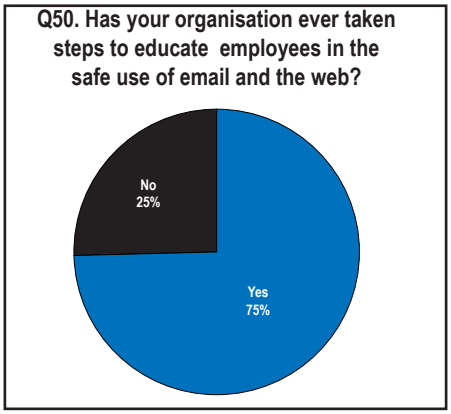
More than 34 per cent of respondents reported their organisation did not have an anti-spam policy in place and 19 per cent didn't know whether they had one or not. Without a policy in place it is hard for an organisation to combat any sort of threat, since it makes a company-wide best practice response and/or a programmatic response impossible. Of those organisations with anti-spam policies in place, only 43 per cent were aware of the policy being communicated to employees. 57 per cent either confirmed that the policy was not being communicated or did not know. Spam is a problem which software and the IT department cannot deal with alone and education of users is vital. It will take a co-ordinated continuous collaborative effort by end-users, IT professionals, email administrators and software to combat the problem.



In 65.5 per cent of our respondents' companies, fewer than 25 per cent of their email users bother to report spam to the IT department. It is clear that there is not a lot of collaboration in combating spam in most companies.





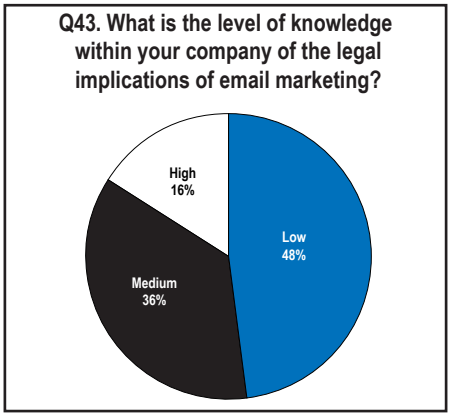


While 22 per cent of our respondents said users in their organisation have replied to a spam offer, only 7 per cent of organisations have taken any action against employees who have responded to spam email.

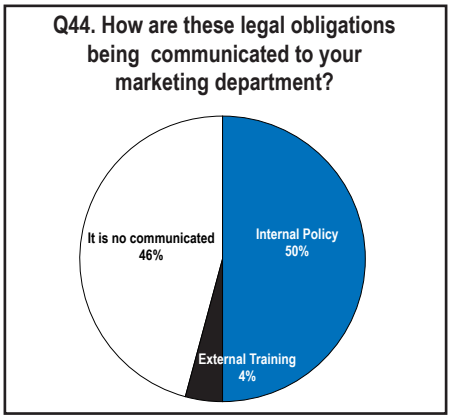
This may indicate that organisations are ignorant about employees responding to spam. It could also indicate that organisations see no value in punishing an employee in order to deter others. It also shows that employers are not educating their employees on dealing with spam.

A quarter of respondents admitted that their organisations had never taken steps to educate employees in the safe use of email and the web. These organisations do not understand the serious implications of not doing so - it can lead not just to higher IT costs, but, more importantly, to serious litigation.

Clearly, a large proportion of companies (44 per cent) use email for marketing purposes. Nobody can deny the fact that it works, and companies who act responsibly should be able to use this means of communication. However, the consequences of doing so without education are quite serious.



Only 16 per cent of companies rated their organisation's knowledge of the legal implications of email marketing as 'high'. One could deduce from this that organisations are inadvertently spamming because of ignorance of email marketing legalities. This is obviously an education and training issue, however, when asked how the legal obligations were being communicated to the marketing department, 46 per cent responded that they were not being communicated. This communication deficiency urgently needs to be addressed and eliminated.

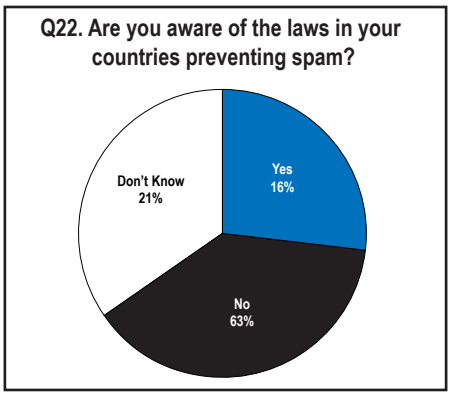


75 per cent of respondents reported that their organisations had taken steps to educate employees in the safe use of email and the web. After studying the results of this survey, one has to question what these steps were and how effective they have been.

The very clear evidence from this survey is that organisations could do a lot more when it comes to combating spam. For one thing, the vast majority of organisations surveyed have themselves contributed directly to the spam problem. With an incredible 84 per cent of respondents admitting to having been blacklisted for sending spam.

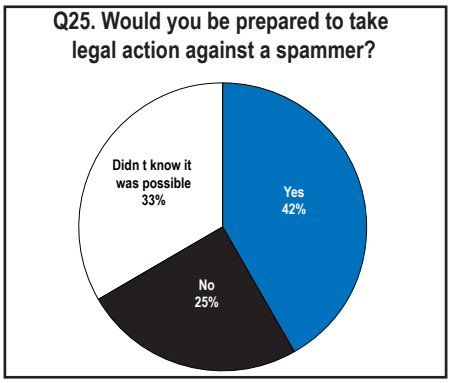
5: Anti-spam and the law

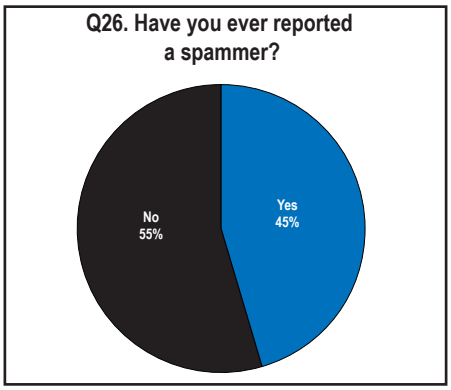
More than 83 per cent of surveyed users were completely ignorant of the anti-spam laws in their country. This is surprising given the high-profile legislation enacted in the USA, Australia and the UK. It is clear that government agencies need to do more to ensure that companies are aware of these laws.

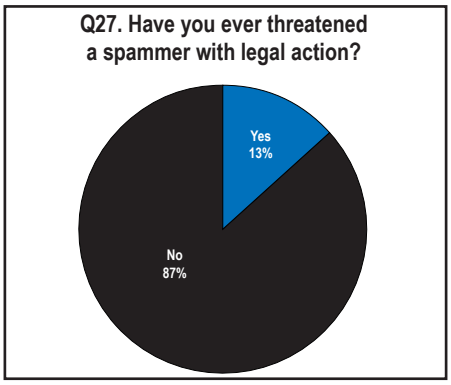


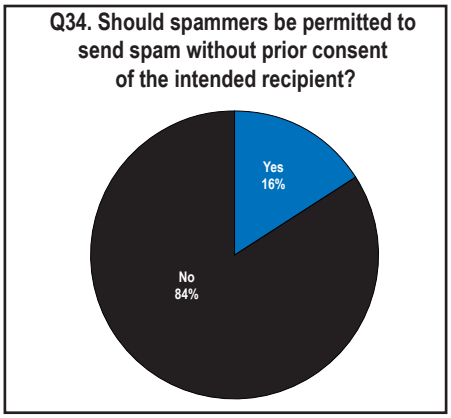
Among those who were aware of anti-spam legislation, a resounding 92.5 per cent felt the laws were inadequate. Given the knowledge that the majority of spam does not originate from the country in which it is received, it is hardly surprising there is scepticism as to the effectiveness of existing legislation.

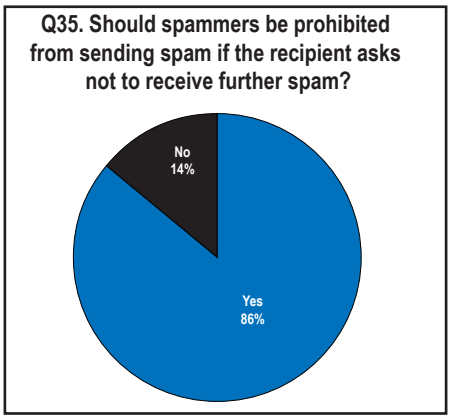
While 42 per cent of users reported











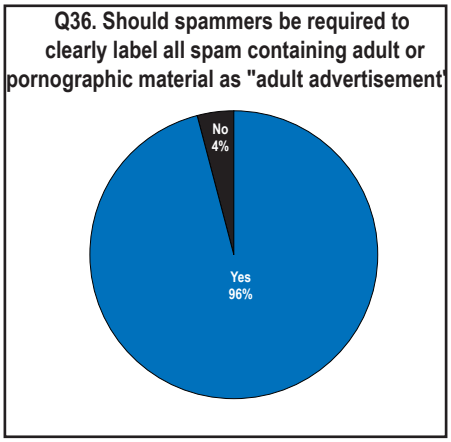
that they would be prepared to take legal action against spammers, a sizeable group of others (33 per cent) did not realise it was possible.

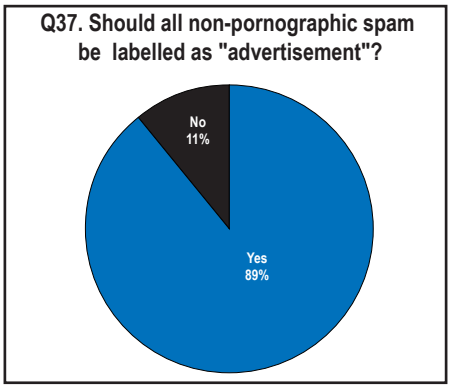
The sizeable desire for tougher legislation indicates the degree of animosity that exists against spammers.

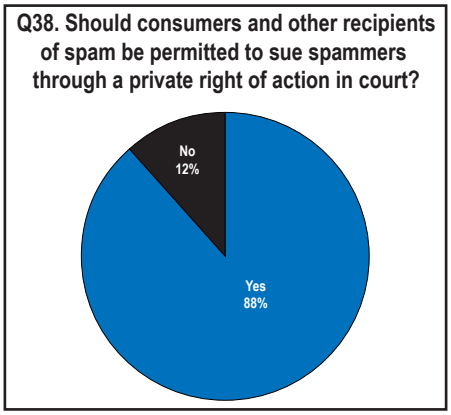
Organisations seem to be prepared to take action. The only problem is that the legislation is so ineffectual that doing so would probably be unsuccessful.

The recent failed AOL case is a telling example. Not only is the law different in every country, it is also to interpret and it is easy to find loopholes to circumvent it.

Most email users (84 per cent) felt that spammers should not be permitted to send spam without the prior consent of the intended recipient. A similarly sized majority also thought spammers should be prohibited from sending further spam if the recipient asks not to receive it. This highlights the issues surrounding the opt-in and opt-out clauses. Opt-out options are much less efficient than opt-ins. Opt-out puts all the burden on the actual recipient, which is not really fair as often the relevant clauses are hard to find (displayed in small print). This is definitely an advantage to the spammers. The results also show the need to provide proper unsubscribe facilities. Unfortunately, as spammers use the unsubscribe process merely to verify email addresses, this is unlikely to be of any help in combating spam.
The following range of questions were



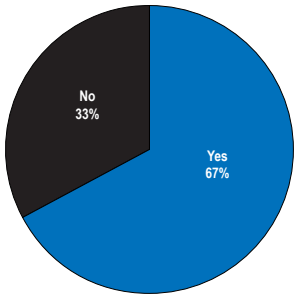




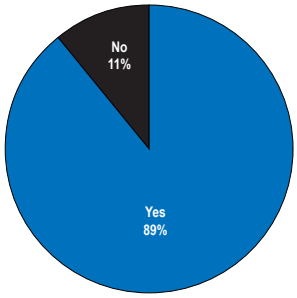
asked which directly related to specific clauses of the US CAN-SPAM Act of 2003.

Unsurprisingly, most email users felt

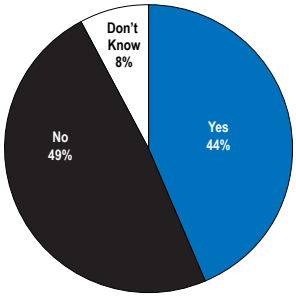
Q39. If senders of commercial email abide by industry standards that are approved by governmental regulatory agencies, should they be protected from criminal penalties and private lawsuits under an industry standard "safe harbour"?



Q40. Should consumers and business recipients of spam be permitted to register their names and email addresses with a governmental agency as part of "do not email" registry?



Q41. If yes, should spammers be subject to criminal prosecution if they email anyone listed in the registry?



that spammers should be required to label all spam containing adult or pornographic material clearly as 'adult advertisement'. A similar majority thought that all non-pornographic spam should be labelled as 'advertisement'.

There was clearly some sympathy for legitimate, responsible emailers. 67 per cent felt that senders of commercial email who abide by industry standards (approved by regulatory agencies) should be protected from criminal penalties and private lawsuits under an industry standard 'safe harbour'.

A large majority of users (89 per cent) thought that consumers and business recipients of spam should be permitted to register their names and email addresses with a government agency as part of a 'do not email' registry. However, email users were evenly divided on whether spammers should be subject to criminal prosecution if they emailed anyone listed in the registry.

CLEARSWIFT™

The MIMEsweeper™ Company

EUROPE

United Kingdom
1310 Waterside
Arlington Business Park
Theale, Reading
Berkshire, RG7 4SA
UNITED KINGDOM
Tel: +44 (0) 11 8903 8903
Fax: +44 (0) 11 8903 9000

Germany
Amsinckstrasse 67
20097 Hamburg
GERMANY
Tel: +49 40 23 999 0
Fax: +49 40 23 999 100

France
54-56 Avenue Hoche
75008, Paris
FRANCE
Tel: +33 1 56 60 58 00
Fax: +33 1 56 60 56 00

Sweden
Frösundaviks allé 15, 4tr
SE-169 70 Solna
SWEDEN
Tel : +46 8 50 90 40 78
Fax : +46 8 655 26 10

AMERICA

West Coast
15500 SE 30th Place
Suite 200
Bellevue
Washington, 98007
UNITED STATES
Tel: +1 425 460 6000
Fax: +1 425 460 6185

ASIA PACIFIC/JAPAN

Australia
Ground Floor
165 Walker Street
North Sydney
New South Wales, 2060
AUSTRALIA
Tel : +61 2 9424 1200
Fax : +61 2 9424 1201

Japan
Eisho Takanawadai Bldg 6F
2-11-8,
Minato-ku Shiroganedai
Tokyo-to, 108-0071
JAPAN
Tel : +81 (3) 5423 8171
Fax : +81 (3) 5423 1274

www.clearswift.com