Spamming and Scamming: The Real Picture!

AIDEEN KEANEY* AND DAN REMENYI[1]**

Derivation of Word Spam

This paper discusses the current phenomenon of spam, assessing its cost to organisations and describing some of its impact on the University of Dublin. It also argues that more research needs to be undertaken by academics in order to combat this phenomenon.

The history of the word "spam" (which is said to be derived from Spiced Pork And haM) dates back to 1937 when a new luncheon meat was first introduced into the market. It was a breakthrough product at that time as it gave apparently "fresh" meat that didn't need the expense of refrigeration. It was hardly a culinary delight but then fresh meat was not widely available. In fact in those days food for most people was not up to much. Then when the Second World War began products like spam came into their own both for the civilians and the military. Made of a mixture of chopped pork shoulder and ham, spam was at this time an important part of many diets. But in the years that followed the Second World War, when food production not only came back to normal, but began to flourish and produce the great variety of high quality products we have grown accustomed to today, spam became a largely unwanted commodity in our society – at least in the western world. As the aphorism goes, "every dog has its day", and by the 1960s spam's day had largely come and gone. Yes, you can still find spam on the shelves of some supermarkets but it is not a highly sought after product.[2]

However, we were not yet finished with the word spam. The Encyclopaedia Britannica reminded us that the word spam was used in a *Monty Python's Flying Circus* sketch written in 1969, when chanting the word spam drowned out the other dialogue.[3] Clearly it is an easy to pronounce monosyllabic term, which sort of rolls off the tongue and so uses other than describing a meat product were to be found for it.

* *School of Systems and Data Studies, Trinity College Dublin, e-mail: aideen.keaney@tcd.ie*

** *School of Systems and Data Studies, Trinity College Dublin, e-mail: dan.remenyi@tcd.ie*

Definition of the Word "Spam"

Today the word spam has been taken over by the users of the Internet to refer to unsolicited commercial e-mail (UCE) or unsolicited bulk e-mail (UBE). However, its definition is not so clear-cut. One possible definition is a false commercial offer made by e-mail; another popularly understood definition has evolved to include all unwanted e-mail. Mulligan (1999) defines spam as "huge volumes of unsolicited messages, irrespective of content". *The New Penguin Dictionary of Computing* (2001) defines spam as "the sending of an unrequested and unwanted e-mail to multiple recipients, usually for the purpose of advertising". There are a number of additional nuances here, which need to be considered. Unsolicited e-mail from charities seeking funding for relief projects may not be regarded by some recipients as spam. Information which the receiver finds useful from sources such as the publishers of e-zines for example may also not be regarded as spam. So clearly what constitutes spam for one individual may not be spam for another. For now, there is no distinction between the unsolicited e-mails that are called spam and those that might be considered a legitimate marketing strategy (Schaub, 2002). For the purposes of this paper, we will define spam as "the sending of an un-requested and unwanted e-mail to multiple recipients".

There appears to be approximately 200 major spam-sending organisations. This estimate was supplied by Steve Linford of Spamhaus at the Spam Summit held on 1 July 2003 by the All Party Internet Group of the UK House of Commons, which is referred to as APIG. According to Linford, these organisations are increasingly operated by individuals who have no regard to any laws or regulations. He claims that those working against the spammers are often harassed and threatened. He believes that the spam problem is likely to grow at exponential rates over the next few months and years.

User Attitudes to Spam

Spam represents the largest growing sector of Internet activity. Spam used to be thought of as rather harmless, but if this ever was really the case, it is no longer so. Spam is now a hazard and is increasingly seen as such. Users can have a strong emotional reaction to spam. Many users are highly annoyed by these constant, uncontrollable intrusions to their work. Add to this the sometimes offensive and fraudulent nature of spam and it is not surprising that the annoyance caused by these unwanted messages can be a greater distraction than the intrusion itself. Adam (2002) states that the rapid increase in the availability of e-mail has resulted in "e-mail overload": users now have cluttered in-boxes containing hundreds of messages, including outstanding tasks and partly read documents. Spam can now be added to this "overload".

Users can also feel that spam threatens their privacy. Fahlman (2002) states that a concern for most of us is the fear that our personal information will fall into the hands of unscrupulous marketers, who will then intrude upon us with unwanted calls and messages. Han and Maclaurin (2002) found in a survey of

attitudes to online privacy that a number of respondents labelled spam as a major privacy issue.

One danger that has been articulated is that users may feel so threatened by spam that they may lose trust in technology and turn away from the central application of the Internet Revolution e-mail.

Nature of Spam

So exactly what is this menace that has the potential to diminish our use of e-mail? We start by examining the different types of spam. In 2003, the USFTC (Federal Trade Commission) carried out a study analysing the contents of a random sample of spam drawn from a variety of sources available to FTC staff. They found that messages fell into eight general categories. These are shown in Figure 2.1.

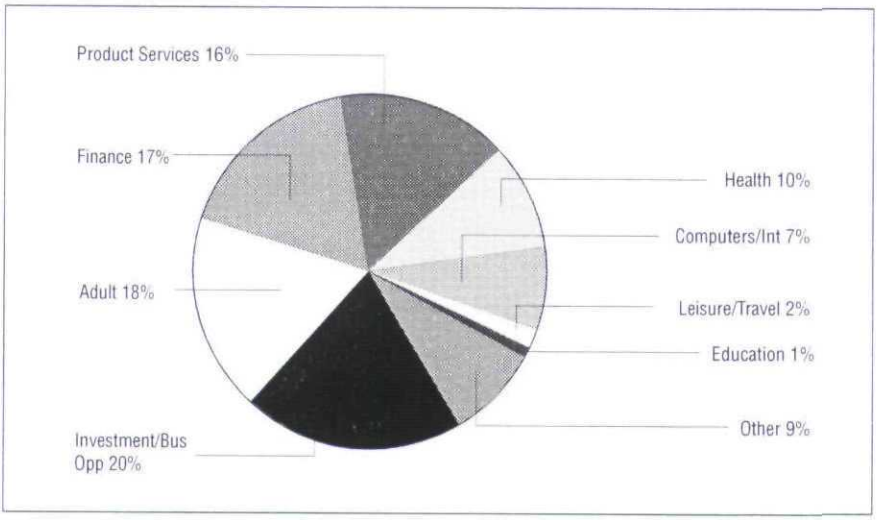
Figure 2.1: Eight Categories of Spam Offers as Defined by the US FTC, 2003

Type of Offer	Description
Investment/ Business Opportunity	Work at home, franchise, chain letters etc.
Adult	Pornography, dating services etc.
Finance	Credit cards, refinancing, insurance, foreign money offers etc.
Products/ Services	Products and services other than those coded with greater specificity.
Health	Dietary supplements, disease prevention, organ enlargement etc.
Computers/ Internet	Web hosting, domain name registration, e-mail marketing etc.
Leisure/ Travel	Vacation properties, etc.
Education	Diplomas, degrees, job training etc.
Other	Catch-all for types of offers not captured by specific categories listed above.

Figure 2.2 describes the prevalence of each of these different types of spam. It can be seen that the so-called Investment/Business Opportunity, Financial and Adult offers accounted for over half of all messages.

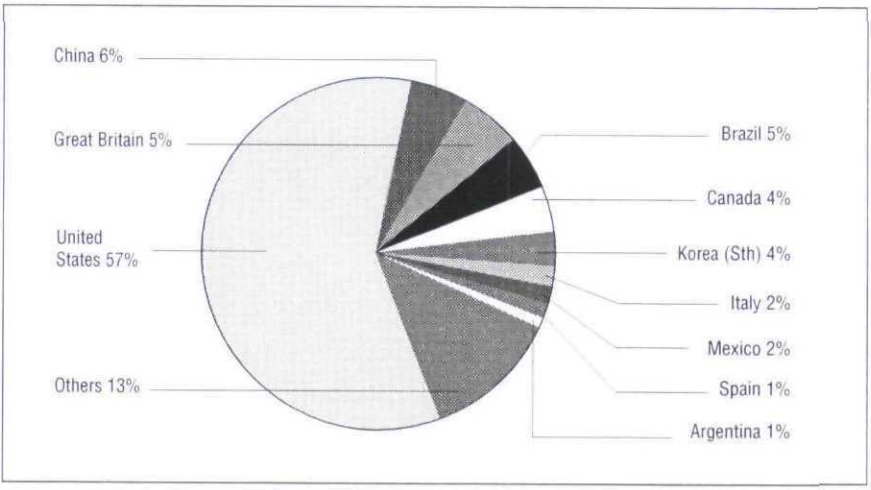
The country of origin of these spam messages is also interesting, as shown in Figure 2.3. In March 2003, the US accounted for nearly 60 per cent of all spam activity.[4] Adding in Canada and Europe, we can account for 70 per cent of the origins of spam.

Figure 2.2: Offers Made via Spam*



*FTC, 2003

Figure 2.3: Spam Activity by Country of Origin*



* MessageLabs, March 2003

Some sectors of the economy are more vulnerable than others to the threat of spam. Figure 2.4 shows a distribution of spam in December 2003. It reflects for the European region, the percentage of e-mail in each sector containing unwanted content.

Figure 2.4: Market Distribution of E-mail Spam*

Sector	Percentage of Spam E-Mail per Sector
Accommodation and Catering	67%
Education	63%
IT Services & Telecommunications	63%
Administration and Support	62%
Health Care	61%
Chemical & Pharmaceutical	56%
Real Estate	54%
Professional Services	48%
Non-Profit	46%
Retail	46%
General Services	45%
Recreation and Leisure	43%
Manufacturing	42%
Marketing, Media and Publishing	42%
Agricultural	36%
Finance, Banking and Insurance	35%
Wholesale and Distribution	34%
Transport and Utilities	23%
Government and Public Sector	22%
Building and Construction	17%

* MessageLabs, December 2003

SCAMMING

The FTC (2003a) currently estimates that in the US 70 per cent of spam is, in terms of current law, illegal. Attempted fraud is one of the more popular illegal spams. Probably the best known are the Nigerian e-mail scams where some person, often purporting to be the son or daughter of a famous but now dead politician or military figure, has an amount of money – often tens or sometimes hundreds of millions of US dollars (the largest sum we have seen was US$500,000,000 – half a billion dollars), which for some reason they need to launder and if we send them our bank account details they will lodge this money in our bank account. These people say that they have found our name in a book on the shelf of their deceased father or they got our name from their Chamber of Commerce. One colleague has received an e-mail from a swindler who had designated himself as The Reverend, to the effect that the Lord had directly given him our colleague's name and e-mail address and had recommended him as an extremely honest and trustworthy person. Another

colleague was very amused to see that the Lord was an e-mail user and that his name was already in the Lord's directory and with such positive connotations. What interests us is the sheer gall of these swindlers and the fact that this activity has been increasing in intensity since we received our first e-mail invitation to swindle the Nigerian Government three years ago.

Usually the fraudulent offer is that you will retain 20 per cent of the capital transferred for your trouble. We do not know anybody who has attempted to collaborate with these swindlers, but we do know someone who says that a friend of his did. Apparently this friend of a friend sent off his details and a few days later was told by the original e-mailer that the funds were ready for transfer but that a difficult bank manager in Nigeria was delaying the process. He was then told that a payment of US$25,000 would speed up the bank manager considerably. The money was sent. A week later another e-mail informed him that there was now a difficult customs and excise officer who was holding up matters and that a US$20,000 would expedite this link in the money transfer chain. Time went by and more and more awkward characters, all of whom were delaying the transfer, crept out of the woodwork. We do not know how much money this person sent off in the hope of making his millions. There was a case reported in the US in 2002 where a woman embezzled over a million dollars from her employers just to feed one of these e-mail swindlers in the hope that they would eventually make her "rich quick".[5] Instead of getting rich she went to jail. It has been said that every day of the week there are people waiting in the lobbies of London hotels for the "big" cheque to be handed over to them by their Nigerian benefactor: all they get is the bill for the coffee they consume while waiting. The UK's National Criminal Intelligence Service[6] states that frauds similar to this committed by West African crime groups is estimated to cost the UK at least £3.5 billion a year.

Besides eliciting money it also appears that the swindlers are involved in identity theft. Hinde (2002) states that this crime is one of the fastest growing crimes in the US. Identity theft refers to circumstances whereby professional fraudsters acquire sufficient information about an individual to be able to access their bank accounts and lines of credit and thus to help themselves to cash and credit and other facilities to which they are not entitled. In many cases the individual whose identity is stolen becomes blacklisted for exceeding credit limits and generally appearing to be financially irresponsible. Identity thieves also break the law in other ways using the name of their victims and this can result in considerable personal inconvenience. In 2003 in South Africa, Stephen Bond, a retired Englishman on holiday, was actually imprisoned at the request of the FBI as a result of his identity being stolen.[7] The FTC recently released alarming figures about identity theft. More than 27 million Americans have been victims of identity theft over the last 5 years, including 9.9 million in the last year. Losses attributed to identity theft totalled nearly $48 billion for businesses in the last year, while consumer victims reported $5 billion in losses.[8]

Another interesting scam is the invitation to collect your winnings from the lottery. You are advised by e-mail that you have won a lottery for which you have not purchased a ticket. A typical message reads:

> You are allotted to ticket number 3 - 0382 - 8642 - 032 , with serial number FV-UX654 drew the lucky numbers 453 - 7333 - 7042 - 992 , and consequently won in category C. You have therefore been approved for a lump sum pay of 750,000.00 Pounds Sterling in cash credited to file REF NO. SLP/026-5B8C8N85074. This is from total prize money of 11,250,000.00 Pounds sterling shared among the international winners in the category C. All participants were selected through a computer ballot system drawn from 30,000 names from Australia, New Zealand, America, Asia, Europe and North America as part our International Promotions Program, which is conducted annually.[9]

When the prize was claimed from this source the following message was e-mailed:

> Thank you for your claims submission. Find attached is your claims form. We will be processing your claims immediately with this form. You are required to forward 750.00 Pounds (SEVEN HUNDRED AND FIFTY) for our processing charges with the UK Gaming Commission and The Lottery Board, which represents 0.1% of your total winnings. This is mandatory, as it will enable us in a timely manner, allocate your winnings with our issuing finance house, for them to immediately forward your winnings to your nominated account.[10]

It would be very interesting to know how many people forwarded a cheque for £750. This is such a serious problem by both e-mail and postal mail that the UK government now has a TV advertising campaign "Prizewinner or *prize fool*?"[11] warning people against these scams.

We have not attempted to supply a definitive list of scams presented in spam but rather to highlight some of the more frequently offered "financial opportunities".

There are other potentially criminal activities being offered, such as the provision of cigarettes at prices that suggest they are probably counterfeit. There are also "real" Rolex watches being offered for US$65. You can have US$200 for free by signing up with an online casino. In September 2003, we saw for the first time direct offers of hard drugs and undisguised child pornography.

Stem this Tide of Spam

To stem this tide of spam, many companies are installing anti-spam filtering software. This software tries to identify spam and deletes it or moves it to a junk folder. To bypass these filters, the spammers are becoming more sophisticated and resorting to more elaborate tricks to get their message through. One way they do this is by using a variety of social engineering methods to induce the

recipient to open and read the content of the message being sent. Kevin Mitnick (2002), probably one of the most infamous social engineers, defines social engineering as "using influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology." To achieve this, spammers often send spam from an e-mail address that is spoofed or forged, concealing the identity of the sender. The e-mail will be sent from an address that you will recognise. One common example is that the sender comes disguised as a corporate network administrator with the subject line: "Your mailbox is over its size limit."[12] You are then asked to load some software to clear your mailbox and in so doing you actually give the spammer full access to your PC. A more recent trend that spammers are using to hide their identities is the use of "open-proxy"[13] machines. This is an approach that has been used by hackers and virus-writers for some time.

The spammers' "compendium of tricks" for getting access is large and growing. Some can be extremely simple such as misspelling keywords that an anti-spam package would be looking for, for example "V1agra". Others are much more technical in nature.

All in all, this means that spammers are generally one step ahead of the software and technical solutions. Cranor and LaMacchia (1998) carried out a six month study analysing the performance of anti-spam software filters in AT & T and Lucent Technologies. They found that the effectiveness of their filters had degraded considerably during the months of the study due to spammers changing tactics. It requires considerable effort to keep up with the spammers. This ongoing struggle with spammers is sometimes referred to as an intellectual arms race and, like the war on drugs, it is not likely that it can be won – the amount of talent spammers can buy is certainly a match for the developers of the spam filters.

The Economics of Spam

Of course spam is much like unwanted mail in the postal system, unwanted faxes or unsolicited phone calls, but it differs in one major way: virtually everyone but the spammer bears the cost of this nuisance.

Once the spammer is set up there is little or no cost to despatch a million e-mail messages. Conversely, using printed commercial brochures there is the cost of creating, printing and mailing and this is borne by the sender, not the receiver. According to Mulligan (1999), spam is very much like receiving unwanted mail with postage due!

Figure 2.5 shows the costs associated with sending printed mail shots and sending spam e-mail.

Figure 2.5: The Economics of Spam

PRINTED MAIL SHOTS	
Cost:	25 cents per piece or more
Response rate:	3% or less
Cost per response:	$8 or more
SPAM E-MAIL	
Cost:	one hundredth of a cent or less
Response rate:	0.25% or less
Cost per response:	4 cents or less

Source: www.computerworld.com

Even a tiny percentage in uptake can generate substantial income for spammers. A recent article in the *Economist* (2003) suggests that a response rate as low as one in 100,000 justifies many bulk mailings, as their overheads are minimal. Wood (2003) states that one million e-mail 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. Of course it is very unlikely that any spammer would be using a dial up line and thus even this cost is not likely to actually be incurred. So it is clear that the economics are all in favour of the spammers.

In Figure 2.6 Schwartz and Garfinkel (1998) identify four separate groups that suffer at the hands of spammers and suggest how the spam actually adversely affects the organisation.

Figure 2.6: Groups that Bear the Cost of Spam*

Group	Nature of Nuisance
Users	For users, there is the waste of time spent sifting through and deleting unwanted messages. There is also the danger that a user may be drawn into a spam offer and thus waste even more time. If a user is using a dial-up connection, there can be an additional cost just downloading these unwanted messages. There is a danger that genuine e-mails can get lost amongst the spam. For some of the newer spam solutions, there is also an overhead in maintaining filters and white lists. There can be a perceived privacy intrusion. (Gopal, Walter et al., 2001). There is also the unsuitable and unsavoury nature of some of these e-mails.
Organisations	Companies have to increase the capacity of their mail servers and network infrastructure to deal with these additional mails. Companies also invest time and effort into installing anti-Spam software that tries to counteract this problem. Much of a systems administrator's time can be spent dealing with this

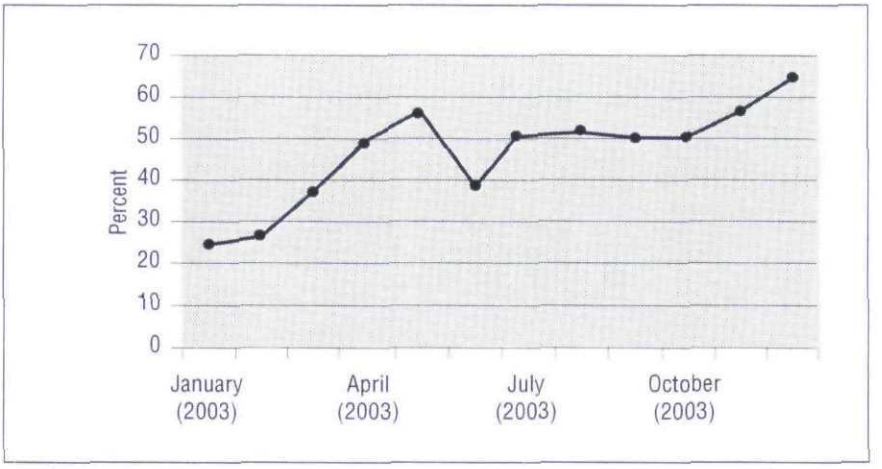
	problem. Another additional cost is the support/helpdesk facilities that are needed to deal with user complaints.
Innocent bystanders	Spammers often relay their messages through other computers on the Internet, often without the knowledge of the owner. This constitutes a theft of service. It can also result in problems for the unsuspecting relay as people mistakenly think that the relay is the spammer.
ISPs	They bear increased storage, transmission and computing costs. In excess, it can lead to denial of service for other e-mail and network traffic. (Denning, 1999). Recently, an Irish ISP fell victim to serious problems with spam. The sheer volume of spam being relayed through the organisation overloaded internal systems and caused an outage.

* Based on the Schwartz and Garfinkel (1998) taxonomy

Quantifying Spam

It is clear that spam is a very profitable business for those engaged in it, but just how much is it costing business and the rest of society? Before we can answer that we need to try to ascertain how large this problem actually is. MessageLabs is a leading provider of managed e-mail security services to businesses worldwide. They scan millions of e-mails everyday (in December 2003 they scanned 463 million e-mails). Their findings (see Figure 2.7) over the last year and in particular the first few months of this year have been interesting (Wood, 2003).

Figure 2.7: Percentage of Spam in Mail, January 2003 – December 2003*[14]



* MessageLabs

The latest statistics for other spam filtering companies confirm this trend. In May 2003, SpamTrap (www.spamtrap.net.au) recorded that 55.8 per cent of all customers' e-mail was spam. If these trends continue, there could be a 600–700 per cent increase in spam growth year to year. Care has to be taken when interpreting statistics from companies such as these. These figures may not be representative, as the incidence of spam is almost certainly higher amongst the clients of spam filtering vendors than other companies. It is clear, however, that the problem is large and growing.

How much does Spam Cost Organisations?

As previously shown in Figure 2.6, there are four main ways in which spam can incur costs. The first is the loss to the user in productivity, personal communication costs and the costs associated with maintaining spam filters. In addition, it is worth reflecting on how much genuine e-mail is lost in the volumes of spam. The second cost is to the organisation in relation to upgrading the e-mail infrastructure to cope with the additional burden of spam. There is also a burden on its helpdesk/support facilities. The third cost is to innocent bystanders (using open relays) and comes into effect when an organisation's computer's response is degraded by unauthorised traffic. There is a knock-on cost when the innocent bystander is accused of being the spammer and their e-mail facilities are blocked.[15] A fourth cost is borne by ISPs. They have similar costs to businesses but on a far larger scale as they have a much higher throughput to deal with. They incur considerable costs in blocking spam. AOL has blocked 2.3 billion spam e-mails in the last year.

Ferris Research[16] (2003) estimate that spam will cost US corporations more than $10 billion dollars in the coming year. They estimate that, on average, it takes 4.4 seconds to deal with a message, this equates to $4 billion in lost productivity for US businesses each year. Another $3.7 billion is a result of companies having to buy more powerful servers and more bandwidth as well as diverting staff time. The rest of the $10 billion can be attributed to companies providing help-desk support to users. This equates to a cost of $14 per user per month.

The worldwide costs are of course higher. A similar study by The Radicati Group[17] projects the worldwide losses for companies, in terms of additional servers they have to deploy and manage to process spam, will amount to $20.5 billion in 2003. The European Union estimate that spam will cost $8 Billion in bandwidth costs alone worldwide in 2003.

The predicted cost of spam to organisations does vary quite considerably in each of these studies. Figure 2.8 looks at the yearly costs of spam per employee as reported by a selection of studies.

The difference in suggested cost can be attributed to how sophisticated the research was for each report. An estimate of the cost of spam to an organisation may focus on a number of issues such as: the volume of e-mail sent and received each day; the volume of spam; the time spent dealing with spam; the

percentage of bandwidth used for mail services; the additional IT infrastructure needed to cope with spam; helpdesk/support facilities; employee numbers; average hourly salary per employee; work hours.

Figure 2.8: Yearly Cost of Spam per Employee as Reported by Various Studies

Study	Yearly cost of Spam per Employee	Attributed to:
Nucleus Research Inc. July 2003	$874	Loss of user productivity, based on 1,000 employees with average earnings of $30 per hour
Ferris Research, January 2003	$168	Loss of user productivity & IT and helpdesk costs
Computer Mail Services – online calculator[18]	$150	Loss of user productivity based on 1,000 employees with average earnings of $30 per hour and receiving 10 spam messages a day
Radicati Group, June 2003	$49	Loss of user productivity based on 10,000 employees

Of course, the real cost of spam needs to be assessed in terms of the actual cash dispersed by the organisation as a result of the spam attacks; therefore, incorporating notional amounts for staff time and cost is often highly questionable.

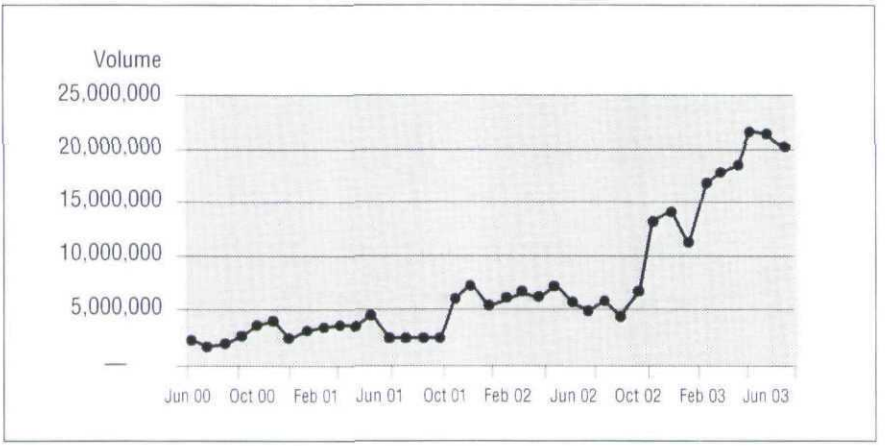
Furthermore, users do not always just delete these unwanted mails, they often talk to their colleagues about these spam messages and sometimes exacerbate the situation by passing these messages around. In some instances users can be drawn into purchasing the products and services advertised by spam and some of these are scams.

There is also a less tangible social cost to spam. A material portion of spam is frequently offensive in nature. While this can be quite disturbing for some adults, it can actually be damaging to children, and parents are now restricting children's use of e-mail.

University of Dublin: The Trinity College Experience

The University of Dublin is located in the centre of the city and is most commonly known as Trinity College Dublin (hereafter referred to as TCD). It is Ireland's oldest university, dating back to 1592. TCD has approximately 20,000 e-mail users and receives up to 900,000 e-mails a day. Figure 2.9 shows the average daily volume of e-mails to and through TCD.

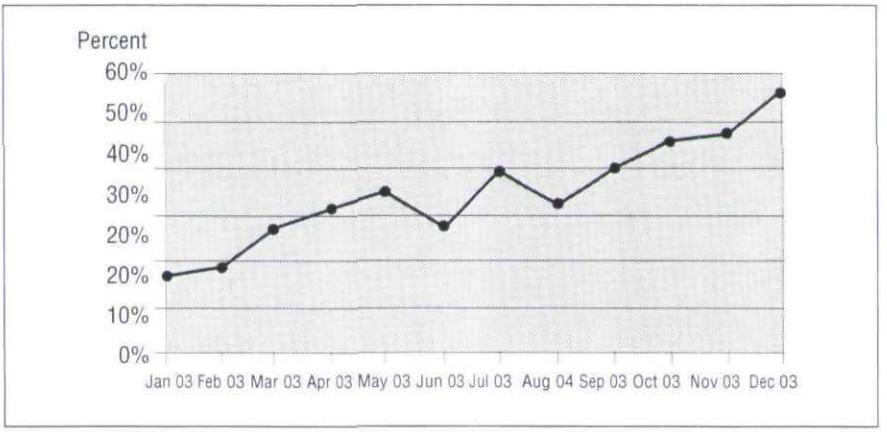
Figure 2.9: Monthly Volumes of E-Mail to and through TCD, June 2000 – June 2003



Source: IS Services, TCD

In conjunction with the increased volumes of e-mail has been the increase in the amount of spam. The issue of spam was initially identified in the autumn of 2001 and since then has become an increasing problem. Figure 2.10 shows the quantity of spam received each month by the IS services manager. This is only the experience of one user who has kept details of his level of spam receipt.

Figure 2.10: Monthly Percentages of Spam for IS Services Manager January 2003 – December 2003



Source: IS Services, TCD

It is clear from Figure 2.10 that the amount of spam being received by the IS services manager does follow the trend as shown by MessageLabs in Figure 2.7. However, the percentage of spam for the IS services manager are lower and hit a peak of 56 per cent in December 2003. For the university, as a whole, it is estimated that on occasions 85 per cent of e-mail arriving is spam. However, the overall estimated daily average of spam is approximately 45 per cent.

The spammers are harvesting the university's e-mail addresses from a number of sources: old usenet (bulletin board) postings; membership of mailing lists; opt-in web pages and opt-out e-mails. The longer established e-mail accounts get more spam. More recently, spammers have been using brute force attacks to reach users. The university receives 500,000 brute force attacks a day. A brute force attack is a "Dictionary attack". The spammer simply sends to a variety of common names hoping to find them in this particular domain. Another recent trend is for spammers to take advantage of read-receipt functionality in e-mail programs. This function automatically sends an acknowledgement to a spammer informing him or her that you have read their e-mail. They therefore know that they have found a valid address. Users may not know that this facility is installed and running in the background.

The Damage Done by Spam

Spam has caused TCD an increasing number of problems, which may be categorised as follows:

1. the annoyance factor caused to staff and students in receiving this unwanted mail
2. the loss of real e-mail among the spam
3. the cost of needing bigger personal systems to cope with the greater through put due to the spam
4. the problem of some of the html e-mail actually containing illegal photographs[10]
5. the university may also have a legal liability if its staff and students are exposed to certain unsuitable e-mails
6. the potential for staff and students becoming involved in some of the scams presented in the spam notices.

In addition to these problems and potential problems there have also been two spam-based denial-of-service attacks on the university's e-mail system in the last year. One occurred when approximately 10 million e-mails were sent to TCD in one weekend. The e-mail infrastructure was unable to cope with this volume of e-mail and this in turn had knock-on consequences for two other universities who were holding some of these mails waiting for the TCD e-mail system to come back online.

It is generally thought that the biggest cost to the university has been the loss of productivity. As said before, there are 20,000 e-mail users and if each user

spends a conservative estimate of 5 minutes a day clearing unwanted mail, then over a year the university has wasted approximately 608,300 hours dealing with spam. If we narrow this down to the staff members with active e-mail accounts of which there are 2,800, the wasted time is 85,200 hours per year. Using an eight-hour day and the average wage, the university is incurring spam-related losses of €1 million.[20]

Of course TCD's problems are in no way unique and the difficulties described here are experienced by many other universities and other organisations around the world. Perhaps the situation in TCD is exasperated by the fact that there is an attitude in TCD that blocking spam is in essence a type of censorship.

Possible Solutions

It is not the intention of this paper to address the solution to the spamming problem in detail. However, it is necessary to say that it is clear that spam is a major problem that is on the increase. It is a considerable annoyance for organisations as they bear the majority of the costs related to this activity. As already mentioned, the cost to the spammers relative to the receivers of the spam is minimal.

The solutions proposed to date are to:

1. install more sophisticated hardware and software filters to protect organisations from spam
2. educate users to avoid doing anything that may help or encourage spammers;
3. introduce legislation to make spam unlawful[21]
4. change the charging arrangements for e-mail.

It is unlikely that any one of these alone will solve the problem of spam. However, as well as installing hardware and software filters it is incumbent upon a university to ensure that it provides extensive education on the problems and dangers to its members becoming involved with any offers presented by spam. Scams are not always all that obvious to young and inexperienced individuals. The principle of *in loco parentis*[22] alone makes this an essential aspect of why they need to combat spam and scams.

But it is clear that the growth in spam cannot be allowed to continue. Sooner or later major action will have to be taken on this issue and, whatever happens, it will no doubt involve additional controls and thus expense. These controls may require government and international agencies to collaborate. These organisations would also have to work together if charging per unit e-mail despatched was to be globally introduced. After all, the Internet is a global issue and it will require global regulations to actually ensure that it is not being attacked and abused. There are certainly interesting times ahead and the sooner a multilateral debate on how to establish policy which will contend with spam

is initiated the better. It always takes a very long time to establish a policy where there are many stakeholders and this is an issue that affects a large number of stakeholders.

Future Research

Despite the increasing menace of this problem there is surprisingly little research related to spam, or the scams offered in the spam, published in the IS management journals. This subject does not appear to have been taken up in any material way. This is despite the fact that the subject has a lot to offer from an intellectual point of view. There is the whole range of policy with regards to actual and potential legislation and codes of practice. There are the management issues, which range from how to ensure organisations are not subjected to fraudulent practices as a result of spam and scams, to the technical issues involved in information systems security management. There are of course articles mostly written by journalists on this subject published in the popular press but in general they are not well focused nor do they present their arguments rigorously. The spam and scam subject needs much more rigorous attention. There are many policy issues to be investigated and aired and there are many interest groups involved. There are numerous opportunities to consider how algorithms or heuristics may be improved to foil the effectors of spammers. And the results need to be given a high degree of visibility.

If satisfactory progress is to be made in the struggle against spam then the IS academic research community needs to become more involved in this area of study. To date, the little academic literature in this field has focused on the computer science research aspects of hardware and software issues related to spam, and not on the social and management issues.

An Anti-Spam Research group (http://www.irtf.org/asrg) has been set up to understand the problem and collectively propose and evaluate solutions to the problem. IS academics could actively contribute to the research group by addressing issues such as:

1. Organisation problems faced due to spam
2. ISP problems faced due to spam
3. Defining spam
4. Privacy considerations
5. Deployment considerations for solutions being proposed
6. Quantifying and categorising spam
7. Identifying scams
8. Disseminating information about scams
9. Developing requirements for solutions
10. Developing a taxonomy of spam solutions
11. Evaluating proposed solutions
12. Developing best practices documents.

Each of these areas offers major research opportunities and the sooner the academic community takes an active interest in spam and scamming as a research topic the better. Rigorous research findings would enable well conceived and well understood policies which have a good chance of success to be put in place at the national level and at the corporate level too. It would also provide individuals with a better understanding of what is actually happening and how they need to be involved in the struggle against spam.

We will continue with our research work on spam at TCD.

---

1 The authors would like to thank the IS services manager in Trinity College Dublin for providing facts and figures used in this paper.

2 For more details of the meat product from which the name has been borrowed see http://media.hormel.com/anm/templates/spam_museum.asp?articleid=8&zoneid=11. In fact according to http://www.safetyalerts.com/recall/f/02.2/f0001930.htm in "Anderson, IN (SafetyAlerts) - US Department of Agriculture's Food Safety and Inspection Service said that Mr. Pizza Inc. is recalling approximately 210 pounds of fully cooked, ready-to-eat pork luncheon meat that may be contaminated with Listeria monocytogenes."

3 There is much more about this subject on the web beginning with http://www.stmoroky.com/reviews/films/hlygrl.htm

4 Current and upcoming legislation in the USA is thought to be likely to move Spammers out of that country and into the developing world. It was suggested at the APIG Spam Summit on July 1, 2003 that many of the illegal child pornographic sites are being located or relocated in parts of the former Soviet Union.

5 See http://www.thirdage.com/news/archive/990726-03.html?std and http://www.freep.com/news/locoak/checks21_20020921.htm for details of these types of frauds.

6 Details of the scam and a Nigerian fraud e-mail gallery is available at http://www.ncis.gov.uk/waocu.asp

7 See http://www.timesonline.co.uk/article/0,,1-591965,00.html

8 See http://www.csoonline.com/metrics/viewmetric.cfm?id=602

9 The detail of a discussion between the Spammer and someone "interested" in collecting the money is provided at http://www.tactics4wealth.com/

10 The typing errors have been deliberately not corrected.

11 Details of the ad campaign are at http://www.dti.gov.uk/ccp/scams/page2.htm#prizedraws

12 See http://news.zdnet.co.uk/story/0,,t269-s2108342,00.html

13 A proxy server is a computer that is used to consolidate Internet access for an organisation. These proxies can sometimes be mis-configured and can be left "open" or insecure and anyone on the Internet can then use it as a relay for their own anonymous Internet activities.

14 The drop in the percentage of Spam in mail in June 2003 may be attributable to the start of the summer holiday season or it could possibly be due to new anti-spam measures such as proposed law suits by Microsoft.

15 With more and more blacklists being created this is an increasing problem which causes interruption and loss of business to many innocent e-mail users.

16 Ferris Research is a San Francisco-based market and technology research firm that specialises in messaging and collaboration technologies, such as e-mail, instant messaging, wireless handheld connectivity and virus and spam control.

17 The Radicati Group publishes extensive market studies analysing market size, trends,

forecasts, as well as offering competitive product and vendor intelligence. (www.radicati.com)

18 http://www.cmsconnect.com/Marketing/spamcalc.htm

19 At the APIG Spam Summit held on July 1, 2003 it was stated that between 75 and 85 new pornographic websites supplying photographs of sexual explicit situations in which children are involved are set up on the web each week. Spam is then used to attract visitors. Pornographic photographs are actually e-mailed.

20 As we mentioned above this type of figure has to be viewed with caution, as the university is unlikely to have to spend anything to make up this annoying loss of staff productivity. Nonetheless we regard this type of calculation worth doing if for no other reason to give some tentative substance to the annoyance caused by Spam. The real cost to the university is incurred in improving the e-mail infrastructure to cope with the additional e-mail load and installing software to detect Spam.

21 As implied above this will probably only drive spammers to set up in countries where these laws don't apply.

22 *In loco parentis* translates for the Latin as "In the position or place of a parent". This refers to the fact that the university has some responsibility for its students' welfare over and above the purely academic issues. This was seen as a very important issue in former times when young people only attained their majority at the age of 21. In today's world when young people attained their majority at only the age of 18 the issue is not as important. There will be few students who will be under 18 years of age but they need to be catered for.

References

"False Claims in Spam", Federal Trade Commission: 15, 2003.

"Spam Control: Problems and Opportunities", San Francisco, Ferris Research, 2003.

Economist, the, (2003) "Stopping Spam", Vol. 367, No. 8321, p. 66.

Adam, R. (2002) "Is E-Mail Addictive?" *Aslib Proceedings*, Vol. 54, No. 2, pp. 85–94.

Cranor, L.F. and LaMacchia, B.A. (1998) "Spam!" *Communications of the ACM*, Vol. 41, No. 8, pp. 74–83.

Denning, D.E. (1999) *Information Warfare and Security*, Addison Wesley.

Fahlman, S.E. (2002) "Selling Interrupt Rights: A Way to Control Unwanted E-Mail and Telephone Calls", *IBM Systems Journal*, Vol. 41, No. 4, pp. 759–66.

Gopal, R.D., Walter, Z. et al. (2001) "Admediation: New Horizons in Effective E-mail Advertising", *Communications of the ACM*, Vol. 44, No. 12, pp. 91–6.

Han, P. and Maclaurin, A. (2002) "Do Consumers Really Care About Online Privacy?" *Marketing Management*, Vol. 11, No. 1, pp. 35–8.

Hinde, S. (2002) "Spam, Scams, Chains, Hoaxes and Other Junk Mail", *Computers & Security*, Vol. 21, No. 7, pp. 592–606.

Mitnick, K.D. (2002) *The Art of Deception*, Indiana: Wiley.

Mulligan, G. (1999) *Removing the Spam: E-mail Processing and Filtering*, Mass.: Addison-Wesley.

Pountain, D. (2001) *The New Penguin Dictionary of Computing*, London: Penguin Books.

Schaub, M.Y. (2002) "Does Europe Allow Spam? The State of The Art of the European Legislation with Regard to Unsolicited Commercial Communications", *Computer Law & Security Report*, Vol. 18, No. 2, pp. 99–105.

Schwartz, A. and Garfinkel, S. (1998) *Stopping Spam*, O'Reilly & Associates.

Wood, P. (2003) "A Spammer in the Works", *MessageLabs*, Vol. 11.