

Perceptions on SPAM in a South African context

Wallace Chigona; Ashvin Bheekun; Melanie Späth; Saba Derakhashani and Jean-Paul Van Belle
{wchigona | jvbelle@commerce.uct.ac.za}

Department of Information Systems, University of Cape Town, Rondebosch, 7700, South Africa

Abstract

The volume of Internet spam has reached alarming proportions. This raises interesting debates on a variety of ethical, social, legal and technical issues. Although a fair amount of spam research has been conducted in the developed world, the socio-economic context and technical infrastructure in South Africa is more typical of a developing world and many issues take on new dimensions.

This research used a survey to obtain the perceptions of e-mail users on various social and ethical issues regarding spam. Information about the legal and technical issues was gathered using structured face-to-face interviews with six ISPs.

The research confirms the typical findings about the high levels of spam, the nuisance factor, the invasion of privacy and cost in terms of time and bandwidth. However, it was also found that many users find different types of spam morally very offensive. While Bayesian and open source spam-filtering mechanisms are in place at South African ISPs, spam levels are about the same as in Europe and North America. Also, ISPs found that the recently promulgated South African ECT Act fails to deal conclusively with spam.

1. Introduction

During the last decade, email use has been growing at an exponential rate throughout the world, becoming an essential communication tool for both individuals and businesses. Not only does email assist in work related activities, but it also plays an important role within the social realm [1]. Consequently, email has been dubbed the killer application of the Internet [2].

Email is relatively inexpensive, easy to use and has a wide range of users. The marginal cost of sending one additional email is next to nothing. This makes email the cheapest and most efficient tool to reach thousands of people from a marketer's point of view. Spam provides businesses with an inexpensive mass marketing tool that proves less costly than direct mail efforts [3; 4].

The rapid growth of spam around the world has caused annoyance and frustration among email users [5]. This leads to many ethical debates, such as, how ethical is it to send spam of a pornographic nature, how ethical is it for spammers to harvest email addresses from web sites or to perform dictionary attacks and how ethical is it to use spam as a means of perpetrating fraud or making false claims. Socially, spam has caused a reduction in productivity as more time is required to determine which emails are relevant and which ones are not.

A number of measures can be put in place to reduce the volume of spam. Different kinds of software packages are used to filter spam at an individual or business level. These measures, however, may also lead to further interesting debates. For example, filtering spam at an Internet Service Provider (ISP) may be infringing the freedom of speech of the email sender. At the greater societal level, government can implement legislation that attempts to decrease the quantity of spam, by placing restrictions on its content or outlawing it altogether. However, the effectiveness of anti-spam laws is yet to be determined.

Generally, four main concerns are considered in spam-related research. These are ethical, social, technical and legal issues of the spam phenomenon. However, most of the previous research done on spam thus far has taken a North American and European perspective. Therefore, there is a lack of objective research conducted into this topic from a South African perspective. Due to the fact that the Internet infrastructure as well as the political and socio-economic environment of South Africa is different to the American or European climate, research findings from a South African perspective may be different as well.

2. Definitions and Background

Definition of Spam

Internet users differ widely in what they perceive to be spam. Some users consider all advertisements, jokes and chain letters or even all unwanted messages to be spam, while others try to define it in terms of existing acceptable use policies or network etiquette rules.

Leung [6] defines spam as unsolicited email messages or news articles sent in bulk to recipients without their permission. The Center for Democracy and Technology [7] uses a broader definition and refers to spam merely as junk mail. Junk mail can consist of jokes and chain letters from business colleagues, friends and family. Solkin [8] identifies the two most common definitions of spam as being unsolicited commercial email (UCE) and unsolicited bulk email (UBE).

A key element in nearly all definitions of spam is that the email messages must be unsolicited. In general, a communication is considered to be unsolicited if there is no prior relationship between the parties, and the recipient has not explicitly consented to receive the communication [8].

Another aspect found in most spam definitions is that spam consists only of messages that are commercial in nature. Commercial refers to the message content rather than the sender's actual or presumed motivation for sending the message, and thus refers to messages that promote the sale of goods and services [8].

The real problem with spam seems to lie in the volume of email messages, not their content [8]. Spam is thus defined as messages sent in large quantities commonly referred to as "bulk". For the purpose of this research spam will be defined as email sent in large quantities or bulk that cannot reasonably be assumed to be wanted or expected by the recipient and where there is no prior relationship between the recipient and the sender. Therefore, spam will be defined as bulk commercial or non-commercial unsolicited email.

Ethical Issues

There are many ethical issues surrounding spam. We discuss the following ethical issues: offensiveness, false claims and fraud, cost shifting, and freedom of speech.

Perhaps, the biggest ethical issue regarding spam is that of pornographic spam [5]. There is much concern about this issue since children may have access to messages with sexually explicit images. In some cases such spam automatically shows pornographic pictures in the body of the email, not giving the email user the option of following a link to an external site. According to the FTC [5], 40% of pornographic spam messages have false statements in their subject lines making it difficult or impossible for the reader or recipient to know what kind of message they were opening. It is therefore very possible for an innocent user to unwittingly and unsuspectingly open an email with a subject line such as "Re: ..." only to find out that it contains sexually explicit and or disturbing images. Pornography is, however, not the only material people may find offensive [9].

Much of the spam that is circulated on the Internet today perpetuates fraudulent schemes or contains false claims. A study conducted by the FTC's Division of Marketing Practices [10] reported that spam containing an investment or business opportunity accounted for the majority of the spam in circulation today. Common offers include work at home plans, pyramid schemes and get rich quick schemes. The problem lies with the fact that 90% of the claims made by investment and business opportunities are false [5]. This is a serious problem for the consumer, who can potentially be easily attracted to false offers [10].

The high volume of spam circulating on the Internet has a direct impact on network traffic. Network traffic is measured in terms of bandwidth.

The more bandwidth an organization needs the more money it will cost that organization [11]. For this reason, organizations are paying more than they used to for the same service. The organisations, rather than the spammers, are being burdened with the cost of spamming. This is what is referred to as cost shifting [12]. Additionally, organizations and ISPs are spending increasing amounts of money on spam protection in terms of hardware and networking, including extra servers and anti-spamming software [13]. Some authors argue that organizations today spend the same amount of money on anti-spamming software as they do on anti-virus software [12].

Arrison [14] points out that the idea of banning unsolicited political messages disturbs free-speech advocates. She argues that spam is not speech at all but simply an action. Seward [15] agrees but raises two other important points. Firstly, the freedom of speech argument only applies in the United States of America, particularly targeted at the press, making it American-centric. Secondly, the freedom of speech argument implies that one is free to speak and write whatever one likes. It does not imply that one can invade, trespass or infringe on another's privacy or property to dump whatever message or advertisement one wishes. However, Samoriski [16] argues that blocking spam should not be protected by legislation, but rather by technology.

Social issues

Not surprisingly, research conducted revealed that there is a general consensus about the dislike of spam [3; 17]. Some of the negative social impacts from spam are the perceived invasion of privacy, the annoyance factor, the reduction of one's personal productivity and the harm to the global internet economy.

In order to understand how spam invades *privacy*, one must first examine what privacy means. Privacy goes beyond the protection against use of one's personal data [18] but also includes the freedom from unauthorised intrusion. Gordon [18] also found that men and women had differing beliefs about privacy. A study by the Information Technology Association of America [19] found that women felt half as safe as men online, in several areas including the control over the disclosure of their private information.

Recipients, mainly women and parents [2], often become *annoyed* due to unwanted messages, especially those that include pornography [20]. Another source of annoyance is the inability to unsubscribe. Users find it quite annoying when they try to unsubscribe only to find that the removal address does not work. In fact, once a user tries to unsubscribe from spam, the spammer actually receives a signal that the account is active and subsequently more spam is sent to the user which thus creates more annoyance.

The opportunity cost of spam is measured by the loss of an individual's *productivity* [21]. The fact that up to 50% of a user's inbox can be spam has direct implications on the amount of time a particular user has to spend filtering and separating messages [2], let alone the time that has already been spent downloading the unwanted messages in the first place. Furthermore, time is needed to respond, unsubscribe or report spam to ISP's in order to ensure that no more spam is received. Spam tends to congest bandwidth, thus interfering with the timely receipt of wanted material and emails are being lost or misdirected by filters. [22]. The loss of individual's productivity brings with it a cost to organisations. These costs are entailed due to the loss of staff productivity as well as storage and access costs.

Spam also adversely affects speech in that individuals may be reluctant to participate in online forums and Usenet groups, or may remove their email addresses from home pages for fear of getting their email addresses placed on mailing lists for UCE [22], thus negatively impacting freedom of speech.

Along with the problems of annoyance, productivity and privacy, UCE may well undermine the public's willingness to embrace email for a range of functions that require a high degree of predictability and reliability. Users have generated an attitude of distrust on the Internet undermining the acceptance and growth of electronic commerce among the scores of new Internet users taking their first steps online. In effect, spam is curbing the growth of e-commerce and killing the Internet economy.

Technical Issues

There are different measures users can take to block out spam. The prevention measures put in place can either be human based (moderation) or computer based. The human based procedures that can be taken include moderation, the domain level black and white list, and distributed blacklists.

Moderation is a manual or semi-automated process, whereby a message, which is sent to a group of recipients, is initially scanned and moderated by a human who may have assistance from a software package. An organisation using moderation needs to have clear policies as to what messages are appropriate and what messages are inappropriate for the community of recipients to receive [24]. However, this method is quite expensive to put in place because of the high cost of labour in developed countries.

The "*Domain Level Black and White List*" is one of the earliest methods that was developed to fight spam. In this method, the IP address of an incoming offending mail is determined and added onto a blacklist by the administrator of the network

so that further email from this address is blocked. Conversely, to make sure that emails from specific senders always go through, a white list is created which contains the specific IP address.

There are a number of difficulties associated with this method. One of the main problems is that it is time consuming and cumbersome to add addresses constantly to a list. Also, to remain effective, these lists need to be constantly updated [23]. Further difficulty arises as spammers often use different IP addresses or even spoof their address when sending out emails and thus using this method will not produce much impact. The Gartner Group shows that this method is effective for stopping 5-10% of emails [23].

Distributed blacklists go further: organisations such as the Mail Abuse Prevention System (MAPS) catalogue and distribute spammer addresses and domains. These are available freely or for a paid subscription. Hence, this method is more effective than a blacklist run by a system administrator. One of the disadvantages is that a legitimate sender's address can get blocked by accident and it can be difficult to remove it from the blacklist due to the distributed nature of the list [25].

Computer filters are software that computers use in order to decide whether a particular email is spam or not. It is usually used in conjunction with a mail server and usually makes use of algorithms. More sophisticated are the *heuristics engines* are essentially rules of thumbs used by software to classify email. These rules are defined by humans and may, for example, look for text such as "Get very rich", "Congratulations! You have won..." A heuristic engine will often have thousands of these rules in order to try and catch spam. Once these words are recognised by the engine, the finding is assigned a score based upon that rule. Hence, the more spam like a message is, the higher the score assigned to it and thus the more likely that the message is spam [26]. However, with open source heuristic engines, spammers are able to gain access to the source code and can use these methods to groom their messages, making sure that they can pass through these filters without being detected.

The most recent and common method of classifying spam is by using *statistical classification*. There are many statistical methods available, but the most widely used one is the Bayesian filtering [26]. The difference with heuristic engines is that this method does not use a rule based filtering but uses the probability of how often words or tokens such as "get rich fast" within that email have appeared in previous spam emails. In order to achieve this, the filter will compare the body of a spam email to that of a legitimate email and will look for spam words. The advantage of using this method above heuristic engines is that statistical engines do not need much input from humans since they are self learning. This

method is highly regarded by experts as the way forward to fight spam [27].

The Gartner Group showed that most of the ISP in North America are making use of commercial software in order to block spam email from coming through their servers. The most popular one in use was Brightmail, a product from Norton Corporation and is efficient in blocking about 95% of spam mail [23]. Open source software accounted for only 8% of the total market share

Legal Issues

According to Overly [28] and Solkin [8], many lawsuits involving UCE have been filed in recent years, and a number of them have been successful. Costly lawsuits, as well as the vague status of the law regarding spam, have led to calls for legislation specifically designed to prohibit or restrict spam. Anti-spam legislation bills have been introduced into the United States Congress; currently 26 states have passed anti-spam laws [29]. Other countries as well as the European Union have considered enacting anti-spam legislation. The following paragraphs will discuss some of the legislation countries have enacted to combat spam.

An example of recent American legislation on spam disclosure requirements is the CAN-SPAM Act or "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003." The act states that it is illegal to send unsolicited email unless the subject header contains a key-word label identifying its content, thus deceptive subject lines and false headers are prohibited. This label is different, depending on the state. Each unsolicited commercial email must have opt-out instructions, allowing the recipient to stop any further unsolicited bulk mail. Finally the act requires that the sender attaches their name, street address and email address. This Act however, is merely an attempt to regulate spam rather than prohibit it [5].

The European Union has taken a different approach to spam, that of prohibition rather than regulation. Even though the EU itself does not prohibit spam, it does permit individual member states to do so. Finland, Germany and Italy are countries within the EU that have implemented laws prohibiting UCE. Austria, however, has implemented laws prohibiting both UCE and UBE [8]. The European E-Privacy directive requires that opt-in consent is necessary for the sending of all commercial e-messages in all forms of communication [29]. Other European countries are also on the verge of considering whether to enact similar restrictions.

In South Africa, spam is addressed in the 45th Section of the Electronic Communications and Transactions (ECT) Act, 25 of 2002 [30]. The Act specifies that spam as such is not illegal in South Africa. However, the spammer must abide by certain rules or else the person may incur an

unspecified fine or 12 months imprisonment. According to Bolin [31] the "Act is fraught with problems. It fails to give a clear definition as to what spam is and it actually even restricts the filtering of spam by ISP."

According to Solkin [8] lawsuits and targeted legislation can improve the spam problem by imposing costs and other disincentives on spammers. However, it is unlikely that legal approaches alone will be successful in eliminating spam. One of the major problems facing countries who are trying to impose spam laws is that they can only be effectively enforced within the country's borders. The distributed nature of the Internet makes it easy for people to send spam from jurisdictions where spam laws are not enforced [14].

Summary of the Research Survey

For purposes of this research, spam is defined as unsolicited email sent in bulk, of commercial or non-commercial nature. Spam is a growing phenomenon, constituting approximately half of the email in circulation. It can also be subdivided into various categories depending on the type of offer being made. The section has explored four main issues pertaining to spam, namely the ethical, social, technical and legal issues of spam.

The rapid growth of spam around the world has caused frustration among email users. The ethical issues discussed refer to the offensiveness of spam, false claims made in spam messages, cost shifting, email harvesting and freedom of speech. Socially, spam is seen as an annoyance, which decreases a recipient's productivity owing to sorting legitimate emails from UCE and can also be viewed as having a negative impact on emails reputation.

As a means of spam prevention or regulation technical and legal issues are discussed. Individuals and businesses can make use of filters or human based approaches as a means of blocking spam. Countries around the world have enforced legislation that either prohibits or regulates spam. Spam however originates from multiple sources, making spam legislation difficult to enforce due to the jurisdiction of such authorities.

3. Objectives of this Research

The primary objective of this research is to establish the extent of the spam problem in South Africa. It was intended that data gathered on spam in South Africa be analysed such that the results of this analysis can be compared to the results of similar research carried out in Europe and North America.

In addition secondary objective was to establish the volume of spam as well as the ethical, social, technical and legal issues of spam in a South African context.

It is hoped that this research can be used to develop awareness, both in South Africa and internationally, with regard to the state of spam and to shed greater light on the potential solutions that can be implemented in order to reduce the impact spam has on ISPs and email users.

4. Research Methodology

Two data collection techniques were used in this research. A questionnaire was used to capture quantitative data from email users and semi-structured interviews were used to obtain both quantitative and qualitative data from ISPs.

Questionnaires

The questionnaires consisted of various multiple choice questions, some taking the form of a likert scale. The questionnaire consisted of twenty-seven questions. The first six questions provided the research team with the respondent's profile in terms of age, gender and email experience. The next three questions tried to establish the respondents understanding of spam as well as the volume of spam email users are receiving.

The ethical issues surrounding spam were investigated in questions on the offensiveness of spam, false claims made by spam advertising, viruses sent through spam attachments, dictionary attacks, email harvesting and the possible violation of freedom of speech through the blocking of spam. The social issues of spam were investigated in four questions addressing the invasion of privacy by spam, the potential annoyance of spam, the productivity lost through sorting spam and finally spam's effect on email, its effectiveness and reputation. Finally, the last three questions of the survey questionnaire pertain to prevention techniques and the legal issues of spam. The questionnaire was piloted to e-mail users.

Interviews

Six interviews with ISP's were conducted. The objectives of the interview were to ascertain the volume of spam ISPs are receiving, to establish the burden in terms of time and cost spam is placing on ISPs and to establish what mechanisms ISPs have in place in order to overcome the burden of spam.

Sampling

The target population was individual and business email users in South Africa. The sample was somewhat contaminated by combining a convenience sample of users known to the researchers with a random sample of students at UCT. The sample is thus not likely to be very representative of all South African email users and the results of this research should be viewed as exploratory and provisional. The interviews with technicians at ISPs were also a convenience sample.

There was a strong bias towards respondents from the Western Cape. A limited amount of the respondents were from outside this province. One of the major constraints was the fact that the major ISP's were very reluctant to being interviewed due to the confidentiality of the information they had to provide. Only medium sized ISP's were willing to share their information with the authors.

Data Quality and Integrity

Questionnaire respondents were made aware of the fact that the data being gathered from them was totally confidential. This was of particular importance to the ISPs being interviewed.

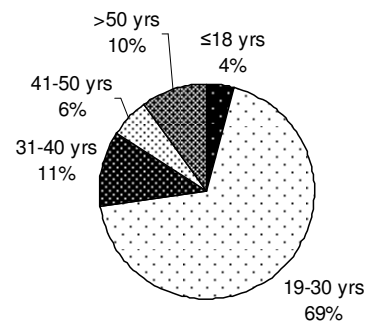
In order to ensure that the data was of a high quality, all the questionnaires that were answered were assessed for inconsistencies. About five of the administered questionnaires had erroneous data and were also carelessly answered and hence they were discarded. All the captured data was verified against the data in the questionnaire by another research team member.

5. Data Analysis for Email Users

Demographic Profile and Extent of Spam

A total of 70 responses were received to the e-mail user questionnaire. Overall, most of the respondents were between 19 and 30 years of age. However, the representativeness of the respondents can be questioned since almost two-thirds are female (63%).

Figure 1: Age Profile of Respondents

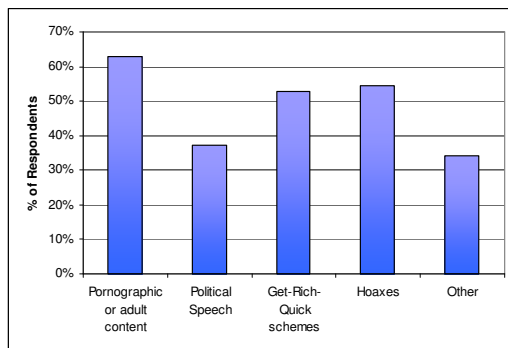


Most respondents (89%) consider themselves as experienced email users. Few of the respondents indicated that they had been using email for less than two years. Furthermore, the majority (78%) of the respondents indicated that they checked their inboxes at least once a day, if not more. When asked about how important e-mail is, the majority (84%) of the respondents said that email was vital for work purposes. Less than half of the same sample (43%) indicated that email was vital to them socially.

With regards to the quantity of spam in circulation in South Africa, the respondents indicated that they receive, on average, 15 spam emails per day. This contributes to (an average of) 27% of their inboxes. Interestingly, ISPs guessed that about 50% of all

email traffic is spam, thus their (or individual organisations') effectiveness in reducing spam is roughly 50%.

Figure 2: Types of Offending Spam



Ethical Issues

Interestingly, only 51% of respondents found spam offensive (29% was neutral and 20% did not find spam offensive). When the first group was queried on what specific types of spam offends them, it was clear that it is not just spam with adult or sexually explicit material or references that was considered offending (Figure 2). Hoaxes and business investment schemes that promised “get-rich-quickly” were considered almost equally offensive.

When asked about their attitudes of South African email users towards cost shifting, it was revealed that email users have a rather broad view. Less than a third of the respondents felt that it is not fair for ISPs to be burdened with the cost of spamming. Interestingly, 21% of respondents felt that ISPs should simply increase their bandwidth to deal with the problem, while a further 28% believe that it is not their problem.

When asked whether they had received a virus through spam, the majority (56%) of the respondents claimed that they were sure they had received a virus from spam before, while only 23% of the sample was sure that they had not.

Only 12% of respondents were of the opinion that blocking email violated someone's freedom of speech (63% did not feel so and 25% was undecided or neutral).

Social issues

With regards to the respondent's view towards privacy, it was found that more than half of the respondent's perceived spam to be an invasion of privacy (56%). 23% of the respondents did not find spam an invasion of privacy; the rest was neutral.

An interesting point that came across was that a few email users actually deliberately open spam emails (4%). Those users who did this did not view spam as an invasion of privacy.

One of the biggest social issues that spam constitutes is that of annoyance. Not surprisingly, 91% of respondents agreed that spam is annoying. Respondents estimated wasting, on average, 21 minutes per day to sort out legitimate email from spam.

Looking at the harm spam is causing, the majority of respondents (59%) perceived spam to be ruining the reputation and effectiveness of email, although 20% of the sample disagreed.

Legal issues

Most respondents (56%) felt that spam should be regulated, while only a third of the respondents felt that spam should be prohibited altogether. A third of the respondents believed that it is the ISPs duty to regulate spam by means of implementing filters. A further third believed that spam is an issue that should be tackled on a global level. 18% believed that it is their own responsibility to regulate spam. Finally 15% of the respondents believed that spam is an issue that should be addressed by the government by enforcing legislation.

Various correlation analyses were performed on the responses, most of them with negative results. Of the significant correlations that were found, none really appeared to reveal surprising insights. For instance, females and older people tended to find spam offensive more easily.

6. Data Analysis for ISPs

Interviews conducted with ISPs shed further light on the volume of spam in circulation in South Africa as well as various ethical, technical and legal issues surrounding spam.

Volume of spam

From the six ISPs interviewed, it was found out that the average amount of spam received on a daily basis was approximately 50% of incoming email.

ISPs also added that the proportion of spam received on a daily basis differed between weekdays and weekends. Figure 3 is a graph that portrays the email traffic during a typical fortnight. Although this graph was obtained from one specific ISP, it should be noted that other ISPs observed similar patterns in email traffic. The white gap between the sent and received emails reflects the amount of spam that was intercepted and deleted by the ISP. The troughs between the weeks represents weekends.

It is interesting to note that the relative proportion of spam to legitimate email messages increases very dramatically in the weekend – where it constitutes between 80 and 90% of all email traffic – even though the number of spam messages which are detected automatically stay approximately the same.

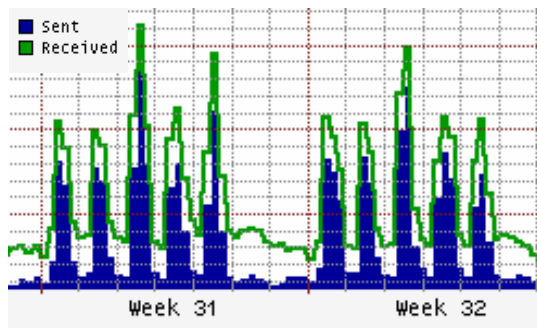


Figure 3: Typical Email Traffic Patterns

Spam can also be divided into categories depending on the content of the spam. Figure 4, obtained from an ISP using Brightmail, a commercial filter, shows the percentage of spam received per category for July 2004. Subsequent interviews with other ISPs confirmed that the major categories from which spam is received in South Africa are products, financial and adult.

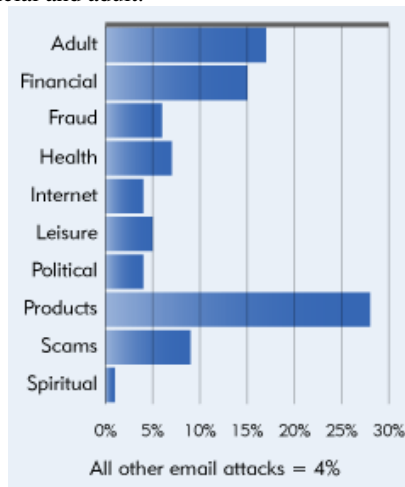


Figure 4: Categories of Spam

Ethical Issues of Spam

The ethical issues that were covered in interviews with ISPs reflected on cost shifting and malicious code.

Not surprisingly, all the ISPs interviewed felt it was unfair for their businesses to be burdened with the cost of spam. The words of one particular ISP stand out: "At least 50% of our incoming emails are spam; hence half of our bandwidth is wasted on junk." This ISP worked out that spam costs their business ZAR 72,000 per server per month (1US\$ \approx ZAR 6.50; Sep. 2005), a cost which is quite significant for a small to medium sized ISP in South Africa.

Interviews with the ISPs confirmed that intrusion does in fact occur quite frequently. Most of the ISPs admitted that they often receive large quantities of spam from legitimate organisations several times a week. These organisations have had

their servers "kidnapped" by a spammer, who is in turn using them to send spam.

Technical issues

The six interviews revealed that most ISPs use open source software, such as Postfix, SPF and Spam Assassin to combat spam. The software is used to filter spam coming through their SMTP servers. Only one ISP made use of commercial software known as Brightmail (a product of Norton).

Furthermore, several other techniques were put into place to filter the volume of spam being received along with incoming email. These techniques are however not used singularly, but are coupled with other filtering techniques so as to reduce the chances of spam penetrating their servers. The most common techniques in place were Bayesian filters, distributed blacklists, heuristic engines and statistical classification engines. Most ISPs agreed that Bayesian filters were the most effective in filtering out spam. However, it normally takes an ISP some time to discover the different headers used by spammers.

Some ISPs filtered spam even before it reached their SMTP server. The software known as Postfix analyses the headers and content of each incoming email and based on predefined rules it either accepts or rejects them. However, there are a few instances of false positives (i.e. a legitimate email being rejected). Furthermore, it was found that the smaller ISP's were not archiving their rejected email for future review, it was merely being deleted. Customers were also not necessarily aware that their emails were being filtered. The major ISP's have proper infrastructure in place so as to enable them to store the rejected spam. Their customers have special folders in their inboxes where all their spam gets stored.

Legal issues

The interviews revealed that ISP's considered legislation not to be effective due to the global nature of spam. They explained that spammers could simply move servers to countries with no legislation in place to avoid local laws. However, they believe that legislation can help to some extent in preventing South African spammers from sending unsolicited email. Further interviews with ISPs revealed that most spam comes from China, India and North Korea.

Currently, there are no specific anti-spam laws in South Africa and electronic communication is regulated by the ECT bill [Bolin 2004]. However, most ISPs believe that the ECT Act is not effective in combating spam because of the grey areas in the act. ISPs felt that the ECT act fails to define spam appropriately. For instance, an email that has an unsubscribe option is no longer considered to be spam according to the ECT act. Another area of concern is the fact that privacy laws in South Africa

do not allow ISPs to block emails, whether they are spam or not. Finally, ISPs are required to store all spam emails. This would cost ISPs a considerable amount of money in terms of bandwidth and storage.

Other interesting findings

Due to the high cost of bandwidth in South Africa, spam is rather costly to dial-up email users who have to download "junk" at a slow rate. The same ISP believed that the introduction of asymmetrical digital subscriber line (ADSL) in South Africa, could blow spam out of proportion due to the increasing amount of available bandwidth to subscribers and spammers.

7. Conclusions and Areas for Future Research

Email is undoubtedly one of the most important office tools in existence today. It also has significant social importance. The advent of spam has tarnished e-mail's effectiveness as a productivity tool. The aim of this research was to investigate the ethical, social, technical and legal aspects surrounding the issue of spam in a South African context.

It has been found that the research findings agree to some extent with the research done in Europe and North America. However, some findings that added to the research done previously.

The volume of spam in South Africa correlates well with that of the rest of the world. Spam is perceived to be unethical and disliked by email users. However, it is not only adult content spam which is considered to be offensive; even among the relatively young email users, the hoaxes and "get-rich-quick" schemes are considered offensive by more than half of the respondents. By contrast to some US research, blocking spam is generally not viewed as being limiting to the freedom of speech of the spammers. South Africa's fairly recently promulgated ECT act also has been found ineffective towards regulating spam. Finally, it was found that South African ISPs prefer open source software above commercial software to filter spam.

Globally it has been found that spam is a burden on both email users and ISPs. South Africa is no exception. It is hoped that this research has shed further light on the extent of the problem of spam in South Africa and that it may be used in shaping future policy concerning spam.

This study has hopefully also created the stepping stones towards further research. In South Africa, more people have access to mobile technology than people who have access to the internet and email. SMS (Short Messaging Services) spam is relatively new. However, if m-commerce follows the same trends as e-commerce, this form of spam may increase significantly. Therefore, research in this area would be recommended. Also, it would be

interesting to investigate how successful spamming campaigns are in South African from a marketer or seller's perspective.

8. References

- [1] Rogerson S. "Email Ethics," *IMIS Journal* Volume 10 No 1, 2000, pp 1-3.
- [2] Fallows D. "Spam: How It is hurting email and degrading life on the Internet," *Pew Internet and American Life Project*, 2003, pp 1-43.
- [3] Grimes G, Hough M & Signorella, M. "User Attitudes towards spam in three age groups," ACM Conference on Universal Usability, Vancouver, Canada, Nov 2003, pp 1-4.
- [4] Reynolds G. *Ethics in Information Technology*. Boston, Thomson, 2003, p99-100.
- [5] Federal Trade Commission. "False Claims in Spam", Report, 2003.
- [6] Leung A. "SPAM: The Current State" TELUS Corporation, White Paper, 2003.
- [7] Center for Democracy and Technology. "Why am I getting all this Spam?" Unsolicited Commercial Email, Six Month Report, 2003.
- [8] Solkin D.E. "Technical and Legal approaches to Unsolicited Electronic Mail" *University of San Francisco Law Review*, Vol. 35, 2001, pp 325-384.
- [9] Baase S. "A Gift Of Fire" New York, Prentice-Hall, 2003.
- [10] Williams C and Ferris D. "The Cost of Spam False Positives", Ferris Research Report #385, 2003.
- [11] CipherTrust. "Spam: A Security Issue". White Paper, 2003.
- [12] Everett-Church R. "Why Spam is a problem?" 1999. [Online] Available: <http://www.isoc.org/oti/printversions/0599preverett.html> [Retrieved 15 April 2004].
- [13] Commtouch. "Delivering an Effective Anti-Spam Solution - What Does it Take?" Report, 2003.
- [14] Arrison S. "Canning Spam: An Economic Solution to Unwanted Email", Pacific Research Institute, 2004.
- [15] Seward W. "Spam and the First Amendment" [Online] available: <http://email.about.com/library/weekly/aa111097.htm>. [Retrieved 12 June 2005].
- [16] Samoriski, J. H. "Unsolicited Commercial E-mail, the Internet and the First Amendment: Another Free Speech Showdown in Cyberspace?" *The Journal of Broadcasting and Electronic Media*, 2000, Vol. 43, No. 4.
- [17] Hermanson S. "Unsolicited Commercial Email (SPAM) and older persons online" AARP Public

Policy Institute, Data Digest Number 94 (2003), pp 1-6.

[18] Gordon S. "Privacy: A Study of Attitudes and Behaviors in US, UK and EU Information Security Professionals," Symantec Security Response, 2003, pp 1-16.

[19] Information Technology Association of America (ITAA). "Without question one of the most annoying feature of being online is spam" 2003 [Online] available: <http://www.ita.org> [Retrieved 2 August 2004].

[20] Kaatman M. "Unsolicited Commercial/Bulk Email and Consumer Privacy" 2003. [Online] Available:<http://www.house.state.mo.us/bills02/bills02/HB1042.htm> [Retrieved 12 June 2005].

[21] Udel J. "Canning Spam," Infoworld.com [Online] available: http://www.infoworld.com/pdf/special_report/Spam030721.pdf [Retrieved 2 August 2004].

[22] Federal Trade Commission. "A Report to the Federal Trade Commission of the Ad-Hoc Working Group on Unsolicited Commercial Email" Report, 1998, pp 1-32.

[23] Gartner Group. "ISPs and Spam: The Impact of Spam on Customer Retention and Acquisition". Report, 1999.

[24] Lazar J and Preece J. "Spam, Spam, Spam, Spam: How can we stop it?" Extended abstracts of the ACM CHI: Human Factors in Computing Systems 2003 Conference, 706-707.

[25] Nguyen K and Truong L.M. "PHEmail: Designing a Privacy Honoring Email System", *Communications of the ACM*, Vol. 12, No. 3, April 2003, pp 922-923.

[26] Gee K.R. "Using Latent Semantic Indexing to Filter Spam" Computational Linguistics Group & Centre for Computing and Language Studies, Trinity College, University of Dublin, 2003, pp 460-464.

[27] O'Brien C and Vogel C. "Spam Filters: Bayes vs. Chi-squared; Letters vs. Words", *ACM Transactions on Internet Technology*, Vol. 15 No. 5, 2003, pp 291-296.

[28] Overly M. "Email, Adult Content and Employment Law: Reducing Corporate Liability with Filtering and Policy Tools," 2002. [Online] Available: <http://www.postini.com/upe/> [Retrieved 10 Sep 2005].

[29] Corker J and Utz C. "SCAMS and Legal Approaches to SPAM," *The Cyberspace Law and Policy Series*, 2002, Continuing Legal Education Conference on International Dimensions of Internet and e-Commerce Regulation, pp 1-14.

[30] Republic of South Africa (RSA). "Electronic Communications and Transactions Bill", Minister of Communications, 2002.

[31] Bolin R. "Spam laws Worldwide: South Africa" Yale Law School, 2004.[Online] Available: <http://research.yale.edu/lawmeme> [Retrieved 31 August 2005]