

ZAMNET COMMUNICATION SYSTEMS LTD
(ZAMBIA)

Spam – The Zambian Experience

**Submission to ITU WSIS
Thematic meeting on countering
Spam**

**By: Annabel S Kangombe – Maseko
June 2004**

Table of Contents

1.0 Introduction	1
1.1 What is spam?	1
1.2 The nature of Spam	1
1.3 Statistics	2
2.0 Technical view	4
2.1 Main Sources of Spam	4
2.1.1 Harvesting	4
2.1.2 Dictionary Attacks	4
2.1.3 Open Relays	4
2.1.4 Email databases	4
2.1.5 Inadequacies in the SMTP protocol	4
2.2 Effects of Spam	5
2.3 The fight against spam	5
2.3.1 Blacklists	6
2.3.2 White lists	6
2.3.3 Dial-up Lists (DUL)	6
2.3.4 Spam filtering programs	6
2.4 Challenges of fighting spam	7
3.0 Legal Framework	9
3.1 Laws against spam in Zambia	9
3.2 International Regulations or Laws	9
3.2.1 US State Laws	9
3.2.2 The USA's CAN-SPAM Act	10
4.0 The Way forward	11
4.1 A global effort	11
4.2 Collaboration between ISPs	11
4.3 Strengthening Anti-spam regulation	11
4.4 User education	11
4.5 Source authentication	12
4.6 Rewriting the Internet Mail Exchange protocol	12

1.0 Introduction

I get to the office in the morning, walk to my desk and switch on the computer. One of the first things I do after checking the status of the network devices is to check my email. Today, I have 150 emails. As I look through my mailbox, I find that I have 2 personal emails, 15 from the mailing lists I subscribe to, perhaps 5 from customers, and the rest is junk mail.

I look through the spam mail and find that it ranges from emails encouraging me to extend the warranty of the car, get a degree without writing the exam, pornographic emails, buy a potency drug or make money fast.

Definitely an annoying way to start the day: and more so for people that have slow links. There has been a noticeable increase in spam in the last 2 years and this has resulted in increased user irritation, increased cost to the customer and the service provider, and an increased load on the servers and a hog of available bandwidth.

1.1 *What is spam?*

The term 'spam' was popularised by a famous Monty Python sketch and has since been adopted by the Internet community to signify Unsolicited Commercial Email (UCE). Hormel and SPAM's position to the use of this term is; I quote:

'We do not object to the use of this slang term to describe UCE, although we do object to the use of the word "spam" as a trademark and to the use of our product image in association with that term. Also, if the term is to be used, it should be used in all lower-case letters to distinguish it from our trademark SPAM, which should be used with all uppercase letters. '¹

Spam is usually sent to a large number of people who did not ask for it. Spam also refers to the inappropriate use of mailing lists.

1.2 *The nature of Spam*

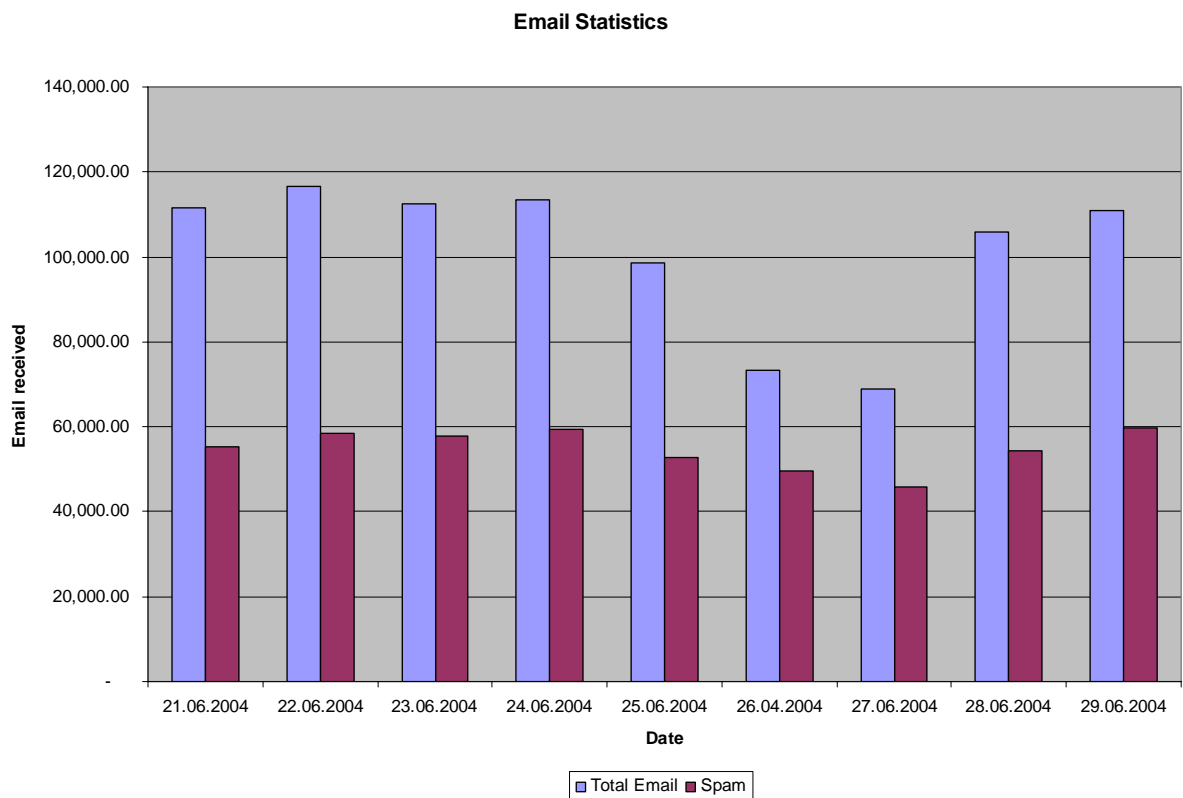
Some unsolicited commercial emails contain material which is vulgar or pornographic in nature. With the increase of Internet access by minors, this poses a great moral problem on the Internet. Other unsolicited commercial emails try to sell real estate, or encourage users to take part in "Make quick money" scams, an example of which is the infamous "Nigerian" scam. Some

spammers try to sell potency drugs such as 'Viagra' while others claim to have drugs that slow the ageing process.

A common factor of spam messages is that the addresses are usually forged in an attempt to mask the source. Other spammers attempt to escape detection by varying the subject or change the spelling of words. For example, Viagra may be spelt as v.i.a.g.r.a or V1.agra. Some UCE or spam emails also contain a link that the user is expected to follow if they wish to unsubscribe or get more information.

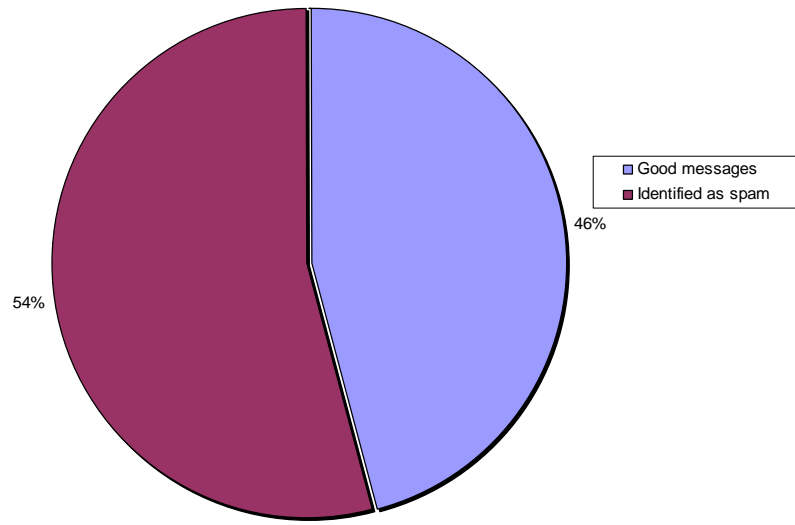
1.3 Statistics

From experience, ZAMNET Communication Systems Ltd, the leading ISP in Zambia, has estimated that more than 50% of email messages passing through their server qualifies as spam. The graph below shows the amount of spam in relation to the total messages received.



The pie chart below gives an illustration of the ratio of spam to legitimate email messages received by ZAMNET's filtering server between June 21, 2004 and June 29, 2004. As can be seen, 54% of emails received were spam as opposed to 46% of genuine messages.

Legitimate email - spam ration (%)



2.0 Technical view

2.1 Main Sources of Spam

2.1.1 Harvesting

Spammers typically use automated software, robots and spiders to search the Internet and collect or “harvest” lists of email addresses from web sites, newsgroups, chat rooms, mailing lists, and other online resources.

2.1.2 Dictionary Attacks

Dictionary attacks use software that automatically requests likely email addresses by combining letters and numbers in an attempt to find or validate active email addresses. These randomly generated addresses are then added to known domains and may reach existing mailboxes.

2.1.3 Open Relays

An open relay is an SMTP server that allows third parties to send mail through it. It is typically a poorly configured server which is open to abuse from anyone. With the growing awareness of the problems associated with poorly configured SMTP servers, administrators are now taking more time securing their servers against third parties. This has resulted in a reduction in spam generated by open relays on the Zambian network.

2.1.4 Email databases

Email databases are available for sale at cheap rates. They are also available in categorised lots, e.g. exporters, importers, etc.

2.1.5 Inadequacies in the SMTP protocol

The SMTP protocol was created at a time when the world had an innocent view of email communication. As a result, the protocol is too trusting. It assumes that you are who you say you are.

The SMTP process is initiated by a user mail request. This results in the sending SMTP server establishing a two-way transmission channel to the receiving server which may either be the ultimate destination or an intermediate. The two servers then enter into a conversation that leads to either the message being accepted or rejected.

2.2 Effects of Spam

Email has proved itself in today's technological world as a fast and reliable means of communication. It is also attractive because of the low cost of sending correspondence.

Marketers today have taken advantage of email for their direct marketing techniques. Off course, one of the other reasons they have decided to use it is because it is cheaper than traditional advertising. As a result, the legitimate email marketers have to continuously adjust their business practices to comply with changing regulations. They also suffer from a dented image because of the stigma associated with spammers to whom they are associated.

On the other hand, customers are inundated by spam filled mailboxes on a daily basis. Whereas some of these messages appear innocent and mild, others are quite offensive. Imagine a mother checking her mail with her young child sitting nearby. She opens a message that turns out to contain explicit sexual material. It is very disturbing and reduces the value that the parent places of email communication. There is a danger that it may be viewed as a threat to the moral training of children today.

Spam has basically resulted in:

- Increased user irritation and annoyance
- Reduction in productivity
Users usually spend valuable time sorting through the messages and deleting spam from their mailboxes. Some ZAMNET customers actually check mail via the web mail interface and delete the spam messages before downloading their messages using an email client.
- Increased email storage space
- ISPs loss of reputation
- increased bandwidth consumption
- Increased customer complaints
- Increased CPU processing time for the ISP
- A degradation in processor performance
- Displacement of normal email

2.3 The fight against spam

Spam has increased to such an extent that the whole world is focused on stopping this assault. Administrators are now trying to use different methods of

stopping spam such as the use of black lists, white lists and anti-spam programmes.

2.3.1 Blacklists

Blacklists use an industry standard format for communicating with email servers. These are basically lists of IP addresses associated with open relay email servers as well as servers that are known to host spamming. Many of these lists are publicly available online either for free or at a fee. A lot of system administrators have started using the lists to block incoming email from listed addresses. A well-known black list is hosted by SpamCop, located at www.spamcop.net and another one is Open Relay Database, located at www.ordb.org.

2.3.2 White lists

White lists are the opposite of blacklists. They list trusted email addresses and domains that are always allowed to send email. Although White lists allow email coming from a trusted source to come through, they do not provide a solution for blocking spam.

2.3.3 Dial-up Lists (DUL)

Some ISPs block access to their servers if the incoming connections originate from dynamic IP addresses. Their goal is to force users that are running email servers on their dial-up connections to send all outgoing email through their ISP's email server.

2.3.4 Spam filtering programs

Some ISPs in Zambia are using spam filtering programs to help identify spam and reduce the number of spam being delivered to customer's mailboxes. These applications examine the email messages and check for specified patterns, listing in blacklists, listing in white lists, among others. Most of these applications use certain algorithms such as Bayesian calculations.

The Bayesian approach estimates the likelihood of an email being spam. Spam filters that use the Bayesian approach use previous examples of actual email and spam messages to classify new mail. Bayesian statistics are also applied to observations to calculate probabilities.

More details about Bayesian spam filters may be found in <http://www.paulgraham.com/spam.html> and <http://www.paulgraham.com/better.html>. An example of such an application is SpamAssassin and MailScanner.

2.3.5 Anti-spam regulations

Many countries in the world are now taking the initiative to come up with legislation that deals with the issue of spam on the Internet. This is an important first step as it may bring some sanity to email traffic. It is important that these laws should not legitimise spam or junk emails. The CAN-SPAM Act seems to have legalised spam provided they meet certain conditions.

2.4 Challenges of fighting spam

Blacklists are thought to be very effective because they stop spam before it reaches the mailbox. Then why is there such an outcry against ISPs that use blacklists to stop spam? The main problem here is that the owners of the lists are not accountable. The procedures set up to add a server to a black list are also quite questionable. For example, if an Internet service provider's email server is blacklisted, the customers that use that server will not be able to send out their messages. Most administrators do not even realise that they have been blacklisted until they start to receive complaints of mail not reaching their recipients. This has serious implications as it can hinder communication via the Internet.

From experience, we have noticed that it is not always easy to appeal once a server has been blacklisted. SpamCop now keeps the server in the database for 48 hours before removal although administrators are also given the option to appeal. Many may find that it is probably easier to wait out the 48 hours.

White lists also pose a problem as they require constant maintenance to be very effective. If not properly maintained, the risk of losing e-mail from legitimate sources is quite high. On the other hand, one has to take into consideration that one man's poison is another man's meat. Some white lists are global which means that if a spammers address is listed, all the other users that use the same spam filtering server will receive messages they consider spam.

Another point to consider is the danger of blocking legitimate email messages by specifying aggressive rules and making reference to blacklists. This causes friction between the service provider and the customers. Although people are against spam being proliferated on the Internet, they also want to be able to receive all their valid emails. Internet service providers there need to strike a balance between allowing more spam through their servers or stopping all spam and causing customers to lose legitimate messages.

There is also the question of what one calls spam. Each person or entity is different from the next. It is likely that some people will prefer to receive email messages that the next person considers spam.

Spammers may be challenged to prove that the measures being put in place are not effective and increase their spam sending efforts. It could be classified as some form of survival instinct. The more Netizens fight back, the more sophisticated spammers become. To prove this point, one only has to look back at the last few years. The increase in spam can easily be traced to the time that an announcement to seriously fight spammers was issued.

3.0 Legal Framework

3.1 *Laws against spam in Zambia*

Zambia does not currently have laws that can be used to fight spam. The existing Telecommunications Act in Zambia, enacted in 1994, is not cyber aware. It is focused on the protection of telecommunication infrastructure.

A part of the Telecommunications Act of Zambia states that:

Any person who without lawful authority-Wilful damage to or interference with Telecommunications disturbs, obstructs or impedes in any way the free and proper use or working of any such apparatus or of any telecommunication system;

This is the closest the Act comes to making reference to the ‘denial of service’ and ‘load on bandwidth’ effects of spam. This is clearly not sufficient to convict spammers.

However, the Act is now under review and gives an opportunity to put clauses that deals with this menace.

3.2 *International Regulations or Laws*

3.2.1 US State Laws

Laws have been enacted in each of the US States that require a label at the beginning of the subject line. For example, the law enacted in Alaska requires a label (ADV:ADLT) at the beginning of the subject line of any sexually explicit UCE message; The law in Arizona require that UCE messages include a label (ADV) at the beginning of the subject line and contain an opt-out mechanism.

The State laws apply if the message is sent from within that particular State in which the law applies or if the recipient’s service provider is based in that State.

Although these laws are quite similar, they carry different variations such as the requirement for an opt-out option and/or instructions, or the ban of false subject lines, or the inclusion of a functioning reply e-mail address, or the misrepresentation of the source address.

3.2.2 The USA's CAN-SPAM Act

The United States of America recently enacted a law that can be cited as 'Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003' or the "CAN-SPAM Act of 2003". This Act is intended to create a national standard of spam regulation and applies to both the person sending the commercial message and the one advertising in such an email. The Act supersedes individual state laws which may, unfortunately, be more strict and have stiffer penalties.

The CAN-SPAM Act prohibits a number of activities such as:

- The distribution of predatory and abusive commercial email messages;
- The sending of multiple email messages that contain false header information
- The unauthorised use of protected computer systems to relay messages
- The use of misleading headers. Senders must identify themselves in the 'From' header line
- Spoofing
- Use of deceptive subject headings
- Sending messages through email or domain names obtained under false identities
- Using automated programming scripts to sign up for email accounts
- Address harvesting and dictionary attacks

The Act requires the sender to:

- include a valid postal address in the email messages
- give a clear indication that the message is an advertisement or solicitation
- include a valid return email address or other means to respond to the message
- Inform recipients of their right to decline the message.
- Issue warning labels in the subject header for messages containing sexually explicit content

The Act also requires that UCE messages include an opt-out option to recipients. This may be provided by furnishing the recipient with an email address to which they can unsubscribe or a hyperlink. It is unlawful for the sender to send commercial emails to the recipient after the opt-out.

4.0 The Way forward

If the dream of a World Information Society affirmed by the 2003's World Summit on Information Society is to be realised, the threat of spam has to be faced head-on. The following are some proposals on possible ways of reducing spam on the Internet today.

4.1 A global effort

The Internet is basically a global community and that means that no nation remains unaffected by the spam scourge. Each nation in the world should sit down and come up with regulations to fight the scourge. But is this enough? Far from it! This is one "NET" disease that the world needs to fight as one. The fight against spam should be a global and concerted effort between nations and governments. The laws and regulations put in place in each country should carry weight even where spam is sent to a country that is yet to come up with anti-spam laws.

4.2 Collaboration between ISPs

Internet service providers need to cooperate in fighting spam on the Internet. Some Internet Service providers are so frustrated by the levels of spam that they simply block a whole domain without warning or notice. This, in most cases, may cause legitimate email messages to be lost, resulting in loss of business opportunities or critical information. It is important for ISPs to be able to communicate. If ISP A has a problem with a customer spamming from a competitors network, ISP B, ISP A is obliged to inform the other ISP and work together to stop the problem. If blocking is required, it would be for a short period of time causing a minimum loss of emails. It is also up to each ISP to monitor customer's traffic and ensure that they comply with the set rules of the Internet community.

4.3 Strengthening Anti-spam regulation

Nations should work towards strengthening legislation so that they clearly spell out the consequences of those found guilty of generating spam or aiding its propagation. This should include penalties for network owners who neglect to secure their mail servers or wilfully expose customers' email addresses.

4.4 User education

User education is another factor that may help reduce spam propagation. The user must know what to do and what not to do. Some users are not aware that

they give away their email addresses or grant the site owners permission to send them marketing emails while 'surfing' the net. They should be advised to make sure that they are not subscribing to mailing lists whose emails they do not want to receive.

4.5 Source authentication

Authenticating senders may also help to curb spam. This would probably be more effective if it is dealt with at ISP level.

4.6 Rewriting the Internet Mail Exchange protocol

Since the SMTP was initially written without this problem in mind, it may be necessary to write a new RFC to define secure and authenticated email exchange protocol. This option would render current mailers obsolete but may be the only workable solution to the problem. Maybe Simple Mail Transfer Protocol is too simple for the emerging Information society!