

Running head: FIGHTING SPAM

Fighting Spam

Benny C. Rayner

East Carolina University

Abstract

Spam is a nuisance to never be taken lightly. Spam can cause personal loss to e-mail users and to businesses. Lost of revenue and internet resource can be two of many affects that spam can have on a business. This paper discusses the affects of spam and how you can protect yourself from spam. Some of the solutions mention to defend against spam is honeypots, whitelists, blacklists, and many other tactics discussed throughout the paper. Spam has been such a big nuisance that now web clients such as hotmail, gmail, etc., has incorporated spam blockers. There is also a discussion on many acts and campaigns against spam to lessen the affects. Because of these acts and campaigns spam has moderately been on a decline.

Have you ever had an e-mail account that hasn't been used for a while? When you think to check this e-mail account, do you have e-mails from random people and places? You have been spammed! Anyone and everyone can attest for these malicious, agitating, self-replicating e-mails. Although e-mail is an important and popular means of communication, spam is a nuisance as it accounts for over half of all e-mail sent each day.

Spam, also known as junk e-mail, can come to have many definitions. Spam can be unsolicited e-mail, often of a commercial nature, sent to multiple mailing lists, individuals, or newsgroups. Chain letters can be spam. The most infamous example is any variation on "Make Money Fast!" but there are others that don't involve money. The ones that do are a felony (mail fraud) in addition to being a form of spam (Mansker, 1999). Spam can also be off-topic or inappropriate posting. This can be either to a mailing list or to a newsgroup. An example of this form of spam is posting a message concerning your litter of kittens on a mailing list devoted to NT security updates.

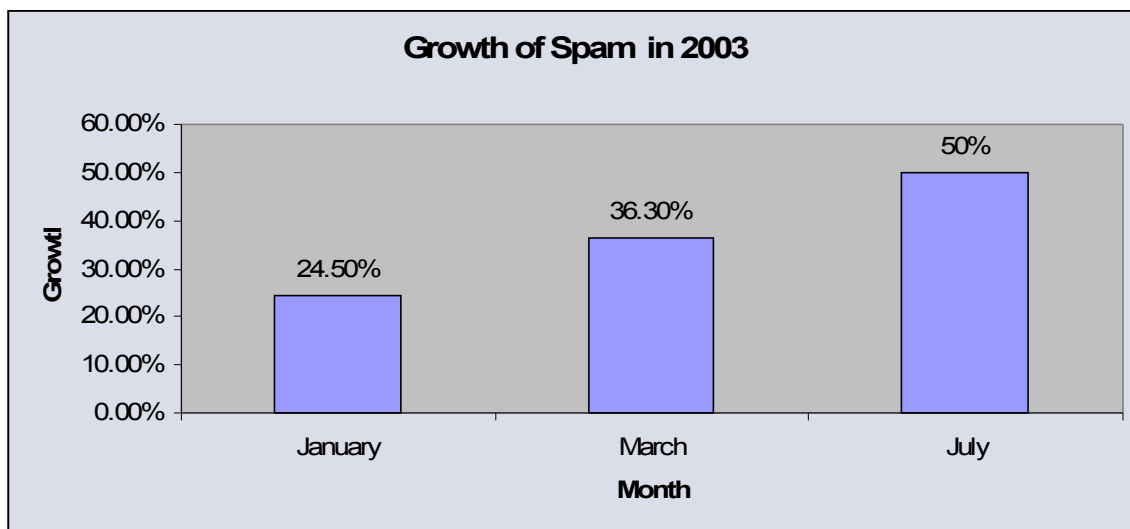
Spam can also be caused by computers hijacked by Trojan horses. MX Logic, an e-mail security company, reported that 56% of all spam filtered by the company in July 2005 originated from hijacked computers (Vamosi, 2005). Networks of these compromised or "zombie" PCs are being used as spam relays because they hide the true sender.

The first known trace of spam was twenty five years ago. This junk e-mail was sent on the Arpanet, the forerunner to the Internet, in 1978 (Hinde, 2003). Spam since then has been an exponentially growing nuisance. A fight has arisen with spam similar to the fight with viruses. Just as a computer virus has a life cycle, spam also seems to

resemble the same life cycle. Spammers eat Internet resources for their own benefit just like viruses eat computer resources for its own benefit.

Spam has created important costs for industry as well as being annoying, time-consuming, and money-consuming. A national survey of e-mail trends found that junk e-mail and spam sent by family, friends, and colleagues can be just as annoying to employees and costly to companies as commercial spam. The growth in spam has now outpaced growth in normal e-mail traffic, from 7% two years ago to 50% (Hinde, 2003). The illustration below depicts the rapid growth of spam from the months of January, March, and July. In June of 2006, spam made up 64.8% of global e-mail traffic, an increase of 6.9 percent over the previous month (Espiner, 2006).

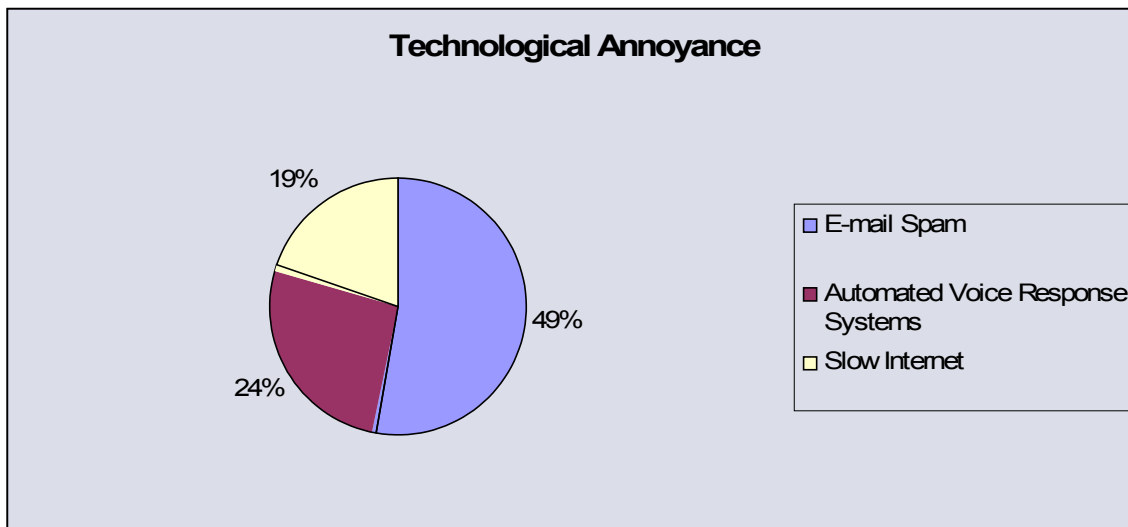
Chart 1: Growth of Spam



Spam has come to be a great annoyance not only for the e-mail user, but also for I/T personnel. I/T and telecom industries have been one of the hardest hit with one in every 2.66 e-mails being spam. Spam cost many companies lost in productivity alone. This includes the time it takes people to delete the messages, the cost of buying larger mail servers and storage systems to cope with the inboxes flooded with the messages, and

the cost of having staff unclog networks overloaded by spam. When comparing spam to other technological annoyances, spam by far is the largest annoyance (see Chart 2).

Chart 2: Technological Annoyance



Spam is a nuisance in many ways. Spam can inconveniently clog up the internet and bandwidth causing impact upon the growth of e-commerce businesses. It is said that if spam keeps expanding at its present pace, it may well bring Internet to an end (Gonzalez-Talavan, 2006). Much of the content is offensive and employers have a duty to protect employees from such material. There has been many cases in the US where employees have sued their employer for not protecting them from sexist jokes. One of the cases settled for \$4 million (Hindes, 2003). Parents also wish to protect their children and on some occasions parents have closed e-mail accounts to protect them.

Spam can cause problems in many different ways for e-mail users and businesses. From a user's perspective, it's wasteful of their time and resources and can mislead people to making wrong decision upon their e-mail. It takes time to filter through e-mails that are mixed with spam. From a business perspective spam can cause cost shifting, resource wastage, and fraud.

From a user standpoint fraudulent tactics have been employed to encourage recipients to open spam messages. A simplistic approach has been to alter the subject line in the message to imply the message is not advertising-related.

Fraudulent message relaying is also employed to disguise the origin of messages. For example, messages may be sent from the source to a third party's server which has been configured to relay messages to recipients. Filtering schemes employed by the ISP will be avoided because the source of the message will appear to be an innocent party. Furthermore, complaints from recipients will be sent to the third party, instead of the actual message source. In this case, the spammer avoids all responsibility for costs involved, while remaining anonymous. Fraud may also be present in the content of the messages themselves, which may advertise miracle cures to diseases, or illegal financial schemes.

For businesses, cost may be measured in many forms, the most obvious of which is the bandwidth consumed by recipients in the processing of spam mail traffic. In large businesses, Internet connections are charged on the basis of traffic, and for such firms, spam mail has a measurable cost in unwanted megabytes of incoming traffic. ISPs also incur costs in the form of CPU time devoted to processing thousands of unwanted messages. If the CPU of the mail server becomes over loaded with spam messages, legitimate messages will be delayed while the queue is processed. Mail servers must not only process junk mail, but also store it, leading to accounts which quickly exceed quota limits. ISPs purchase bandwidth which is used to provide services to subscribers. If significant volumes of bandwidth are consumed by junk mail messages, the ISP is faced with one of three scenarios (Cournane, Hunt, 2003):

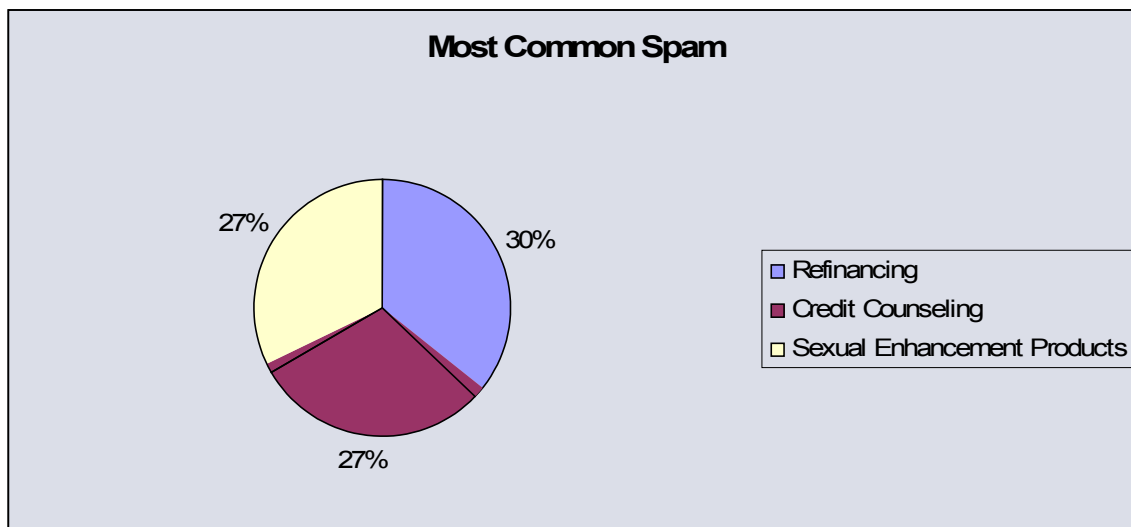
1. Continue to provide subscribers with a slower Internet service due to junk mail traffic.
2. Absorb the costs of increased bandwidth usage.
3. Increase charges to subscribers to compensate for greater bandwidth usage.

Traffic congestion is a severe problem in the current internet infrastructure.

Messages sent to millions of recipients' compound congestions as packets are flooded onto the internet which essentially contains unwanted data. System administrators are forced to handle routers with overloaded queues of e-mail packets from a single source. The burden of handling spam lies not only with recipients, but also with intermediate networks which route the packets. This is regarded as a waste of network resources, as the data are typically deleted as soon as they reach their destination.

The most frequent form of spam is refinancing (see chart 3). Spammers are now turning, however, to mobile text-messaging. They are doing this to bypass e-mail based anti-spam measures and more effectively target recipients based on their age, location, and other characteristics (Espiner, 2006). Social-networking sites, such as MySpace.com, offer spammers a new level of convergence and capability to profile people.

Chart 3: Most Common Spam



A company by the name of MessageLabs has seen an increase in Instant Message (IM) spam, also known as spim. IM and the Web has seen huge hike in link spam. Spammers send just a hyperlink, which can lead to a malicious site, or a phishing site.

Spam is a serious threat amongst e-mail users. The infamous '419' advance fee fraud scam is a major source of spam which takes its victims for hundreds of millions of dollars yearly (Edelson (2003)). 419 refers to the relevant section of the Nigerian criminal code. The spam comes in the form of a letter. The goal of the letter is to rob you. The sender claims to be a bureaucrat, banker, royal toadie or relative of a powerful personality who wants to cut you, and only you, in on the financial deal of a lifetime. He claims to be in a position to skim public accounts, siphon off an unclaimed inheritance. You are to help move the funds abroad by providing a bank account, in return for a generous commission. It is all to be kept quiet. The letters infrequently arrive in multiples, with attachments containing the e-mail address of numerous other recipients. Many people have become victims of this spam letter. This is one of many 'scam spam' letters. The victims are often people in modest circumstances, who think they are helping somebody. Many have been ruined in this manner.

There has been many cases of spammers being prosecuted for their malicious acts. Two Russian immigrants were caught and sentenced to two years in jail for their part in an e-mail spam scam that clogged US ISPs with more than 50 million e-mails and defrauded victims of more than \$250,000 (Hancock, 2001). The two Russians were able to harvest e-mail addresses and then send out more than 50 million e-mails through a Flashnet (a division of Prodigy Communications LP), with the use of some commercial

software. E-mails were sent out by the two asking job seekers to pay \$35 to learn how to make thousands of dollars by working out of their homes stuffing envelopes.

What can be done to eliminate spam? What can e-mail users do? There are many ways to combat against spam. Preventive methods can be taken such as trying to prevent spammers from including one's e-mail address in their lists.

Blacklists are lists of e-mail or machine addresses from which it is known that spam is sent. They may be personal or public, local, or distributed. When a message arrive coming from an address or machine listed on the blacklist, it is rejected.

Honeypots, in connection with blacklists, consists of invented e-mail addresses. Their aim is to attract as much spam as possible in order to alert other users or take further measures. They are based on spam usually being distributed in bulk. Characteristic features are obtained from received messages. User software connects to the honeypot to find out if the relevant message has already been received there.

Whitelists are opposite of blacklists. They consist of a list of address from which all mail is accepted. Mail coming from other addresses is transferred to a low priority folder. A few commercial implementations are available and some of them evaluated in PC Magazine (Gonzalez-Talavan, 2006).

Content filters compute a score for each incoming message as a function of some previously user-established criteria. If the score of the message is greater than a given threshold, the message is consider spam.

Bayesian filters uses statistics about the content of the message for purpose of being able to classify it as spam or not. Users must train their filters to make them learn which messages is spam and which is not. This method is appealing because it is

adaptable. It learns from its users' concept of spam as more and more messages are processed.

Although no systems are currently available commercially, some efforts have been made for neural networks. If a human being is easily capable of detecting spam, perhaps artificial intelligence should be tried out.

Sender Id is a method devised to get rid of forged sender information (domain spoofing). It asks the presumed sender domain for IP addresses from which that message can be sent. The message is considered spam if the e-mail connection did not come from one of those.

There are many ways that an average user can avoid spam. One way is to try not to display your e-mail address in public. That includes newsgroup postings, chat rooms, websites or in an online service's membership directory. Another way is to check the privacy policy when submitting your address to a website. See if it allows the company to sell your address. Using two e-mail addresses, one for personal messages and one for newsgroups and chat rooms is another way of cutting down on spam. Also considering using a disposable e-mail address service that creates a separate e-mail address that forwards to your permanent account may prove to be useful. If one of the disposable addresses begins to receive spam, shutting off the account will not affect the permanent address. Use a unique e-mail address (You've Got Spam, 2002). The choice of e-mail address may affect the amount of spam received. Spammers use "dictionary attacks" to sort through possible name combinations at target ISPs or e-mail services, hoping to find a valid address. A common name such may get more spam than a more unique name. Using an e-mail filter works well. E-mail accounts normally provide a tool to filter out

potential spam or a way to channel spam into a bulk e-mail folder. All of these are ways to avoid getting 'spammed by spammers'.

There is light at the end of the tunnel with accordance to spam. E-mail users do not have to fight the fight against spam alone. According to the Federal Trade Commission (FTC), the public are getting less spam because of better anti-spam technologies (Hilley, 2006). America Online (AOL) reported that its members received 75% less spam in 2004 than in 2003. This reduce in spam could be the caused by cutting off zombies, which are used to distribute 60-80% of nuisance e-amil. The Anti-Spam Technical Alliance, which represents a number of ISPs, have blocked zombie access to port 25 making it difficult for them to send spam.

Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM) is a U.S. statute introduced January 1, 2004 that allows spammers to be fined up to \$6 million. The Can-Spam Act has helped in the fight against spam. The Act has given low enforcement a tool to prosecute spammers. Fifty cases have been brought against spammers since the Act's introduction.

To help the fight even more against spam, AT&T Worldnet, Concentric Networks, Earthlink, Excite, Fastnet, Flashnet, and Juno Online Services, have joined Bright Light Technologies' Global Probe Network (Wehde, 1999). The Probe Network uses 20 million fake e-mail addresses to gather e-mail. Because the addresses have no purpose other than to gather unsolicited e-mail, and e-mail received at them is necessarily spam. The messages are then transmitted in real-time to the Bright Light Operations Center (BLOC). Using this method, Bright Mail defeats many spam attacks before they damage communication infrastructures or enter users' mailboxes.

There is also a device called the Spam Cube which is designed to fight against spam. This cube is 4.5 inches and sits between your cable modem and computer or router. The Spam Cube automatically downloads spam definition updates from its manufacturer and can filter any POP3 mailbox (Ackerman, 2006). This could be a good way to get people's money for the cube does the same thing as other "free" antis spam software.

There are many software products on the market to help prevent spam. Syamntec Brightmail AntiSPAM not only defends against real-time spam attacks, but also proactively identifies first-time spam. With flexible and powerful spam management capabilities, it meets enterprise security needs without a significant administrative burden.

SpamPal is free software that sits between your e-mail program and your mailbox, checking your e-mail as you retrieve it. Any e-mail messages that SpamPal considers to be spam will be "tagged" with a special header. After that you can configure your e-mail client to filter anything with this header into a separate folder and your spam won't be mixed up with the rest of your e-mail.

Almost every web-based e-mail client has some type of spam deferent. Web clients such as hotmail, gmail, yahoo mail, and many others has incorporated ways to identify spam. If you are constantly getting e-mail from a source that you think is spam, you can label that particular e-mail as spam and it will automatically be transferred in to a spam folder. This is very much like the SpamPal mentioned in the previous e-mail.

In conclusion, spam is not to be taken lightly. Spam can cause e-mail users and businesses a lot of headaches and pain by causing a lost in cost and resource wastage.

Overtime spam has gotten better, but as with hackers, where there is a will there is a way. Maybe one day the meaning of spam will merely a canned meat product consisting primarily of chopped pork pressed into a loaf.

References

- * Cournane, A., Hunt R. (2004). An analysis of the tools used for the generation and prevention of spam *Computers & Security*, 2004, Volume 23, Issue 2, 154-166
- * Edelson, E. (2003). The 419 scam: information warfare on the spam front and a proposal for local filtering *Computers & Security*, 2003, Volume 22, Issue 5, 392-401
- Espiner, T. (2006, July 6). Retrieved July 14, 2006, from Spim, splog on the rise Web site: http://news.zdnet.com/2100-1009_22-6091123.html
- * Gonzalez-Talavan, G. (2006). A simple, configurable SMTP anti-spam filter: Greylists *Computers & Security*, 2006, Volume 25, Issue 3, 229-236
- * Hilley, S. (2006). Spam whacking working in US says FTC *Computers & Security*, 2006, Volume 2006, Issue 1, 2-3
- * Hinde, S. (2002). Spam, scams, chains, hoaxes and other junk mail *Computers & Security*, 2002, Volume 21, Issue 7, 592-606
- * Hinde, S. (2003). Spam: the evolution of nuisance *Computers & Security*, 2003, Volume 22, Issue 6, 474-478
- Mansker, A. (1999, May). Retrieved July 14, 2006, from Email s-p-a-m: It comes in many forms, but none have any meat Web site: <http://itimes.ucdavis.edu/v7n6may99/spam.html>
- Vamosi, R. (2005, August 10). Retrieved July 13, 2006, from Zombie PCs spreading spam Web site: http://reviews.cnet.com/4531-10921_7-6293937.html
- (2002, April). Retrieved July 13, 2006, from You've Got Spam: How to "Can" Unwanted Email Web site: <http://www.ftc.gov/bcp/online/pubs/online/inbox.htm>