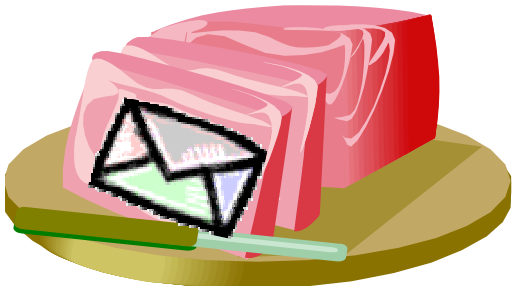
SPAM: *It's not just for breakfast anymore.*



One Victim's Rant

by Kurt E. Berger

Abstract

This paper is a somewhat lighthearted look at the origin and proliferation of spam and its mutation from mere annoyance to serious security threat. Many laws have been proposed, but very few have actually passed both House and Senate and none have been effective in any way. Spammers, like criminals, can be profiled and share common traits. There are countless approaches to solving the spam problem, and no one solution fits every situation. While spam will never be eliminated entirely, an industry standard form of authentication likely holds the key to a nearly "spam-free" future.

Introduction

What follows is a brief discussion of an annoyance which doubtlessly plagues every person who uses the Internet – particularly email or newsgroups. The term "Internet" encompasses, but is not limited to: email, newsgroups, the web, ftp resources, and the invisible web. While it is possible that email and the web could be mutually exclusive for some, it is much more likely that users partake in at least two or more online resources. Spammers often troll these areas for victims which they view as potential customers. The origin of the term "spam" is unclear, but it is likely a product of Monty Python or was coined by Usenet users. Spam is practically free compared to direct mail, and it is logical that many direct mailers have upgraded to spamming as a means of eking out a living on that proverbial one percent response rate. Businesses and network administrators share a healthy loathing for these unwanted solicitations that consume bandwidth, hard drive space, and employee productivity. There have been many attempts to legislate the problem away. The result of such legislation has been entirely ineffective. There are countless approaches to solving the spam problem. Some firms slew their spam dragons while others got burned. What does the future hold? Countries could pass more stringent laws or someone may create that perfect program that would solve the problem once and for all. The future of spam is clear in this writer's humble opinion – it will be added to life's certainties: death, taxes, and spam.

Origin of Spam

Were does the term come from? One might have guessed that spam was an acronym, but according to many web sites, there are no acronyms. Spam is loosely defined as "unsolicited commercial email sent to a large number of addresses." [1] Predating email spam, unsolicited

posts to Usenet in the early 1990s caused newsgroup users to harbor acute acrimony for spam as it drove many people from using the forums. Webopedia proposes two origins for the term:

> There is some debate about the source of the term, but the generally accepted version is that it comes from the Monty Python song, "SPAM SPAM SPAM SPAM, SPAM SPAM SPAM SPAM, lovely SPAM, wonderful SPAM…" Like the song, SPAM is an endless repetition of worthless text. Another school of thought maintains that it comes from the computer group lab at the University of Southern California who gave it the name because it has many of the same characteristics as the lunchmeat spam:
>
> - Nobody wants it or ever asks for it.
> - No one ever eats it; it is the first item to be pushed to the side when eating the entree.
> - Sometimes it is actually tasty, like one percent of junk mail that is really useful to some people.[2]

Other than Hormel's Spiced Ham, there are none that apply to junk mail. How about this one: Sales-oriented Profoundly Annoying Messages (or Mail)?

Who is Spamming and Why?

One could make the argument that the precursors to spam were direct mail and door-to-door salesmen. Of the two, direct mail, which had a typical response rate of two percent at best, still generated over $31 billion in US revenue in 2002.[3] According to The Consumer Research Institute, "Americans throw away 44 percent of bulk mail unopened, yet still spend eight months per lifetime opening bulk mail."[4] While it is obvious there is much waste involved, let us not forget we live in a capitalist society, and $31 billion is a respectable percentage of the American

GNP. There are still companies that use direct mail as a method to reach existing customers and build market share, but they no doubt realize that the costs associated with direct mail are at least ten times greater than that of email. The decision seems simple – spam is superior.

Why do people and companies send spam when it is known that spam is the bane of the Internet? The driving force behind spam is the second greatest motivator – money. As the following article states taken from Spamsite.com states, a successful spammer can make upwards of six figures annually.

> **Spammer Profile**
> Predominantly male; 16 - 35 years old; Single; living in or working from home
> Technically competent (these guys are not idiots)
> Tendency to be involved in other illegal activities (e.g. credit card fraud)
> Considers his or her activities to be harmless
> Can/will work with other spammers on large campaigns
>
> **Types of Spammers**
> **Smart Spammer**
> Uses spoofing and open relays; never uses the same IP address twice
>
> **Thief Spammer**
> Sets up a webpage/portal that looks exactly like that of the company they target
> Sends out spam mail to this company's customers advising them to update their payment information or billing details
> The customer responds to this by going to the website and entering credit card details
> The spammer then uses acquired credit card details to purchase goods online
>
> **Favorite Spam Software**
> News Blast, MailBomb, Prospect Mailer
>
> **Amount of Spam**
> A single spammer can, potentially, send 84,000,000 (84 million pieces of spam per day). This is an extreme case but is possible. Ronnie Scelson boasts that he can send this much junk mail every single day via three super fast email servers.
>
> **Income potential**
> A "good" spammer can easily earn $100,000 per year. Spammers work on a piece rate so the more spam they send the higher their income potential. On average 1,000,000 pieces of junk mail sent out will result in 150 "sales" or leads. This, in turn, generally means big profits for the spammer.

> **Ronnie Scelson** is currently one of the most notorious spammers in the world. He claims to have covert agreements (sometimes referred to as pink agreements) with ISPs to allow him to send the 84,000,000 pieces of junk email per day that he claims to. Typical of spammers/virus authors, he sees nothing wrong with his "business".[5]

Spam Scope

How big is the spam problem? According to Electricnews.net article entitled "US Lawmakers lose Their Patience over Spam," a congressional hearing places current lost revenue estimates at $10 billion in the US and over $50 billion worldwide.[6] Erika Morphy reports that:

- The average employee receives nearly 7,500 spam messages per year, up from 3,500 in 2003.
- Average lost productivity per year, per employee is 3.1 percent, up from 1.4 percent in 2003.
- Companies using spam filters report that on average they are able to filter only 20 percent of the incoming spam, down from a reported 26 percent in 2003.
- The average cost of spam per year, per employee more than doubled in a year's time to US $1,934, according to the Nucleus Research report, "Spam: The Serial ROI Killer."[7]

Spam is a serious issue facing businesses and individuals alike. Enrique Salem, CEO of Brightmail, states that nearly half of all emails sent are spam. His quote is now outdated as Brightmail posts a chart on its homepage which estimates that spam now accounts for 65 percent of all email. In fact, at its current rate of growth, spam will soon represent 80 percent of all email on the Internet.[8] This compared, he said, with just seven percent in 2001. No one can argue that spam is not a serious problem facing the entire world.

Is Legislation the Answer?

How have our lawmakers answered this growing quandary? They have frustrated the masses by passing dentally challenged legislation – one after the other. These laws are anti-spam

at heart but lack any real power or teeth to instill fear in violators. There has yet to be a single landmark, well-publicized case where sizeable damages have been awarded or incarceration resulted. Both of these unpleasant outcomes have befallen programmers who have unleashed viruses on the world – and rightfully so. Until lawmakers become this aggressive with spammers, users will continue to delete the majority of the email they receive. Let's take a quick look at some, but not all, of the proposed and passed legislation of recent years.

Unenacted bills of the 106th Congress:

Unsolicited Electronic Mail Act of 2000 (H.R. 3113)

Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2000 (S. 2542)

Can Spam Act (H.R. 2162)

Email User Protection Act (H.R. 1910)

Inbox Privacy Act of 1999 (S. 759)

Internet Freedom Act (H.R. 1686)

Internet Growth and Development Act of 1999 (H.R. 1685)

Netizens Protection Act of 1999 (H.R. 3024)

Protection Against Scams on Seniors Act of 1999 (H.R. 612)

Telemarketing Fraud and Seniors Protection Act (S. 699)

Wireless Telephone Spam Protection Act (H.R. 5300)

Unenacted bills of the 107th Congress:

Anti-Spamming Act of 2001 (H.R. 718)

Anti-Spamming Act of 2001 (H.R. 1017)

Controlling the Assault of Non-Solicited Pornography and Marketing (CAN Spam) Act of 2001/2002 (S. 630)

Netizens Protection Act of 2001 (H.R. 3146)

Protect Children From Email Smut Act of 2001 (H.R. 2472)

Who Is Emailing Our Kids Act (H.R. 1846)

Unsolicited Commercial Electronic Mail Act of 2001 (H.R. 95)

Wireless Telephone Spam Protection Act (H.R. 113)

Unenacted bills of the 108th Congress:

Anti-Spam Act of 2003 (H.R. 2515)

Ban on Deceptive Unsolicited Bulk Electronic Mail Act of 2003 (S. 1052)

Computer Owners' Bill of Rights (S. 563)

Criminal Spam Act of 2003 (S. 1293)

REDUCE Spam Act of 2003 (H.R. 1933)

Reduction in Distribution of Spam Act of 2003 (H.R. 2214)

Stop Pornography and Abusive Marketing Act (S. 1231)

Wireless Telephone Spam Protection Act (H.R. 122)

Enacted legislation:

CAN-SPAM Act of 2003 (S. 877)

The Controlling the Assault of Non-Solicited Pornography and Marketing Act requires unsolicited commercial email messages to be labeled (though not by a standard method) and to include opt-out instructions and the sender's physical address. It prohibits the use of deceptive subject lines and false headers in such messages. The FTC is authorized (but not required) to establish a "do-not-email" registry. State laws that require labels on unsolicited commercial email or prohibit such messages entirely are pre-empted,

> although provisions merely addressing falsity and deception would remain in place. The CAN-SPAM Act takes effect on January 1, 2004.
>
> The CAN-SPAM Act of 2003 was introduced by Senators Conrad R. Burns (R-MT) and Ron Wyden (D-OR) in April 2003, with minor changes from the previous year's version, S. 630 (2002). Two other bills (S. 1231 and S. 1293) were subsequently merged into it. The final version was approved by the Senate in November 2003 and by the House of Representatives in December 2003, and was signed into law by President Bush on December 16, 2003.[9]

These are over 20 items of un-enacted legislation. What a monumental waste of time and taxpayers' money! The only law that successfully made it through the House and Senate is the 2003 CAN-SPAM Act S.877. It took affect on the 1st of January of this year, and there has yet to be any CNN coverage of a spam trial. Perhaps the penalty for violating this law is forfeiture of one's computer. That will surely teach those spammers to thumb their noses at Congress!

Considering that spam has continued to grow despite all of this legislation, one might think that reasonably intelligent lawmakers would have figured out one simple fact that even most children realize: the mere presence of law will never be a deterrent. It is the resulting punishment that gives potential offenders pause. The point is that until lawmakers put shark teeth into their "slap the wrist" legislation, spammers will continue to scoff at legal authority and fill our inboxes with offers of better health, greater wealth, and a longer lifespan.

Spam Solutions

Until the collective IQ of Congress reaches 1000, what are companies and individuals doing to shield themselves from the onslaught? The most drastic measure is to stop using email altogether. Possibly the most effective measure is to implement a whitelist where all emails from anyone other than persons listed are deleted at the server. Some software packages use blacklists which filter email based certain addresses, domains, and keywords. The most common alternative is to implement a software solution. Hardware solutions are available but are quite expensive and configuration is a nightmare.

There are myriad software packages available for both users and businesses that run the gamut from freeware to $10,000 server programs that monitor and filter every email coming and going. For corporations, Brightmail, recently acquired by Symantec, has distinguished itself from the pack and boasts among its clientele Bellsouth and numerous government and state agencies. I Hate Spam is an effective product and has a catchy name that well-reflects the attitude of customers. This product is free after a rebate and works seamlessly with Outlook and Outlook Express. It is approximately 99 percent accurate in positively identifying spam and not erroneously identifying desired mail as spam. There are frequent updates from the corporate server, the program is highly configurable, and it improves in accuracy as it learns the user's emailing habits.

Anti-spam filtering is a subject as deep as it is wide and cannot be covered at length here. The long and short of it is that there are different types of filtering, and no one solution is best for all users. There is Internet Based Filtering, Integrated Algorithmic Filtering, Proxy Filtering, Whitelist Filtering, Blacklist Filtering, Real Time Filtering, Domain Filtering, Pattern Filtering, and the list goes on. A common sense approach advises the home user to use a free web-based

email service like Hotmail, Yahoo, or Google (coming soon) for a public address and hand out your private email address to only friends and family. This tactic is not perfect, but will stem the tide a bit. Be sure to insist that people in your address book not include your address in their mass mailings to others.

Authentication in the form of digital certificates or stamps offers the best promise of a serious solution to the spam problem. Only those persons or entities that you have approved will be able to send you mail. Disposable email addresses are also available but present a hassle for users. Gilbert Held, editor of the International Journal of Network Management, suggests a passive approach in that we should "spam the spammer." He suggests that recipients "respond with a courteous 'No thank you – remove my name from your mailing list'."[10] However, security analysts advise recipients not to reply to spammers because this only serves as notification that our address is valid! An alternate solution involves more effort. Pawel Gburznski and Jacek Maitan describe a "remailer" system where a user's true address is masked by multiple aliases. Their scenario divides the aliases into one of three types: regular, quick, and master aliases. These would vary in use according to the situation. If an alias began to receive a lot of spam, that "appendage" is merely cut off.[11] Their approach might serve the needs of some firms, but it represents the opposite end of the spectrum in that it requires a lot of initial effort and ongoing maintenance. The solution that an individual or firm chooses to implement will ultimately depend on how serious the problem is and how much the time, money, and effort an individual or firm and is willing to spend. The most effective answer to this problem is likely to be a multi-layered approach in which more than one spam-blocking method is employed.

Success and the Cost of Failure

There is no need to focus on a single firm's losses due to spam because the spam pandemic affects practically every going concern with Internet access. Here is an excerpt from a Washington Post article:

> "Companies will lose $1,934 for every employee in 2004, compared to $874 in 2003. We found the effectiveness of spam filters and other anti-spam technologies was being rendered ineffective by the growing volume of mail. Spam currently accounts for more than 70 percent of total email volume worldwide, according to anti-spam filtering company Postini Inc."[12]

In considering success stories, many companies that won the spam battle did so with a variety of solutions rather than a single piece of hardware or software.

> Hudson Research receives between 400 and 800 emails a day, of which about 85 percent comes from China. The layers of spam protection are:
>
> - Brightmail
> - Router/hardware firewall
> - McAfee Spam-Killer
> - Symantec Software Firewall/Anti-Virus
> - Email Client
>
> By implementing a multi-layered anti-spam approach, Hudson claims to have adequately eliminated their junk mail woes.[13]

Conclusion

Thankfully, spammers seem to be moving away from pornography and are favoring health products and online gaming. What exactly the future holds for the spammers and the spammed is anyone's guess. Here is mine: regardless of culture and country, there is one unifying principal that will raise the tide against spam: money. Coincidentally, money is also the motivation for spammers to survive legislation and to somehow work around the latest software tactics. While I would like to believe that stiffer laws will mitigate the problem, any reduction would be marginal at best. It is my opinion that the Holy Grail lies with better security in the form of authentication. It involves more work up front, but the payoffs make the effort well worth it. Ideally, the Internet community will adopt an anti-spam authentication solution and have software providers integrate the authentication method into their products. This certificate would apply to Instant Messaging, Newsgroups, Web-based and POP email. If you are one of the few individuals who aren't bothered by spam, consider your level of irritation as you noticed the word spam, repeated over and over throughout this essay. Perhaps in truth, spam is more annoying than you are willing to admit.

Spam Resources

If you are interested in some aspect of spam not covered here, the following excellent website contains a number of essays on spam: http://www.templetons.com/brad/spam/

Recommended Software for Individuals: I Hate Spam

Recommended for mid-sized to large companies: Brightmail.

Alternate source of software solutions: TUCOWS. http://www.tucows.com/SPAM95.html

For a summary of all US State Laws: http://www.SPAMlaws.com/state/summary.html

For a summary of all European Laws: http://www.SPAMlaws.com/eu.html

For a summary of Spam Laws in other countries: http://www.spamlaws.com/world.html

References and Citations

[1] Joanna Glasner, May 26, 2001. "A Brief History of Spam and spam": Wired News. Retrieved from http://www.wired.com/news/business/0,1367,44111,00.html

[2] Retrieved from http://www.webopedia.com/TERM/s/spam.html

[3] Retrieved from http://www.euromonitor.com/Direct_marketing_in_USA_(mmp)

[4] Retrieved from http://www.newdream.org/junkmail/facts.html

[5] Retrieved from http://www.spam-site.com/profile_of_spammer.shtml

[6] Electricnews.net, May 24, 2003
Retrieved from http://www.theregister.co.uk/2003/05/24/us_lawmakers_lose_patience_over/

[7] Erika Murphy, June 10, 2004. "Spam Costing Businesses Big Bucks". Newsfactor Network
Retrieved from http://www.newsfactor.com/perl/story/24523.html

[8] Retrieved from http://www.brightmail.com/spamstats.html

[9] Retrieved from http://www.spamlaws.com/

[10] Gilbert Held, March 1998, "Spam the Spammers". International Journal of Network Management
Volume 8 Issue 2.

[11] Pawel Gburznski and Jacek Maitan, February 2004, "Fighting the spam wars: A remailer approach with restrictive aliasing". Transactions on Internet Technology Journal. Volume 4 Issue 1

[12] David McGuire, June 7, 2004, "Spam Costs are Rising at Work". WashingtonPost.com
Retrieved from http://www.washingtonpost.com/wp-dyn/articles/A21657-2004Jun7.html

[13] Staff Writers, December 9. 2003, "Case Study: An SME's Spam Success Story", TechRepublic
Retrieved from http://www.zdnet.com.au/insight/0,39023731,20281745,00.htm