INFORMATION CAPSULE
Research Services

Vol. 0814
February 2009

Christie Blazer, Supervisor

SPAM:
A Growing Problem for E-Mail Communication

At a Glance

Approximately 75 to 90 billion spam emails are sent worldwide every day. This Information Capsule discusses spam's negative impact on organizations and how email users can reduce the volume of spam they receive. A brief description of Miami-Dade County Public Schools' (M-DCPS) anti-spam applications is provided. With the district receiving almost one million incoming spam messages per week, these applications and Information Technology Services' maintenance of the systems save M-DCPS over $12 million per year.

Trillions of emails are sent worldwide each day. About 75 to 90 billion of these messages, or 67 to 90 percent of all emails sent, are spam. Experts estimate that the average computer user receives anywhere from 10 to 116 spam messages every day (Aykac, 2008; Business Wire, 2008; Callow, 2008; The Computer Technology Industry Association, 2008; Gudkova, 2008; MessageLabs, 2008; ProtectWebForm, 2008; Websense Security Labs, 2008; Webroot, 2008; Liyakasa, 2007; Symantec, 2007; Walsh, 2007).

Spam is defined as unsolicited and unwanted email messages sent to an indiscriminate set of recipients, or the electronic equivalent of junk mail (Ralla, 2008; Wikipedia, 2008; Center for Democracy & Technology, 2003; Krevy, 2002). It is widely believed that the term spam originated from a 1970 *Monty Python's Flying Circus* sketch, set in a café where almost every item on the menu included SPAM lunch meat. The word came to represent something that is repeated to great annoyance. It became part of the electronic world's vocabulary through chat rooms. When a new chat room member tried to monopolize the conversation, the existing members would type lines from the *Monty Python* skit ("spam, spam, spam"). The term eventually came to mean excessive multiple postings of the same message (Dee, 2007).

Spam can be used to sell goods or services, advertise money-making schemes, solicit opinions, or advertise web sites. The most frequently sent spam messages are advertisements for medications and health-related goods and services; adult products; financial opportunities, such as pre-approved loans and credit card applications; and travel and leisure opportunities, such as vacation offers and online casinos (Business Wire, 2008; Gudkova, 2008; ProtectWebForm, 2008; Websense Security Labs, 2008; Market Wire, 2006; Krevy, 2002). According to Symantec's (2007) *State of Spam* report, approximately 13 percent of spam promotes some type of scam or fraud. Most analyses have found, however, that less than one percent of spam messages contain viruses that take control of computers or implant software to gather personal information (MessageLabs, 2008; Websense Security Labs, 2008).

Research Services
Office of Assessment, Research, and Data Analysis
1500 Biscayne Boulevard, Suite 225, Miami, Florida 33132
(305) 995-7503 Fax (305) 995-7521

Security outfits that monitor spam traffic have concluded that the U.S. and China relay more spam than other countries, accounting for approximately one-fourth of all global spam (BBC News, 2008; Help Net Security, 2008; ProtectWebForm, 2008; Sophos, 2007). Although the U.S. relayed more spam than any other country during the last two years, Winder (2008) reported that November 2008 statistics indicated China may now be producing more spam than the U.S.

How Spammers Benefit

Email is a very inexpensive mass medium and professional spammers have automated their processes so that millions of messages can be sent with little or no labor costs (Schirmer, 2005). Andad (2008a) reported that a large spam outfit needs only one response to every 12.5 million spams sent in order to make a profit. Kanich and colleagues (2008) conducted an analysis of a major spam campaign and found that over the course of 26 days, only 28 sales resulted from 350 million email messages. However, with an average purchase price of close to $100, the researchers extrapolated that spam advertising the company's product would produce approximately $3.5 million of revenue in one year, not including repeat business.

A spammer, convicted in 2004, sent 10 million spam emails per day as part of a fraudulent money-making scheme. Only about .003 percent of messages resulted in a sale, but the spammer, who earned $40 per sale, grossed between $400,000 and $700,000 per month, with only about $50,000 in overhead expenses (Schirmer, 2005).

Evett (2007) reported that 28 percent of computer users reply to spam email and eight percent purchase a product or service from spam email. A survey conducted by the University of Maryland and Rockbridge Associates found that 14 percent of online adults reported reading the spam they received and four percent stated they had purchased a product or service advertised in spam during the previous year (Claburn, 2005).

The High Cost of Spam

Spam has a significant financial impact on corporations and organizations. Callow (2008) reported that spam cost businesses over $100 billion in 2007. Costs associated with spam include:

- **Lost worker productivity.** Researchers have estimated that spam costs U.S. businesses $70 billion annually in lost worker productivity alone (Business Wire, 2008; The Computer Technology Industry Association, 2008). Employees spend the equivalent of two full working days every year sorting, downloading, reviewing, and deleting unwanted spam messages (Jelveh, 2008; Knight, 2008; ProtectWebForm, 2008).

- **Anti-spam technology.** Most organizations spend thousands of dollars on anti-spam software and hardware solutions, in addition to monies spent on the manpower needed to plan, deploy, and maintain the technology systems (The Computer Technology Industry Association, 2008; Knight, 2008).

- **Wasted storage.** Spam drains network resources and consumes significant amounts of bandwidth and disk storage space, which reduces processing speed and results in decreased systems performance (Callow, 2008; Ispwitch Imail Server, 2008; Knight, 2008; Greencomputer Innovation, n.d.).

- **Security breaches.** When systems become infected by malicious software (malware), organizations must pay for expensive clean-up operations (Andad, 2008b; Callow, 2008). Webroot (2008) conducted a survey of 1,500 email security product decision-makers in companies across seven countries, including the U.S. They reported that approximately one in five organizations reported sensitive online transactions had been threatened and confidential information had been compromised as a result of spam.

- **Intangible costs.** Knight (2008) stated that spam also has a broader economic impact on society. He cited the case of Nigeria as an

example. Because of the volume of deceptive email sent by Nigerian spammers, most spam filters block any mail with the word "Nigeria" in the title or text, preventing almost all email users worldwide from communicating with anyone from Nigeria or about Nigeria.

Spam Filters

Organizations can reduce the number of spam messages they receive by installing anti-spam filters (Aykac, 2008; Help Net Security, 2008; Center for Democracy & Technology, 2003; Evett, n.d.; Greencomputer Innovation, n.d.). Spam filters decide whether incoming messages are legitimate or spam. They use a variety of techniques to catch spam before it is delivered to users' email accounts, including word lists (lists of words that are known to be associated with spam); black and white lists (lists containing known addresses of spam and non-spam senders); and probabilistic systems (systems that learn word frequencies associated with both spam and legitimate messages) (Andad, 2008b; Karlberger et al., 2007).

BBC News (2008) reported on a study conducted by security firm McAfee. The firm asked 50 people from around the world to surf the Web without spam filters for one month. The researchers concluded that the average computer user surfing the Web unprotected would receive 70 spam messages per day.

The effectiveness of anti-spam filters varies and no perfect spam filter exists. Therefore, although most organizations use some spam filtering technology, it has not completely solved the spam problem. Experts have stated that until anti-spam filters are capable of blocking all spam and allowing all legitimate email to pass through with 100 percent accuracy, they will never be totally effective (Business Wire, 2008; Clapperton, 2008; Karlberger et al., 2007; Schirmer, 2005; Evett, n.d.).

It should be noted that several security companies have cautioned against overly aggressive filtering approaches. False positives (when a legitimate message is mistakenly identified as spam and blocked) can have an adverse effect on productivity (Clapperton, 2008; The Computer Technology Industry Association, 2008). Brockmann (2007) reported that 36 percent of organizations suffered lost productivity because legitimate emails were caught in spam filters.

Additional Ways to Reduce Spam

In addition to using spam filters, experts have suggested additional ways computer users can reduce the volume of spam they receive (The Computer Technology Industry Association, 2008; Schirmer, 2005; Center for Democracy & Technology, 2003; Evett, n.d.).

- Don't open spam. When spam is opened, the computer informs the spammer that the email address is in use.

- Don't reply to spam. When users reply to a spam email, they confirm the legitimacy of the email address to the spammer. Users should never opt out of future spam emails. A study conducted by Schirmer (2005) found that computer users who opted out received three times more spam than those who never responded.

- Guard email addresses. Once an email address has been posted on a website (personal or professional) or entered into an online guest book, news group, contact list, or anywhere online, it is an invitation for spammers to take the address. Spammers' programs continually search the Web for email addresses to be used in future campaigns.

- Use false email addresses. On Web sites that require an email address before a user can proceed through the site, enter a false address.

- Encrypt email addresses. Use a combination of letters and numbers that are inconvenient to remember but make it less likely a spammer's program will randomly send emails to the address. For example, choose "s18all56y" instead of "sally1" or "sallysmith."

- Use longer email addresses. Spam is more likely to be directed to shorter addresses ("bob2") before it is directed to longer addresses ("robertwilliams2").

On a Local Note

M-DCPS' Information Technology Services (ITS) maintains approximately 50,000 email addresses. Two different applications are used to block spam from infiltrating the system. The first application, Fortiguard Antispam Service, provides automatic updates to reduce the amount of spam at the network perimeter, using technology to identify, tag, and block spam messages. The Fortiguard service uses a multi-layer approach and a number of filtering techniques to detect spam. Once Fortiguard has determined that emails are clean, they are passed into the district's email server and then the Sophos PureMessage system is activated. This application protects against new or unknown email borne threats missed by Fortiguard, using virus detection files and hourly spam rule updates.

M-DCPS anti-filter systems block close to one million spam messages each week. ITS data indicate that during an average week in November 2008, more incoming messages were classified as spam than legitimate email. District email accounts received a weekly average of 990,282 (54 percent) spams and 841,602 (46 percent) clean email messages. In addition, an average of 104 blocked email messages per week were considered viral. M-DCPS accounts also received a weekly average of 25,075 suspected spam emails. Therefore, 1.4 percent of incoming email messages were suspected of being spam but allowed into the district's server. As previously discussed in this report, when email is filtered too aggressively, it can have an adverse impact on worker productivity, requiring employees to spend time searching for legitimate emails caught in spam filters.

Netriplex, a company that offers anti-spam applications, provides an online spam calculator on their web site (www.netriplex.com/solutions/spam/roi.aspx). Data input into the spam calculator by ITS staff estimated that without the use of the Fortiguard or Sophos anti-spam services, spam would cost M-DCPS over $12 million dollars per year. This figure included the cost of lost employee productivity, bandwidth costs, storage costs, and support costs.

Spam volume was also reduced in 2008 when ITS staff deactivated the email addresses of former district employees. Email addresses had previously remained active even after employees left their positions at M-DCPS, in case they returned to work in the district.

In conclusion, district anti-spam applications and ITS employees are saving M-DCPS millions of dollars each year by reducing the volume of spam received in the district. M-DCPS employees receive almost one million fewer spam messages each week because of the district's anti-spam applications and ITS staff's maintenance and monitoring of the systems. The next time you open Microsoft Outlook and have 20 new email messages, two of which are spam, remember that without the systems currently in place, you would have 40 new emails, 20 of which could be spam.

Summary

Between 75 and 90 billion spam emails are sent worldwide every day. Large spam outfits need only one response for every 12.5 million spams they send in order to make a profit. Spam has a negative impact on organizations, including the costs of lost worker productivity and anti-spam technology, wasted storage space, and security breaches. Organizations can reduce the number of spam messages they receive by installing anti-spam filters, although no perfect filter system exists. Experts have suggested additional ways computer users can reduce the volume of spam they receive, such as carefully guarding email addresses and remembering not to open or reply to spam. A brief description of M-DCPS' anti-spam applications was also provided in this report. With the district receiving almost one million incoming spam messages per week, these applications and ITS' maintenance of the systems save M-DCPS over $12 million per year.

References

Andad, B. (2008a). *DaniWeb IT Discussion Community.* Retrieved from http://www.daniweb.com/blogs/printentry3506.html.

Andad, B. (2008b). *DaniWeb IT Discussion Community.* Retrieved from http://www.daniweb.com/blogs/printentry1902.html.

Aykac, M. (2008). *Spams and Their Filtering Techniques.* Retrieved from http://www.articlesbase.com/spam-articles/spams-and-their-filtering-techniques-603096.html.

BBC News. (2008). *Spam Experiment Overloads Inboxes.* Retrieved from http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/1/hi/technology/7482991.stm.

Brockmann, P. (2007). *The Problem With Email.* Retrieved from http://www.brockmann.com/index.php/20070501508/abstracts/messaging-research/the-problem-with-email.html.

Business Wire. (2008). *Nucleus Research: Spam Costing US Businesses $712 Per Employee Each Year.* Retrieved from http://www.businesswire.com/news/google/20070402005669/en.

Callow, B. (2008). *The Business Cost of Spam.* Retrieved from http://www.brighthub.com/computing/smb-security/articles/5732.aspx.

Center for Democracy & Technology. (2003). *Why Am I Getting All This Spam? Unsolicited Commercial E-Mail Research Six Month Report.* Retrieved from http://www.cdt.org/speech/spam/030319spamreport.shtml.

Claburn, T. (2005). Spam Costs Billions. *Information Week.* Retrieved from http://www.informationweek.com/shared/printableArticle.jhtml?articleID=59300834.

Clapperon, G. (2008). *DaniWeb IT Discussion Community.* Retrieved from http://www.daniweb.com/blogs/printentry3300.html.

The Computer Technology Industry Association. (2008). *How Much Does Spam Cost Business?* Retrieved from http://www.focusonmsp.com/articles/200800819-2.aspx.

Dee, R. (2007). The REAL Origins and Meaning of the Word SPAM. *Ezine Articles.* Retrieved from http://ezinemarticles.com/?The-REAL-Origins-and-Meaning-of-the-Word-SPAM&id=430328.

Evett, D. (2007). *Spam Statistics 2006.* Retrieved from http://spam-filter-review.toptenreviews.com/spam-statistics.html.

Evett, D. (n.d.). *Spam Safety Tips.* Retrieved from http://spam-filter-review.topttenreviews.com/spam-safety-tips.html.

Greencomputer Innovation. (n.d.). *The High Cost of Spam on Business.* Retrieved from http://powerelf-server-appliance.greencomputer.com/solutions/cost-of-spam.shtml.

Gudkova, D. (2008). *Spam Evolution: September 2008.* Retrieved from http://www.viruslist.com/en/analysis?pubid=204792038.

Help Net Security. (2008). *Latest Spam Statistics.* Retrieved from http://www.net-security.org/secworld.php?id=6056.

Ipswitch IMail Server. (2008). *How Much Does Spam Cost Your Enterprise?* Retrieved from http://blogs.imailserver.com/2008/09/03/how-much-does-spam-cost-your-enterprise.

Jelveh, Z. (2008). The Cost of Spam. *Condé Nast Portfolio.* Retrieved from http://www.portfolio.com/views/blogs/odd-numbers/2008/10/20/the-cost-of-spam.

Kanich, C., Kreibich, C., Levchenko, K., Enright, B., Voelker, G.M., & Paxon, V., et al. (2008). *Spamalytics: An Empirical Analysis of Spam Marketing Conversion.* Paper presented at the Conference on Computer and Communications Security, Alexandria, VA, October 2008.

Karlberger, C., Bayler, G., Kruegel, C., & Kirda, E. (2007). *Exploiting Redundancy in Natural Language to Penetrate Bayesian Spam Filters.* Proceedings of the first USENIX Workshop on Offensive Technologies, Boston, MA, August 2007.

Knight, M. (2008). *DaniWeb IT Discussion Community.* Retrieved from http://www.daniweb.com/blogs/printentry2149.html.

Krevy, J. (2002). Spam: Electronic Junk Mail. *LRDC Computing Services.* Retrieved from http://www.lrdc.pitt.edu/compserv/News/Articles/Spam-Electronic Junk Mail.htm.

Liyakasa, K. (2007). *Spam Statistics.* Retrieved from http://us.deskdemon.com/pages/us/techcenter/spamstatistics.

Market Wire. (2006). *February Virus and Spam Statistics: Swift Virus Attacks Continue to Gain the Upper Hand.* Retrieved from http://newsblaze.com/story/20060320172732000001.mwire/topsstory.html.

MessageLabs. (2008). *Message Labs Intelligence: 2008 Annual Security Report.* Retrieved from http://www.messagelabs.com/intelligence.aspx.

ProtectWebForm. (2008). *Anti Spam News.* Retrieved from http://blog.protectwebform.com/p/category/statistics.

Ralla, N. (2008). *Some Internet Marketing Tips With What Exactly is Spamming?* Retrieved from http://www.articlesbase.com/spam-articles/some-internet-marketing-tips-with-what-exactly-is-spamming-607073.html.

Schirmer, M. (2005). A Year of CAN-SPAM, a Year of More Spam. *Foresight, 43.* Retrieved from http://www.kltprc.net/foresight/Chpt_81.htm.

Sophos. (2007). *Security Threat Report, Update 7/2007.* Retrieved from http://www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-threats-update-2007_wsrus.pdf.

Symantec. (2007). *The State of Spam: A Monthly Report - August 2007.* Retrieved from http://www.symantec.com/avcenter/reference/symantec_Spam_Report_-_August_2007.pdf.

Walsh, S. (2007). *2007 Spam Trends.* Retrieved from http://www.igotspam.com/50226711/2007_spam_trends.php.

Webroot. (2008). *The State of Internet Security.* Retrieved from http://www.webroot.com/En_US/land-sois-home.html.

Websense Security Labs. (2008). *State of Internet Security Q1 - Q2, 2008.* Retrieved from http://www.websense.com/securitylabs/docs/WSL_Report_1H08_FINAL.pdf.

Wikipedia. (2008). *Spam (Electronic).* Retrieved from http://en.wikipedia.org/Spam_(electronic).

Winder, D. (2008). *DaniWeb IT Discussion Community.* Retrieved from http://www.daniweb.com/blogs/printentry3565.html.