Global Information Assurance Certification Paper

GIAC GSEC Practicum, v1.4b
James E. King
May, 2003

Unsolicited Electronic Mail (SPAM) – a SysAdmin's Perspective

---

SPAM is a significant distraction in time and financial resources[1] for today's System Administrators. In addition to being on the firing line in dealing with this major annoyance and potential security threat, System Administrator's also bear the brunt of end-user complaints.

This document will define SPAM, provide insight on how SPAM is generated and received, provide statistics on the quantity of SPAM received, indicate what can be done to reduce the flow and provide specific recommendations for educating your organization.

What is SPAM?

SPAM is a term used to define the sending and receipt of unsolicited, usually unwanted electronic mail message(s) to a single e-mail address, or more commonly, to thousands of addresses simultaneously. Typically, these unsolicited messages contain advertisements, referrals to pornographic web sites or attempts by scam artists to swindle potential victims.

How is Unsolicited Electronic Mail generated and received?

With special software, spammers can generate millions of e-mail messages using brute-force, or a combination of letters and numbers tied to a specific domain name (@mycompany.com); enough random addresses are generated that many match real e-mail accounts. In most situation, though, brute-force or random address generation is not required, and most SPAM originates from address harvesting.

Address harvesting is the process by which spammers gather e-mail addresses from multiple sources including web sites, publicly sold address lists, Internet yellow/white pages, newsgroups, chat rooms, domain name registrars, and mailing lists. In addition to the techniques just mentioned, some web sites can manipulate your browser into revealing your e-mail address as you visit specific web sites. Some browsers give your e-mail address to every site you visit. To determine if browsers in your organization are vulnerable, visit: http://www.privacy.net/analyze.[2]

Once the spammer has a list of addresses, the next step is to automate the sending to all those addresses, this is accomplished by using one or a combination of several methods:

SMTP Server Hijacking: In this scenario, the spammer uses a legitimate, unprotected mail server to relay the unsolicited message(s) to thousands or millions of addresses. Using others mail servers without permission may soon be illegal if government agencies pass SPAM oriented legislation (see below), but for now this is a routinely used tactic.

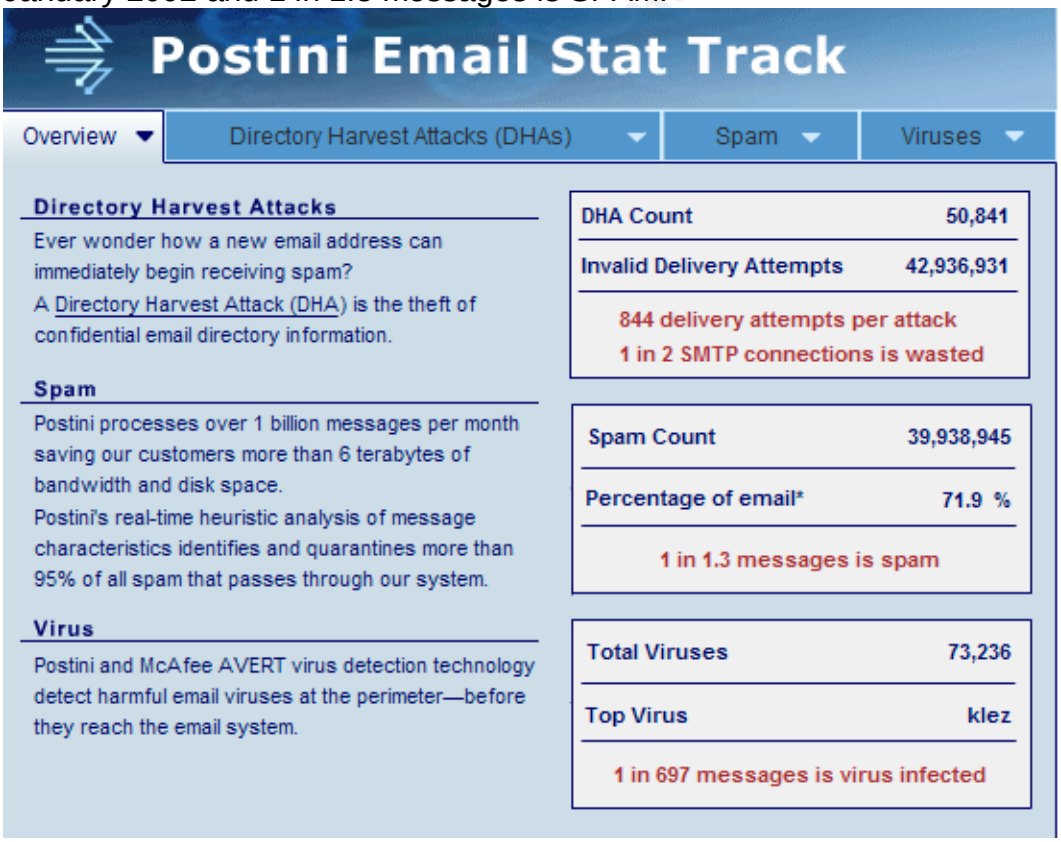
Bulk email service: In this scenario, companies offer mailing lists and servers for purchase with addresses that can't be traced back to the spammer.

How much SPAM is there?

On an average week, a typical 500 employee company receives 22000 unsolicited, unwanted messages. In addition, an average company processes over 6000 messages per day containing content that is filtered or restricted (improper language, sexually explicit material, etc).

Generally, statistics indicate that upwards of 75-85% of all mail messages are unsolicited bulk e-mail (SPAM).

According to Postini Email Stat Track, SPAM activity has increased over 65% since January 2002 and 1 in 1.3 messages is SPAM.[3]



What can be done to control SPAM?

Most companies leverage one or more technologies to reduce the amount of unsolicited or restricted electronic mail. The technologies employed reside at the server, desktop and procedural level.

Technology:

These solutions provide fields for specific keywords and domain names, and filter all in- and/or-outbound messages based on specific, manually defined rules and parameters. Since these devices require human intervention in the form of rule updates and new keyword entries, these devices must be used in conjunction with other resources.

Current devices available to assist in the filtering process include (note, prices are retail/street):

McAfee e250/e500 appliance - $15,000 for 500 users
BSD Unix based appliance, provides for antivirus and spam filters. Requires manual input via browser for configuration.

"The McAfee WebShield appliances are integrated solutions, combining award-winning anti-virus and content management software with enhanced hardware. Tuned for performance, the WebShield e250, e500 and e1000 appliances offer award winning McAfee anti-virus protection that quickly resolves your major business security worries. All of the appliances scan e-mail traffic (SMTP), web traffic (HTTP), file transfers (FTP) and dial up mail traffic (POP3)."[4]

CipherTrust Ironmail - $15,500 for 500 users
Appliance based device, recently reviewed and awarded in PC Magazine[5], combines email security and spam filtering in a single solution.

According to CipherTrust, "It is the only product capable of providing several layers of defense including a secure platform, unified email policy enforcement to deal with all types of email threats, including viruses, hackers, worms, intruders, spam, libelous content and offer secure delivery of email, including web mail."[6]

Alladin eSafe - $13,000 for 500 users
Multi-function Linux based appliance that provides for anti-virus, SPAM, HTTP and FTP filtering.

According to Alladin: "eSafe Appliance is a single purpose device incorporating eSafe's proactive content security technologies. By easily fitting into any existing security infrastructure, high-quality corporate content security can be deployed in no time and at affordable cost."

Brightmail Anti-Spam - $5-15 per user
Intel server based software that provides SPAM filtering and integration with Brightmail's BLOC service. This solution requires the least amount of administrative overhead, as it's almost fire-and-forget.

According to Brightmail: "Brightmail Anti-Spam is a high performance software solution that blocks spam at the Internet gateway. Combining several patented techniques, Brightmail Anti-Spam offers the industry's leading accuracy and effectiveness with the lowest administration costs of any anti-spam solution."

Postini Perimeter Manager - $17 per user
Hosted service with web-based administration and the ability to delegate updating of filters to both technical administrators and standard end-users.

According to Postini: "Postini can be deployed in less than a week, with no software, hardware or ongoing maintenance. Updates are deployed automatically, with no support required or additional costs."

Messagelabs Skyscan AS - $102 per year for 10 users
Simple to use hosted service for SPAM detection and elimination. Messagelabs also integrates with RBL's for added filtering capability.

According to Messagelabs: "Email security is not just about installing software at server the and PC level. These solutions are only effective only once a threat is known. By that time the damage can already have been done. Above all they offer no protection against fast-breaking or dynamic threats. They also require an investment in hardware or software, are difficult to manage and require additional administrative support. The most effective solution is one that sits outside your network and can eliminate email threats, both inbound and outbound, *outside* the boundaries of your network and *before* they reach you."

Anti-Spam Products Comparison

Product	Type A=Appliance S=Software H=Hosted	Cost per 500 User	SPAM	Anti-virus	Secure	HTTP	FTP	Admin Overhead H=High, M=Med, L=Low	Rating 1=Low 2=Med 3=High
McAfee e500	A	$15,000.00	X	X	X	X	X	H	2
Ciphertrust Ironmail	A	$15,500.00	X	X	X	X	X	M	3
Alladin eSafe	A	$13,000.00	X	X	X	X	X	L	3
Brightmail Anti-Spam	S	$11,500.00	X					L	2
Postini Perimeter Manager	H	$ 8,500.00	X					L	2
Messagelabs Skyscan AS	H	$ 5,100.00	X					L	1

Anti-SPAM clearinghouse / RBL:

An RBL (Real-time Blackhole Lists) is typically a 3rd party subscription service that compiles lists of domain names and/or email addresses that are known or suspected spammers. This service can interact with content filtering to reduce the total number of unwanted inbound messages.

Be advised that using an RBL can and does periodically cause valid messages to become filtered and/or rejected. In addition, RBL's are fairly easy to circumvent, by obtaining a new e-mail address and/or domain name.

RBL Options include:

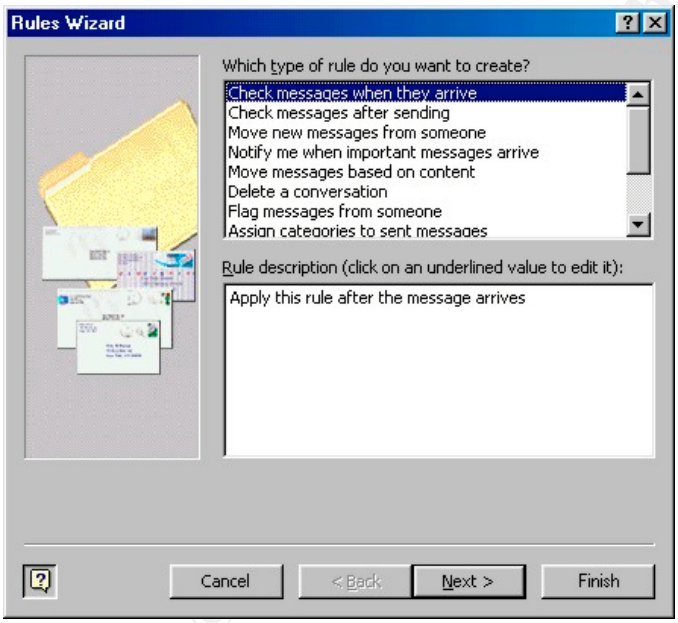
MAPS RBL
ORBS RBL
ORBL RBL
Spamhaus

To check most known RBL's for blocked servers by IP address, access http://rbls.org/

E-mail client based rules / filters:

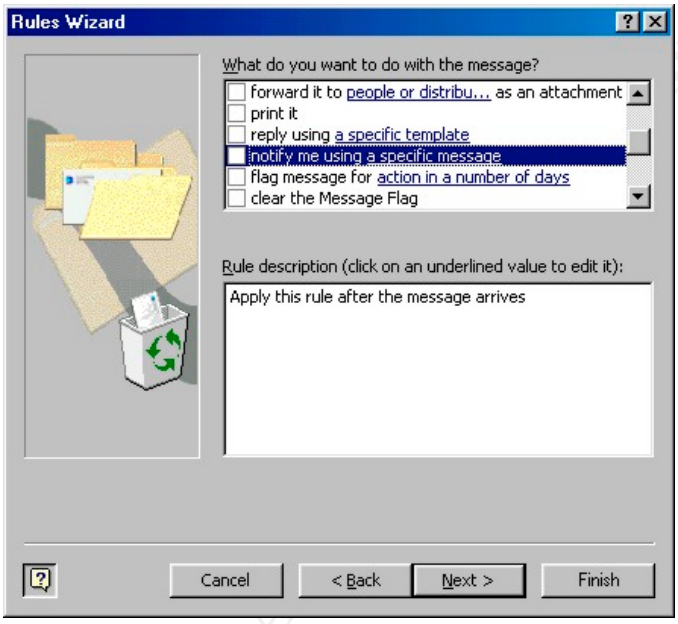
Most electronic mail clients provide for localized filtering and rules based on keywords, addresses and other criteria. While not widely used, enhanced filtering can be achieved by leveraging the rule facility within most e-mail clients. Examples for specific email clients include:

Microsoft Outlook:



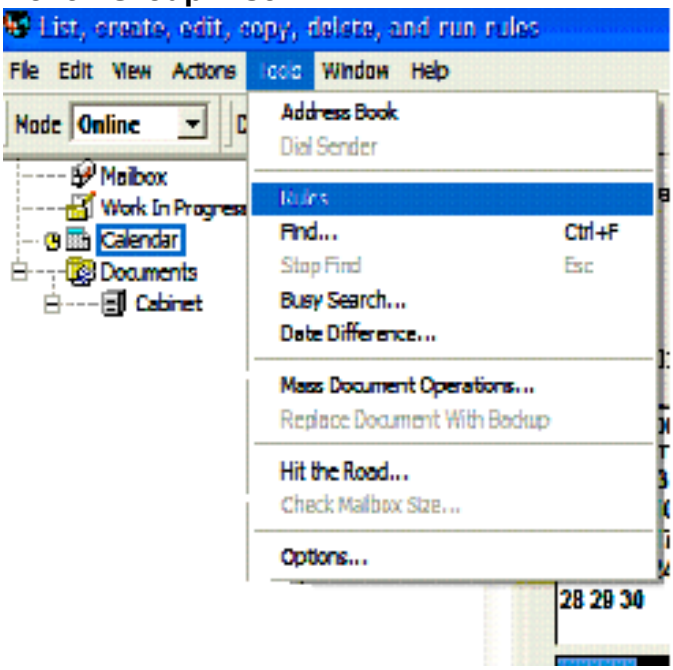
Select Tools, Rules Wizard

Select “with specific words in the subject”

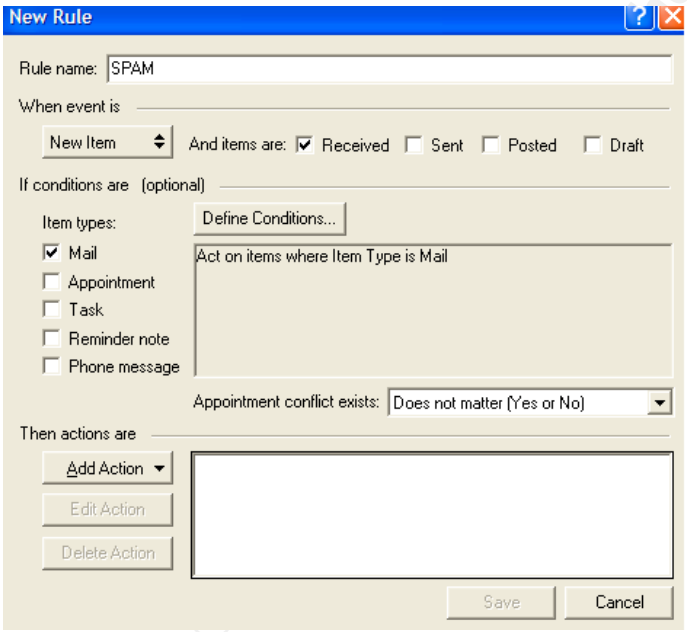


Select Action to perform (usually delete)

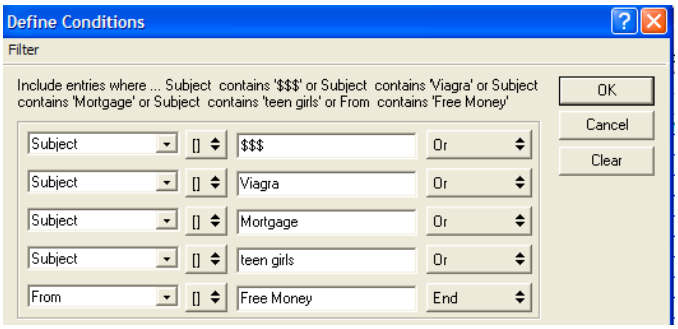
Novell GroupWise:



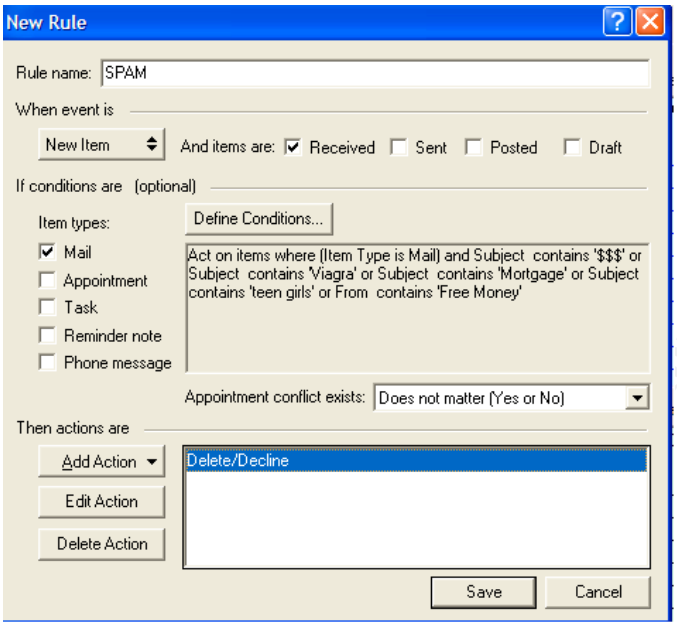
Select Tools, Rules



Name Rule, Select Mail



Define Rule, Select Subject and insert key words or phrases



Add Action, Delete.

Procedural:

While most companies do not yet have a policy approved or in circulation, implementing and deployment a policy is another option. This management supported and sponsored policy, when used in conjunction with technical solutions, can assist in reducing exposure to unwanted electronic mail.

Consider adding the following verbiage to any organizational sponsored policy.

- Generally, all electronic and telephone communication systems are to be used primarily for business purposes. However, associates may use the e-mail system for limited personal use from time to time as long as it does not interfere with job performance or interfere with or threaten the security or operation of, the Company's communication system, and does not transmit or discuss the Company's confidential information.

- E-mail and voice-mail messages reflect the Company image. They should be composed in a professional manner using the same care used to draft letters and formal memoranda. Messages should not contain material that might embarrass the Company, its personnel, or its customers, that might damage the reputation or good name of the Company or that is otherwise contrary to the Company's best interests. It is important to recognize that associates using the Company's communication system may be viewed by third parties as "representatives" of the Company, and so associates should exercise discretion and act so as to present the Company in a positive manner at all times. Also, Associates should keep in mind that electronic files are subject to discovery and may subsequently be used in litigation involving the Company or the associate.

- All messages must be consistent with the company's policies and procedures of ethical conduct, safety, compliance with laws, and proper business practices. It is a violation of this policy to use the Company communications systems for any prohibited use such as e-mail content, electronic or voice communications or Internet access that involves pornographic, obscene, sexually related, profane, derogatory, false, malicious, threatening, harassing, defamatory, or offensive material, images or language.

- No e-mail content, electronic or voice communications or Internet access that violates or may be construed to violate any Company policy or any federal, state and/or local laws, regulations or standards, including those relating to pornography, harassment, discrimination, defamation, copyright infringement, security and privacy rights, solicitation, and/or statues relating to electronic media~~.~~, are permitted.

- No electronic or voice communication messages may be created or sent that constitute intimidating, hostile or offensive material on the basis of race, color, creed, religion, national origin, age, sex, marital status, lawful alien status, physical or mental disability, veteran status, sexual orientation, or any other basis prohibited by law.

- The Company's e-mail system may at no time be used to transmit bulk "junk mail," chain letters, pyramid schemes or anything that would constitute "spamming" or which is likely to cause network congestion, or to transmit any messages that violate any Company policy or any applicable local, state or federal law.

- Receiving or downloading, or sending or uploading of Company proprietary information is prohibited without prior authorization. Such information includes copyrighted materials, trademarked materials, trade secrets (such as customer lists, pricing information, etc.), proprietary financial information, or similar materials. Also prohibited is using Company's systems to gain unauthorized access to remote computers or other systems, damage, alter, or disrupt remote computers or systems in any way, using or disclosing - without authorization -

someone else's code or password; enabling unauthorized third parties to have access to or use of Company's systems; or otherwise jeopardizing the security of Company's systems.

Legal:

- If your business is in Virginia, a law has been enacted that would impose felony violations against companies convicted of sending messages by fraudulent means. [7]

- Senator Charles Schumer of New York recently introduced a federal bill designed to impose criminal penalties on sender's that repetitively generate unsolicited mail. In addition, another federal bill is pending called the "Reduce Spam act of 2003", in which deceptive subjects and illicit advertisements would be banned by federal statute.[8]

- In several states, and in California, legislation has passed that requires unsolicited mail to contain "ADV" or "ADV: Adult" in the subject field[9]. Violations of this legislation would require financial remuneration or jail time for violations.

- Major corporations are routinely litigating and winning lawsuits related to SPAM, address harvesting and email identity theft. Specifically, eBay recently was awarded $1.2 million from ReverseAuction.com for harvesting eBay addresses, then Spamming those eBay members. In addition, Microsoft and AOL are routinely litigating those that fraudulently target or misrepresent those firms' electronic mail systems or addresses.

Suggestions for avoiding or reducing unsolicited/unwanted electronic mail

- Do not use your name@mycompany.com email address to register at any non-business oriented web sites. Instead, get an @yahoo.com, or other free email based address for these requirements, or when posting your e-mail address to a message board or news group, use "bobs at mycompany dot com" instead of bobs@mycompany.com.

- Never reply to spam or send a return email requesting to be removed from a non-reputable mailing list. In most cases, this will confirm your live email account and will actually increase the amount of unwanted email messages you receive.

- Implement, distribute and maintain corporate policies defining "Acceptable Use", SPAM/Virus avoidance procedures and processes for dealing with unwanted/unsolicited electronic mail.

- Avoid using profanity in outbound electronic mail messages. In addition, attempt to minimize the potential for receiving electronic mail containing profanity.

Messages containing profanity will trigger filtering rules, which would subject the message(s) to quarantine and/or deletion.

- Ensure that all SMTP servers are secured and appropriate access controls are in place to validate that each mail server can't be used as an open relay.[11]

Consolidated Approach:

Although the complete elimination of SPAM is unlikely, layering an approach to defend against SPAM is possible. To implement the strongest defense possible, consider layering as many of the ideas suggested so far, to include:

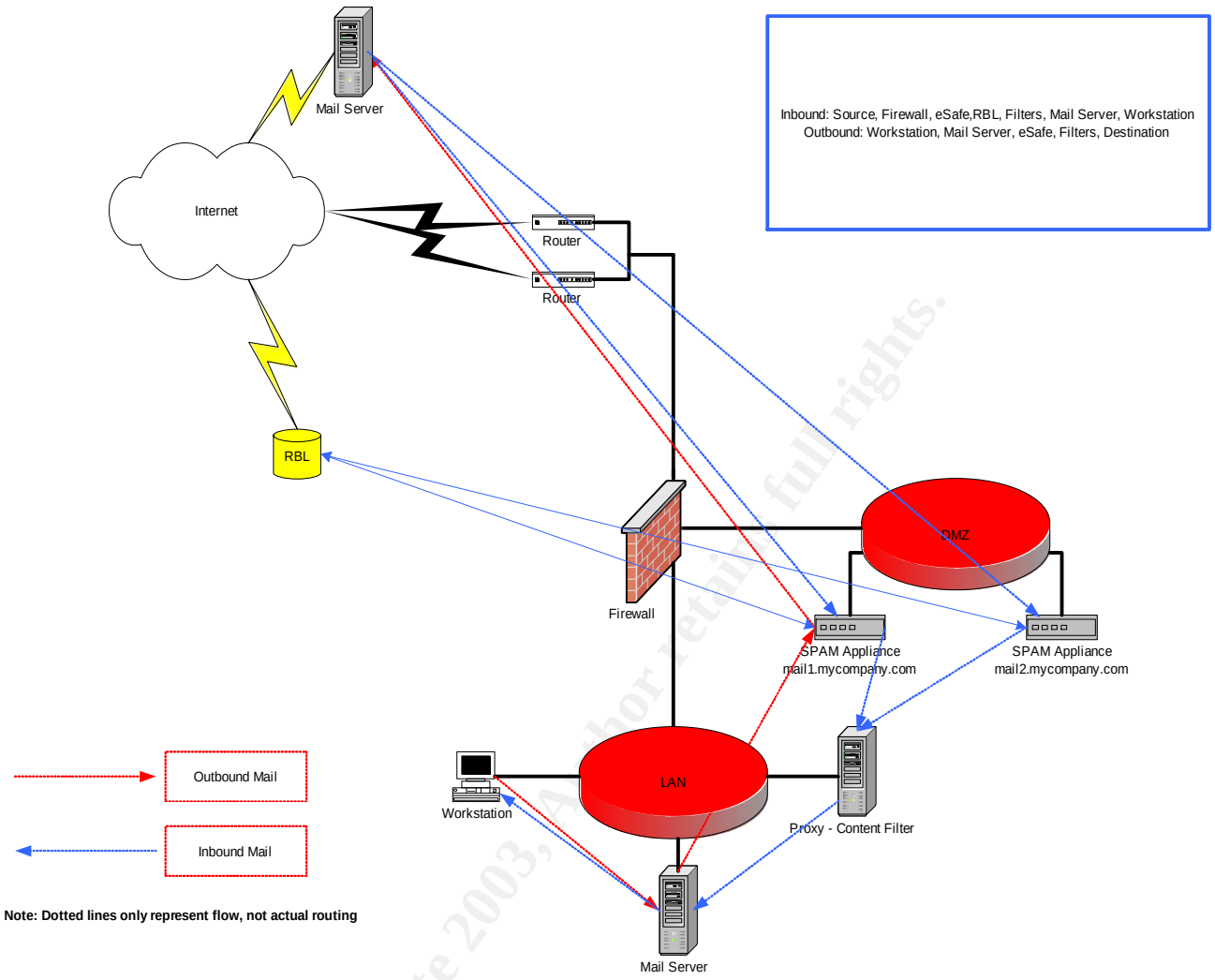
- Secured mail servers, to ensure your servers aren't used as open relays or leveraged for address harvesting.

- SPAM/Anti-virus Appliance or software with RBL's and keywords (filtered criteria) defined and procedures for maintaining/updating the technology.

- Policies regarding electronic communication distributed to associates and business partners.

- End-user education sessions specific to appropriate use of technology and SPAM avoidance.

Referenced is a diagram depicting the potential flow of electronic mail for both inbound and outbound recipients.



In conclusion, combating SPAM is a layered approach. From a System Administration perspective, associate education, combined with technical mechanisms and policies will assist in combating SPAM. Unfortunately, with the pervasive nature of the problem, there are no guaranteed solutions for completely eliminating SPAM.

Index of References:

[1] washingtonpost.com. “Spam's Cost to Business Escalates”
URL: http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A17754-2003Mar12&notFound=true
(March 13, 2003)

[2] Raq, Uri. net-abuse-faq. “How do Spammers get people’s email addresses?”
URL: http://www.faqs.org/faqs/net-abuse-faq/harvest/
(May 1, 2003)

[3] “Postini – Email Stat Track”
URL: http://www.postini.com/stats/index.html
(May 20, 2003)

[4] pcmag.com. “McAfee e500 Review”
URL: http://www.pcmag.com/article2/0,4149,135831,00.asp
(July 1, 2002)

[5] pcmag.com. “Ciphertrust Ironmail 210 Review”
URL: http://www.pcmag.com/article2/0,4149,135960,00.asp
(February 25, 2003)

[6] ciphertrust.com. “CipherTrust: IronMail – The secure email gateway appliance”
URL: http://www.ciphertrust.com/ironmail/index.htm
(May 20, 2003)

[7] Hansell, Susan. “Spam sent by fraud is made a felony under Virginia law”.
URL: http://news.com.com/2100-1029-998888.html?tag=fd_top
(April 29, 2003)

[8] Sorkin, David. spamlaws.com
URL: http://www.spamlaws.com/federal/108hr1933.html
(May 20, 2003)

[9] Weiss, Todd. “N.Y. Sen. Schumer to introduce do-not-spam list legislation”
URL:
http://www.computerworld.com/governmenttopics/government/policy/story/0,10801,80767,00.html
(April 28, 2003)

[10] Sorkin, David. spamlaws.com
URL: http://www.spamlaws.com/state/summary.html
(May 20, 2003)

[11] Lynn, Danny. GSEC Practicum, 2003. “Spam-Spam-Spam”
(2003)

Last Updated: May 29th, 2017

Upcoming Training

SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event