Global Information Assurance Certification Paper

GIAC Security Essentials Certification (GSEC)
Practical Assignment, Version 1.4b (amended August 29, 2002)

It's Spam, It's real, So Deal With It!

By Bob Hillmer, Submitted August 27, 2003

Abstract/Summary

Information security is founded on the principles of Confidentiality, Integrity, and Availability. A current and growing threat to availability of information systems is spam or un-requested bulk commercial e-mail (UCE). This paper will inform the reader on e-mail Spam's origins, the significance of the problem, what is being done by various groups of pro and anti-spam organizations and what can be done within a company to deal with the problem. Spam has to be taken seriously and dealt with as an information security concern because it has a significant and measurable impact on availability. A company's chosen spam solution must provide a suitable environment plus enable business activities without hindering the interaction with customers and with business partners. The choices security professionals make and the courses of action they take in regard to spam solutions will affect the ROI in people, technology, and processes. Spam cannot be ignored, it won't go away anytime soon, and an active defense will ensure your business continues despite the threat.

Introduction

Information security is founded on the principles of Confidentiality, Integrity, and Availability. A current and growing threat to availability of information systems is spam or un-requested bulk commercial e-mail (UCE). Spam has to be taken seriously and dealt with as an information security concern because it has a significant and measurable impact on availability. Availability of information is key to productivity of information-workers and business coordination in contemporary enterprises. If one doubts the significance or interest in spam, just do a search on the Internet. A recent Alta Vista search on the word "spam" netted 2.8 million hits in the U.S. alone with 3.9 million when opened up to a worldwide search. Articles on Anti-spam numbered nearly 300,000 in the U.S. and nearly 400,000 worldwide. As with most contentious issues there are two sides to the spam story. On one side are the spammers, the people developing the ad campaigns and pushing out the commercial e-mails. On the other side are the groups of recipients, individuals and companies, anti-spam vendors, and government bodies at the state and federal levels. Spam represents a serious security problem that can't be ignored. Information security professionals must deal with it through understanding the problem, examining potential solutions, putting those chosen solutions into place, and gaining allies from within and without to mitigate the threat posed by a growing volume of unwanted e-mail.

Where did spam come from? As opposed to the canned meat product introduced by Hormell in 1937.[1] contemporary spam began arriving in the 1990s with the widespread adoption of e-mail over the Internet as a way to communicate between individuals and businesses. There are an estimated 200 million e-mail addresses. The two largest populations are in the US and China. The numbers are 100 million and 68 million as of the end of June 2003, respectively.[2]

Each one of those addresses is a potential customer in the eyes of the electronic direct marketers otherwise known as "spammers." So, UCE or spam became the way to reach millions of people within a short period of time. Unlike snail mail, with spam there is no paper, no stamp, and no delay. It is serious business for a small number of individuals or groups who send out spam to make a living.

Steve Linford, of The Spamhaus Project, an anti-spam organization in the UK, estimates that 90% of all spam received by Internet users in North America and Europe is sent by a hard-core group of under 200. These professional, chronic spammers are loosely grouped into spam gangs and move from network to network seeking out Internet Service Providers known for not enforcing anti-spam policies.[3]

The amount of e-mail that can be sent by spammers is staggering. One such person is Juan Garavaglia, also known as "Super-Zonda." Garavaglia is believed to send out some 30 to 40 million spam each day.[4] The spammer's livelihood comes from two sources. Spammers receive fees for delivering the e-mail advertisement itself and for the information that is obtained. Out of those 30 to 40 million e-mails, if only a few percent of the targeted addressees respond, the numbers are still staggering. What else is staggering is the volume of UCE or spam that floods the systems of Internet Service Providers, corporate e-mail systems, and private computers. One estimate from a prominent Anti-Spam company, Brightmail, puts the number at 50% of all e-mail traffic in the world is spam.

Not everyone is against spam. Electronic direct marketing claims to be a legitimate extension of what has been in people's snail mailboxes for years. The lawyer for notorious spammer Eddy Marin is Mark E. Felstein, Esq. Felstein purports himself to be the Director & Chief Counsel for a group named EmarketersAmerica. In his letter to other direct marketers he raises the rallying call. "We're the direct marketers. It's time for us to flex our combined muscle and deliver our message! We generate millions of dollars that help stimulate our economy. We continually invest in equipment, inventory and technology. And, most importantly we create jobs!"[5] Not everyone shares that opinion when it comes to dealing with spam.

[1] Spam In Time
[2] Spam Warning Issued
[3] Register Of Known Spam Operations
[4] Sullivan
[5] Felstein

Spam is beyond an annoyance, an irritant, a minor problem, it can be a significant disruption to productivity and a drain on resources both system and human. From a technical perspective, detecting and diverting spam is a form of exception processing; that exception processing has to be done up front. Just as when writing code for input error checking, one has to account for the unexpected or unwanted cases first. Spam is the unwanted case for e-mail. Companies want to keep their corporate environments relatively free of spam. Individuals want the same for their own computers at home.

The spammers' efforts have a purpose. Just as the casinos in Las Vegas do all they can to bring customers into their buildings, so do spammers work hard to put their adds in front of prospective clients. Despite the fact the proportion of successful leads and customer follow through is low, by sending millions of spam e-mails there will be money made even with the small fees collected per successful hit.

In his August 1, 2003 Techlaw article from the Miami Herald, Mark Grossman a cyber lawyer sounds the alarm about even more costs from spam that are occurring beyond the desktop. "As spam invades text based messaging over cell phones, PDAs, Palms, and Pocket PCs, people are already paying for the privilege of reading the junk. Today the problem is most felt in Europe and Japan where text messaging is prevalent."[6]

What's the big deal? Even Bill Gates of Microsoft has felt the pain and has declared corporate opposition to spam. In a letter to Congress on May 21, 2003, the Chairman and Chief Software Architect of Microsoft Corporation lamented the current state of spam on the Internet and suggested the problem be dealt with as a cooperative effort.

> Microsoft firmly believes that spam can be dramatically reduced, and that the solution rests squarely on the shoulders of industry and government. There is no silver-bullet solution to the problem. Rather, we believe that fully addressing this problem for the long-run requires a coordinated, multi-faceted approach that includes technology, industry self-regulation, effective legislation, and targeted enforcement against the most egregious spammers.[7]

Kym Gilhooly in a July 28, 2003 article in Computerworld quantifies how the problem has a financial impact. According to Ferris Research in San Francisco, spam cost U.S. corporations $8.9 billion in 2002, a figure that's expected to rise to $10 billion by the end of this year. [8]

How big is the problem? There are impacts to everyone on the Internet from individual users at home to small businesses, to Internet service providers, to medium and large corporations. Even government is impacted both in receiving the spam and in receiving complaints from individuals and companies complaining about spam. The FTC collects an estimated 50,000 complaints about misleading e-mail messages each day.

---

[6] Grossman
[7] Gates
[8] Gilhooly

Businesses have devoted people resources and invested in infrastructure to cope with spam. AOL currently blocks over 800 million spam messages every day, the equivalent of 23 e-mails from every AOL account every day.[9]

In a typical Fortune 100 company whose primary business is not the Internet, there can be between 250,000 and 500,000 e-mails from outside the company processed everyday by the corporate e-mail system. The legitimate e-mail traffic is the lifeblood of the company. If the estimates for 50% of all e-mail is spam are correct, that's a significant load that wasn't intended nor scaled for in the company's network capacity planning. Still, companies have had to respond. That response has been to increase infrastructure spending to accommodate both the legitimate traffic as well as the spam. Beyond the raw processing power required to inspect and filter all inbound e-mail, there are storage requirements to hold suspected spam e-mail in quarantine, and dedicated people who manually review those stores. There are technicians who operate and update the gateway filters. Besides the technical side there are people who will spend time answering help calls and fielding irate comments from internal and external associates over the inconvenience. There is also the sheer loss of productivity while the offending e-mail is opened, reviewed and discarded at the employee's desk. For a company that depends on mobile users, spam can take up considerable time. When mobile users are dialed in, checking e-mail, they have to deal with spam, too. If they are using a filter to go through their mail and half of it is spam, half of their connected time is wasted. One large company estimated that spam costs them $7.2 million in one year.

Do the numbers. According to a December 2002 study by the Gartner Group, as much as 50 percent of all messages in a given corporate in-box are unwanted e-mail.[10] Spam wastes bandwidth, processing power, disk space and most importantly, people's time. If each message takes only 5 seconds of their time, enough to read the first sentence and delete it, then take one-third of your message traffic, multiply by five seconds, and you find out approximately how much time people are spending on spam. The situation is usually a great deal worse.

As an example, if a company's e-mail volume is 250,000 messages each day, the time spent at 5 seconds each works out to be 116 hours. At $100 an hour, that's $11,600 per day or just over $3 million per year. Of course, it is probably worse and worsening because the volume of both legitimate e-mail and spam is growing. According to one anti-spam vendor who has tracked the figures, since January of 2002, the percentage of e-mail that is spam has steadily risen from 17% to 50% in that 19-month period. The distribution of types of spam for July of 2003 is an expected mixture with the top four categories being general products, financial offerings, adult oriented sites, and health sites.[11] Whatever action one takes to reduce that totally wasted time means money that could be spent on improving business.

[9] Weaver
[10] Bowman
[11] Spam Attacks and Spam Categories

Do the numbers yourself: factors to consider include incoming volume, rate of occurrence, cost in productivity of workers, the cost of help desk staff, cost of storage to quarantine suspected files, security analysts to stay current and design counter measures, and managers who must deal with peers, superiors, and workers. As a security professional, it's important to quantify the impact of a particular threat and decide on the course of action and the appropriate level of energy to spend mitigating the threat. Of course, with every action comes reaction, so too, with the spam and defenses against it.

Challenges of the evolving counter-counter measure escalation spiral. Because spam can conceal its identity it mixes in with legitimate business messages and has to be sorted out. Just as modern electronic warfare evolved from radars that track aircraft to jammers carried by aircraft that hide the aircraft to radars that can track on jamming, to stealth technology that avoids radar through geometry, the battle against spam is not static. There are evolving and escalating tactics on both sides whether anti-spam or pro-spam. Early in the history of spam, content filtering techniques were used to detect particular words or phrases. Spammers soon found out what filters were being used and avoided using trigger words in their subject lines. By making their materials look like legitimate e-mail correspondence, using innocent sounding subjects and text, the spam slips past the filtering software. Within the framework of HTML e-mail, spammers use format tricks to avoid detection by character string comparing content filters. Early use of simple deception included putting spaces or special characters between letters. The content filters did not recognize the resulting string of characters as matching any "bad words" list, while the targeted human could easily see the intent of the text when they opened their e-mail. Signature based filtering programs can stop most elementary spam but the determined spammer will still get the message across to the human reader.

What's in it for the spammers? There is money in what the spammers do. Although it's a long path, the motive and pay-off for spam can be traced to developing leads on potential customers from their activity on the Internet. For example spam e-mail may offer low rates on a loan whether on a home mortgage, a car, or as a home equity loan. If someone is curious and fills in the request, the spammer obtains that information and can sell it to a company that compiles lists of potential customers. In turn, that intermediate company sells the compiled list to loan companies. Given that lead, the loan company then sends an e-mail offer to the prospective individual. Direct marketing is the name for that last step, but the lead originally came from spam. In a practical sense, this process provides a more focused target audience for the loan company for which they are willing to pay a premium.

Volume bulk mailings can be of enormous size. This activity costs the spammers money but there is a pay back. One estimated ROI calculation starts with the cost to send e-mail. At the rate of .025 cents per e-mail, one million e-mails cost $250. If the commission is $400 that means there is a 60% profit margin. There are even higher payments for lists of potential customers with confirmed e-mail addresses.[12]

[12] Hansell, "Totalling…"

What's in it for the anti-spam vendors? Vendors of anti-spam software have sprung up in response to the growing onslaught of spam. There is money to be made in software that promises to block unwanted e-mail. Just as anti-spam vendors are proclaiming the need for their products, the spammers question those motives. Notorious spammer Eddy Marin asks the question on his home page, "Do Anti-$pam Activists Have A Hidden Agenda?"[13] He speculates that the business for anti-spam software and services has a bright future with cited estimates of $653 million in spending for this year and increasing over the next 4 years to a figure of $2.4 billion in 2007.[14] Marin concludes from this "…spam won't or can't be eliminated…" consequently, he sees an equally bright future for spammers.

What's in it for you? For the enterprise information security professional, it's a headache. Not only do you need a plan to block the obvious, you have to separate the legitimate traffic from the unsolicited. If your company is in the medical support business, references to bodily functions, body parts, and legitimate behavior or sexual problems is normal. Your filters could block correspondence that is important to your successful business operation. If insurance is your business, there will be correspondence from customers that may be colorful, graphic, and intense. To provide customer service, you have to be able to receive and respond to what many would consider offensive e-mail. By blocking on particular key words you may be missing an important client's complaint. By not responding, you make a significant negative impression on your customer. George Tillmann, vice president and CIO of Booz Allen & Hamilton Inc. makes the point "The last thing I want is to have a million-dollar consulting assignment go south because I filtered out a customer e-mail."[15] So, simple word pattern blocking won't be enough to effectively improve the situation.

How much pain can you bear? Regardless, you must have a plan and a balanced one of infrastructure, processes and education. Examples of what you'll need are gateway and desktop filtering, blacklists of known spamming sites, white lists of expected good sites, a network spam policy, and user education. You must make a commitment to handle the volume. For example, Booz Allen quarantines e-mail that gets filtered as spam—2.5 million e-mails per month, roughly 45% of its e-mail traffic.[16] This raises another issue related to spam, which is the cost of storage. When spam is filling your databases, that space represents wasted resources that could be supporting your business.

Is there anything laws can do? Although spam is costly and annoying, it is legal under federal law. However, the bulk of spam appears to be deceptive or fraudulent, opening it up to a crackdown by the federal government's consumer protection agency. In prepared testimony before the Senate Committee on Commerce, Science and

[13] Marin
[14] Berr
[15] Gilhooly
[16] Gilhooly

Transportation, Federal Trade Commissioners Mozelle Thompson and Orson Swindle said spam is multiplying so rapidly that "solving the problem of bulk unsolicited commercial e-mail will likely necessitate an integrated effort involving a variety of technological, legal, and consumer action, rather than one single solution," The FTC has brought more than 53 actions against spammers who used deceptive content or used deceptive "from" addresses or subject lines, among other charges.[17]

Consult you legal department or legal advisor regarding the implications of spam on your network and your company. Since spam is not illegal, are you responsible to keep spam out? Find out exactly what responsibilities your company has regarding providing a non-harassing work environment. Is the presence of any offending material enough for one of your employees to bring a harassment lawsuit? The circumstance of multiple unwanted e-mails may constitute a hostile environment in the minds of your employees. Due diligence in this regard is an expectation that your company has a plan and is working on improving the situation. One visible way to show your efforts is by keeping your employees up to date on the situation and broadcasting your efforts to provide help. This notification and assistance can take many forms. Publishing informative articles in your company newsletter, publishing tips on your intra-net web sites either on the home page or on the information security site. Keep your help desk in the know about actions expected of employees regarding spam. In some cases it may mean dropping particularly hard hit e-mail addresses and building new ones for those offended individuals. This is a cost that isn't obvious but must be part of your plan.

What's going on in the courts? Spam vs. anti-spam. A group of direct marketers have joined together and filed suit against anti-spam companies claiming their rights are being violated. In Florida, this past April, a group called EmarketersAmerica.org filed suit against several anti-spam organizations such as Register of Known Spam Operations or ROKSO. As an anti-spam organization, ROKSO collects information and evidence on known hard-line spam operations and puts them on a published list for people and companies to cross reference and block. The criterion for being placed on the register is to have been rejected by a minimum of 3 consecutive ISPs for serious spam offenses. The purpose of the suit is to stop the anti-spam activities of the named organizations. Even though it may simply be a nuisance suit, it is drawing attention and bringing the issue into the courts.

In another recent court case, a judge in California overturned a lower court ruling that a former employee of Intel Corporation was not guilty of trespassing by sending e-mail 30,000 at a time.[18] The individual had been fired and was sending critical and unwanted e-mails into the Intel e-mail network. The basis for the decision was in response to Intel's contention of trespass. In this particular decision, there seems to have been no consideration for the cost to Intel to handle neither the mail volume nor the productivity lost by workers having to deal with the e-mails they found in their mailboxes. However, the decision does not prevent companies from suing spammers

[17] Weaver
[18] Singel

for overloading their servers. The case for business impact has to be more convincing in the future or spam will be unstoppable.

Potential attack vector of the future. Spamming and spamming techniques present a potential as an attack vector for viruses and other malware. With the SoBig.F e-mail virus currently infecting hundreds of thousands of machines and turning them into spam generating zombies, the future may already be here. The blend of using innocent sounding subject lines, spoofed source addresses, and imbedded calls back to web sites for additional malicious code, the reality is we're all being spammed by the virus. Malicious code that can come in through a called web site may do damage immediately, leave program code to be executed on a command or at a particular time, or may open a backdoor that can be used to gain access without the owner's knowledge at a later time.

Actions to take because it's a battle; there will be winners and losers. A layered approach from gateway to desktop is the way to provide a defense in depth and is the approach common among most larger companies. Do the research on products that recognize and respond to more than just pattern recognition or character string matches and signatures. This requires software and hardware. The software has to be adjustable to your specific business needs of policy enforcement, incorporation of inappropriate word lists, suspected domain names and e-mail addresses, plus web site references.

Selecting the hardware and the software plus deciding where to insert the equipment into your network topology are considerations that call for a team approach. Coordinate your efforts among those people responsible for the network's physical topology, the internal e-mail service, the firewall team and other filtering efforts. A typical configuration would include enterprise class servers running the anti-spam and anti-virus gateways inside the DMZ firewalls and ahead of the enterprise e-mail servers. The size, speed, and storage requirements of your chosen solution will depend on your volume of traffic and expected performance. The software licensing agreements for anti-spam products can cost $30 per seat for a smaller operation. Volume discounts will bring the cost per seat down for larger organizations. The hardware for gateway software running Sun Solaris or HP UX is in the $50 - $60K region. Single purpose servers can also be used and many companies use smaller, older technology boxes to handle this mundane and simple task. Design your solution using resources of hardware and software you already own. Many anti-virus vendors have newer versions of their software that also filters for content and thus blocks spam. Look carefully at the performance impact of running the content filtering in addition to the anti-virus code. There may be a need to increase your processing power to achieve the same throughput of traffic as you had before turning on the new capability. Finally, plan a minimum of 20% spare capacity to handle surges and periodically measure what the steady state condition is because it will continue to climb.

Your people network should be part of the solution. Educate your people. Don't keep your users in the dark. Educating users through your information awareness program is

a visible way to engage your employees. Include them in your efforts. Your work force is a powerful network of smart people. Help them recognize the significance of the problem and how they can participate in combating the effects of spam in a personal way. For those already impacted you won't have to convince them it's a problem. Those who haven't yet suffered will be more alert plus be ready to put up their own filters ahead of the problem getting out of hand. Providing a place to send examples is one way to get your employees focusing on dealing with the problem instead of simply complaining.

Provide information about your activities at the gateway, within the e-mail infrastructure of your enterprise, and on their own desktops. Prepare your information security staff to answer questions. Prepare your help desk staff to provide information on setting up filters to divert spam to a review folder. Gather statistics on reported incidents. With those numbers, you will be able to get an idea of the impact on work and on business. Publish lists of actions your people can take to lessen the impact of spam on their work. The better informed your users are, the more likely they are to assist you in the battle through individual filtering and reporting the problems in the first place.

Examples of Individual actions your users need to know and do:
Delete spam e-mail
Do not respond to spam e-mail as this confirms a valid address and may bring on more
Do not forward junk e-mail messages to other coworkers
Read a website's privacy statement before submitting your e-mail address
Be cautious about posting your work or primary home e-mail address on newsgroups
Report to the helpdesk or management when spam is impacting your work success
Set up a spam filter on your desktop

Don't limit your efforts to internal people and organizations. Work with your company's ISP to identify problems impacting your operation. There are standard clauses within the contracts or user agreements ISPs have with their customers prohibiting spam. Call on your ISP to follow through on that commitment when one of their customers violates the spam policy. Also enforce your own policies if you provide Internet service yourself. Within your corporate policies, include a clear statement of expectations of employees. Then check to confirm that policy is being followed. That includes monitoring the responses your employees are giving to spam that does enter the corporate network. When internal policy violations occur, it is important for credibility that you take action. That can be in the form of notifications, warnings, counseling, and ultimately releasing offenders.

Outside your own network and immediate service provider, establish communication and a working relationship with other ISPs. When you have an offending spammer clearly targeting your enterprise, work with the ISP who is supporting the offending individual. First determine and engage the source ISP through the IP address or e-mail address you identify as the source domain of spam. One company spent three days wrangling with an ISP that was not blocking what amounted to a denial of service attack

from one of it's subscribers. Eventually, the offender was blocked but it took convincing the ISP to pull the plug.

This situation indicates that you may find less than total commitment to stop offenders on the part of your ISP. Stopping spam may be an internal conflict for the ISP. On the one hand there are sales people wanting to bring in new business and collect the revenues from prospective clients. On the other hand are the support and complaint-handling staffs trying to rid their domain of the offenders who are generating customer complaints. Spammers are paying customers to the sales staff, but a drain on resources to the support staff. Persistence and clarity will work to eliminate offending subscribers, but the relief may only be temporary since those offenders will likely move to another ISP willing to take the new business, unaware of previous problems. Therefore be prepared for the protracted interaction.

Control your own environment, report significant problems to government entities, put spam blocks in place and stay current. You will need to put on enough staff or outsource the activity of keeping current with black listed sites, trigger word lists, and content filter maintenance. As the defenses get better, so will the offensive tactics of the spammers. Be prepared to increase efforts or obtain better filters and processes for adjusting or upgrading your equipment and your people. If the trends continue, spam, as a percentage of total e-mail volume will grow. So include the expected volume rises as you plan for infrastructure purchases. Don't expect to effectively clean 100% of your e-mail traffic but do make visible and serious efforts to eliminate known problems while continuing the flow of legitimate traffic. The nature of your business will dictate the flexibility you will be able to exercise. Keep your employees and business partners aware of the situation regarding spam. Efforts to make the situation better has to become a team effort not just your problem.

Conclusion Spam is real; it's a legitimate information security problem with a significant bottom line business impact. To counter its impact on your business, use a layered approach to lessen the impact at each succeeding level of your network infrastructure from the perimeter on the DMZ and inward toward the end user workstation. Do the research to explore and compare the variety of available products. Deploy solutions that will scale to your company's needs, accomplish the level of filtering and sustain the level of availability and performance your business demands. Your spam solution must do it's work plus enable business activities without hindering interaction with your customers and with your business partners. The choices security professionals make and the courses of action they take in regard to spam solutions will affect the ROI in people, technology, and processes. Spam cannot be ignored, it won't go away anytime soon, and an active defense will ensure your business continues despite the threat.

List of References:

Berr, Jonathan. “Spam filters causing legitimate e-mail to get lost.” Bloomberg News. May 13, 2003. URL: http://216.239.51.104/search?q=cache:k1HsFPz7HzEJ:www.sun-sentinel.com/business/local/sfl-zspam13may13,0,7288453.story+Jonathan+Berr+anti-spam+Bloomberg+News&hl=en&ie=UTF-8

Bowman, Lisa M. “Study suggests spam-stopping tricks.” CNET News.com. March 19, 2003. URL: http://news.com.com/2100-1024-993333.html

Felstein, Mark E. Esq. “Organization that sued anti-spammers.” URL: http://EmarketersAmerica.org/

Gates, Bill. “Letter from Bill Gates to the U.S. Senate Commerce Committee Regarding Spam Hearings.” May 21, 2003. URL: http://www.microsoft.com/presspass/misc/billgspam05-21-03.asp

Gilhooly, Kym. “Spam Battle Plans.” Computerworld. July 28, 2003. URL: http://www.computerworld.com/softwaretopics/software/groupware/story/0,10801,83386,00.html?nas=SEC-83386

Grossman, Mark Esq. “Spam.” The Miami Herald. August 1 2003

Hansell, Saul. ”Diverging Estimates of the Costs of Spam.” The New York Times. July 27, 2003. URL: http://www.theledger.com/apps/pbcs.dll/article?AID=/20030728/ZNYT05/307280400/-1/ZNYT

Hansell, Saul. “Totaling Up the Bill for Spam.” The New York Times. July 28, 2003. URL: http://www.dgl.com/uop/readings/totaling_up_the_bill_for_spam.pdf

Leyden, John. “Florida Spammers Sue Anti-Spam Groups.” April 23, 2003. URL: http://www.theregister.co.uk/content/6/30368.html

Marin, Eddy. “Do Anti-$pam Activists Have A Hidden Agenda?” URL: http://www.eddymarin.com/edit.html

“Register of Known Spam Operations.”.The Spamhaus Project. URL: http://www.spamhaus.org/rokso/

Singel, Ryan. “Ex-Intel Coder Wins E-Mail Case.” Wired News. June 30, 2003. URL: http://www.wired.com/news/technology/0,1282,59450,00.html

“Spam Attacks and Spam Categories.” URL: http://brightmail.com/spamstats.html#spam_percentages

"Spam In Time." URL:http://www.spam.com/

"Spam Warning Issued.". China Daily. August 9, 2003. URL: http://www.msnbc.com/news/940490.asp?0dm=B214T&cp1=1

Sullivan, Bob. "Who profits from spam? Surprise." August 8, 2003. URL: http://www.msnbc.com/news/940490.asp?0dm=B214T&cp1=1

Weaver, Jane. "FTC: No 'silver bullet' in spam fight." MSNBC.com. May 21, 2003. URL: http://www.msnbc.com/news/916420.asp?cp1=1