Global Information Assurance Certification Paper

You Got Mail – I Mean Spam!

John T. Granato

Introduction:

Not too long ago e-mail was actually mail from someone a person knew, or information that was asked for. "You Got Mail" in the early days of e-mail was the swan song of electronic mail sophistication. Today that swan song should be changed to "You've Got Spam".

Spam is slang for unsolicited commercial e-mail (UCE). People who receive spam often consider it an unwanted intrusion in their mailbox. Internet Service Providers (ISPs) like MSM.com and AOL.com try to stamp out spam whenever they can because these unwanted messages clog up the ISP's available bandwidth and slow legitimate business-to-business activity. Spam has also been linked to business scams, chain letters, virus attacks, and offensive sexual and political messages.(Tipton &Krause). In fact, the federal government enacted the Computer Fraud and Abuse Act of 1986 in an attempt curb the growing computer crime.

How Does Spam Work?

Companies and advertisers rarely send spam directly over the Internet themselves. They will hire a 'spammer' company to do the work of distributing the desired unsolicited e-mail. A company or advertiser enters into an agreement with the spammer who in-turn generates the e-mail advertisements to unsuspecting e-mail accounts. This is good business for the company or advertiser -- instead of spending thousands of dollars on postal mailings the company or advertiser will spend less than $100 per 10,000 e-mails. (Mueller)

Right now you are wondering where the spammer got the e-mail addresses it used for the mailings. The spammer obtained the addresses from a "harvester" who obtained them from you. That's right, you, yourself! In your eagerness to obtain information, join a newsgroup, or obtain some other service on the Internet, you gave them your identity in the form of your e-mail address. Once given, the address is often sold many times to different spammers. (Stim)

Not all the spam you receive is unsolicited. Because you didn't read the site carefully when asking for information or subscribing to a magazine, you let a checkbox get by that basically says "send me all your advertising". This advertising will continue to hit your mailbox until you ask then to stop.

Harvesters today go to great length to obtain valid e-mail addresses. They will deploy software programs that develop random e-mail addresses and create mailing lists. Using these mailing lists and linking a very obnoxious message to it, the harvester will bombard a domain. The idea behind this method is quite simple. The harvester wants the receiver of the message to become angry enough to respond back to him by either

the reply button at the top of the e-mail or the “remove me” statement at the bottom of the e-mail. If the receiver responds, the harvester gets a validated e-mail address.

To protect against harvesters of e-mail addresses, some ISPs try to ‘poison’ the harvester by generating bogus e-mail addresses. This practice, along with blocking and filtering, works for a while but becomes costly in the end because the harvester will eventually find a way around the current ISP defense. Thus the ISP will have to escalate its anti-collection defense in an attempt to stop the harvester.

The Problem with Spamming

People who defend spamming claim that it’s no different than the junk mail received via the U.S. Postal system. You toss the junk mail received into the garbage; with e-mail the recipient can just hit the Delete key in the e-mail program.

While there is some truth to the spammer’s claim that receiving spam in e-mail is not unlike getting junk mail in the postal system, it’s actually more like receiving an unwanted fax or a sales call on a cellular phone. Why? This is because the cost of distributing the spam is borne by the recipient and his/her ISP, not the spammer who sent it. Unlike direct mailers that cease mailing if only a few people respond, a spammer is actually encouraged to increase the intensity of spamming even if the previous spamming yielded only one or more confirmed addresses. (Levine)

Every ISP pays for the privilege to be on the Internet by buying what is known as bandwidth -- the space used to transmit on the Internet. As the volume of spam increases through an ISP, the purchased bandwidth becomes crowded, slowing down the ISPs ability to function properly. ISPs counter the spam volume by buying filtering software and passing the cost of the software to the subscriber in the form of increased fees. (Levine)

Most legitimate companies do not employ spammers. Most of the spam people receive involves some kind of shady practice. For instance, the pornography spammers disguise their spam with innocent subject lines like “Where have you been” or “Remember me?” Some spam messages will try to scam you with pyramid schemes, chain letters, bogus stock options and pirated software deals. Attempts have even been made to pass off malicious code such as worms as innocent spam. These worms are designed to collect the recipient’s e-mail address and the addresses in his personal address book, and mail them to a specific address for collection. Woe to the spammer or harvester who has stepped over the thin line between annoyance and crime. A really good prosecutor using The Computer Fraud and Abuse Act of 1986 can obtain a huge fine and imprisonment for up to 10 years. (18 USC 1030)

The War Against Spam

Avoiding spam is an exercise in futility. Recipients of spam can take the easy road and

just delete the message without responding. But even that is no guarantee because the recipient often opens the message to determine if its spam. Spammers attach a "return receipt request" to the messages they send so as soon as the recipient reads the message the address is validated back to the spammer via a 'returned receipt'.

ISPs often allow their users to block incoming e-mail from unknown sources. This is great until a much-needed legitimate message gets deleted.

Some anti-spam groups recommend replying to the spammer with a stern message requesting removal from the e-mail list. This is a waste of time. Spammers often provide fake return addresses, addresses to another organization that has nothing to do with the spam sent, or provide bogus phone numbers to call. In one case the spammer provided the toll-free phone number of a weather station in Jamaica. The best way to fight a spammer is to complain to the spammer's ISP and support anti-spam legislation in Congress and in each state.

Let's consider complaining first. Before you race off to complain, it's a good idea to find out the entire path that the message traveled to get to the inbox of the e-mail system. With e-mail message active, open the properties dialog box listed under "File" in the standard menu bar. In the properties dialog box click on either the "Detail" or "Header-ID" tab. What appears is the extended e-mail headers for the message. (Mindspring)

Copy the extended e-mail headers into the message, making sure the headers appear first in the message followed by the body of the message. Now save the message changes. An extended e-mail header may look like the following:

```
Return-Path: owner-nolist-admin*majac**MAJAC*-
COM@MAILSVRSQL.CLEARLOW.COM
Received: from mailsvrsql.clearlow.com ([206.65.166.76])
        by mail2.tuntek.net (8.11.2/8.11.0) with ESMTP id f27NDAE40442
        for <majac@MAJAC.COM>; Wed, 7 Mar 2001 16:13:10 -0700 (MST)
        (envelope-from owner-nolist-admin*majac**MAJAC*-
COM@MAILSVRSQL.CLEARLOW.COM)
Message-Id: <200103072313.f27NDAE40442@mail2.thuntek.net>
Received: from mailsvrsql (206.65.166.76:4032) by mailsvrsql.clearlow.com (LSMTP
for Windows NT v1.1b) with SMTP id <0.00000FEC@mailsvrsql.clearlow.com>; Wed,
7 Mar 2001 17:14:26 -0500
Date: Wed, 7 Mar 2001 17:08:58 -0500
From: Kevin Johnson <kevin@easywin.com>
Subject: Ever wonder what your high school friends are doing?
To: majac@MAJAC.COM
MIME-Version: 1.0
Content-Type: multipart/alternative;boundary="--==--==_Seperator1"
X-UIDL: 060b74912dba1e34a6ae65872d21394c
```

Once the headers are inserted into the suspected spam, forward the spam to

"spamcop@spamcop.net". The site will return a message with authorized URLS for reporting the spam. The address used to send the spam to spamcop will be the one from which SpamCop reports are sent. (SpamCop)

SpamCop is just one of several sites that performs this type of service. However, the reports are not always conclusive – sometimes a "nothing to report" is returned. When this happens, finding the spammer's ISP must be performed manually.

A detailed explanation of how to read extended e-mail headers can be found by going to the Internet site http://help.mindspring.com/features and selecting "How to Interpret Headers". This site will also lead you to a document titled "Figuring Out Fake Email & News Posts" which provides a comprehensive method of finding the proper ISP to send a strongly worded complaint.

When the ISP address is determined, send the complaint addressed to abuse@ (for instance, abuse@aol.com, abuse@hotmail.com, etc.). All ISPs have an abuse monitor and are interested in stopping spam because it costs them money. The complaint should be worded carefully and factually. One example that has worked well in the past:

> Dear abuse@(insert ISP name)
>
> Without prejudice I submit to you that this Unsolicited Commercial E-mail is from your user (insert name). The UCE is unappreciated because it costs my ISP (and ultimately myself) money to process just like an unsolicited FAX. Please look into this matter.
>
> Thank you.
>
> (Insert the expanded headers and the body of the message here) (Kingdon)

If the federal government employs the recipient, stronger wording can be added to the complaint. This is because spam arriving at federal government installations falls under the Code of Federal Regulations (CFR) number 41, Chapter 101, subpart 20 and Section 227 of Title 47, United States Code (U.S.C.).

CFR 41, Chapter 101, subpart 20 pertains to the management of federal facilities. Subpart 20-308 and 20-309 prohibits anyone involved in a commercial enterprise to knowingly send unsolicited advertisement to any federal facsimile machine. If caught, the sender could face fines of up to $500 per occurrence.(41CFR)

Section 227 of Title 47 U.S.C., Restrictions on Use of Telephone Equipment, deals with the restrictions on the use of telephone equipment on federal government installations. Subsection (a)(2)(B) defines a telephone facsimile machine as any machine that can transcribes text or images to and from electronic signals received over regular telephone lines. A computer with a fax board and a printer certainly fits

that description.

Subsection (b)(1)(C) of Section 227 prohibits the use of any telephone facsimile machine, computer, or other device to send unsolicited advertisement to a telephone facsimile. The maximum fine that can be imposed is again $500 per occurrence. (Cornell)

The complaint form the government could forward to the spammer's ISP could now look like this:

> On [Day, MON DD, YYYY at HH:MM:SS], [insert senders name] sent e-mail messages with a subject of "[insert subject of e-mail]" to numerous personnel of our organization. The address '@[insert name].GOV' that the message(s) was sent to is NOT a private address. It is a Federal Government resource provided to assist its employees in the performance of their official duties. It is a violation of the Federal Property Management Regulations for any person or organization to use government-controlled property for the solicitation of business, without first obtaining permission from the site manager (see 41 Code of Federal Regulations, section 101,20.308 & section 101,20.309).
>
> You may also be in violation of US Code Title 47, Section 227(a)(2)(B), since a computer, modem or printer meets the definition of a telephone fax machine. And, according to Sec.227(b)(1)(C), it is unlawful to send any unsolicited advertisement to such equipment, punishable by action to recover actual monetary loss, or $500, whichever is greater, for EACH violation**.**
>
> Therefore, please remove any and all addresses containing the suffix '@[insert name].GOV' from your mailing lists.
>
> This incident has been brought to the attention of our office of legal counsel.
>
> If you have a business reason for contacting the [Insert government agency name], please call our phone locator/assistance number at [insert telephone number]. The assisting operator will transfer you to the appropriate party.
>
> Thank you for your cooperation and prompt attention to this matter.
>
> [Insert Chief Security Officers name]
> [Chief Security Officer's title]
> [Chief Security Officer's Telephone number]
> [Chief Security Officer's e-mail address]
>
> [Insert message here with extended headers] (Besson)

While sending out complaints to ISPs, also take the time to support anti-spam legislation at the federal and state levels. Although there is a law prohibiting junk faxes

and unsolicited commercial calls to cellular phones – The Federal Telephone Consumer Protection Act of 1991 – there is no federal anti-spam act. Generally anti-spam law proposals have a tendency to fall into two categories. First, there are the tough anti-spam laws which Internet privacy groups' favor. These tough laws would allow the ISPs to sue spammers and provide criminal penalties for deceptive practices.

The second type is called the "opt-out" law, which the spammers favor. This law would allow recipients to elect to be removed from junk e-mail lists. This type of anti-spam law has been heavily criticized because it does not cost or punish the spammer and requires the recipient to take all the action to avoid further mailings.

According to the coalition Against Unsolicited E-mail (CAUCE), anti-spam legislation has been proposed in 17 or more states. So far only California and Washington have enacted tough anti-spam laws. California laws allow the ISPs to sue spammers that violate an ISP's anti-spam policy. It also requires that commercial spam include opt-out instructions and in some cases the law requires "ADV" at the beginning of the subject line.

Washington's anti-spam law is even tougher, prohibiting any mail that uses a third party's Internet domain name without permission. E-mail with fake or invalid return addresses, or contains a false header is also illegal in Washington. Records show that in 1998 a Washington man became the first person to recover damages under the law when he accepted a $200 payment as settlement for an unsolicited commercial e-mail.

Conclusion

Without a doubt spam is one of the biggest problems facing the ISPs and the Internet in general today and in the future. Each year more and more people are obtaining computers and turning on the Internet and delving into the e-mail environment. Each year these new people, and experienced Internet surfers, get spammed. Spam costs the Internet Service Providers and its customers millions of dollars in costly upgrades to combat the ever growing spam.

Keeping up-to-date on the techniques to eliminate or reduce SPAM is very important. The following are sources for more information about spamming and actual methodologies implementing filtering.

SPAM FAQ
http://www.cs.ruu.nl/wais/html/na-dir/net-abuse-faq/spam-faq.html
Legal and Legislative Information
http://www.cauce.org
Filtering mail to your personal account
http://spam.abuse.net/spam/tools/mailblock.html#filters
Blocking spam e-mail for an entire site
http://spam.abuse.net/spam/tools/mailblock.html

Blocking IP connectivity from spam sites
http://spam.abuse.net/spam/tools/ipblock.html
Sendmail Information
http://www.sendmail.org/antispam.html

By not actively opposing unsolicited commercial e-mail, the spammers will eventually rule the Internet. By actively fighting back and supporting legislation at the federal and state levels some sense of integrity will return to the Internet. Won't you fight back?

References:

Besson, Gordon D. "Junk E-Mail Response Form", URL:
gbesson@doeal.gov

CAUCE, "Pending Legislation", URL: http://www.cauce/legislation/index.html

Cornell University Law School. "US Code Title 47, Section 227" URL:
http://www4.law.cornell.edu/uscode/47/227text.html

Kingdon, Jim, "How to Complain to the Spammer's Provider". URL:
http://www.spam.abuse.net/howtocomplain.html

Levine, John, "Spammers do more than Spam", URL:
http://spam.abuse.net/scams/index.html

Levine, John, "Why is Spam Bad", URL: http://www.spam.abuse.net/spambad.html

Mindspring. "How to Interpret E-Mail Headers", URL:
http:// help.mindspring.com/docs/006/emailheaders/CIHDAIHF.php3

Mueller, Scott Hazen. "What is Spam", URL: http://spam.abuse.net/whatisspam.html

SpamCop. "Sick of spam?", URL: http://spamcop.net

Stim, Richard. "You've Got SPAM", URL:
http:/www.nolo.com/encyclopedia/ilaw/articles/gotspam.html

18 USC 1030. "Computer Fraud and Abuse Act 1986", URL:
http://austlii.law.uts.edu.au/au/other/crime/123.html

41CFR. "Soliciting, Vending, and Debt Collection", URL:
http://www.access.gpo.gov/nara/cfr/waisick_99/41cfr101-20_99.html