Global Information Assurance Certification Paper

Drowning in Spam!
GSLC V 1.0
Roger Finney

Abstract
In an Internet article published in 1998 Bill Gates said, "Wasting somebody else's time strikes me as the height of rudeness. We have only so many hours, and none to waste".[1] What Mr. Gates was referring to was the problem of electronic junk mail, commonly referred to as 'spam'.

Spam or spamming is generally referred to as "unsolicited bulk email" (UBE). "Unsolicited" meaning that you didn't ask for it to be sent to you and "bulk" meaning it was sent as a part of a mass e-mail. It's not certain how this junk email became known as "spam". Many claim it originated from a Monty Python skit where the SPAM meat product was featured. In the skit, a group continuously sang "spam, spam, spam, spam…" growing louder and louder, drowning out the other conversation. That analogy was applied to how unsolicited email can drown out normal communications on the Internet.[2]

Just as junk faxes flooded the corporate world in the 1980's, unwanted emails are flooding the inboxes of users all over the world, wasting time and money. It's not uncommon for people to get dozens of pieces of spam a day in their in-boxes.

Who Uses Spam?
Now that we have a general understanding of what spam is, it may help to know who is advertising using spam. The CAUCE (Coalition Against Unsolicited Commercial Email) organization listed the following examples[3]:

- Chain letters
- Pyramid schemes (including Multilevel Marketing)
- "Get rich quick" or "Make money fast" schemes
- Phone sex lines and ads for pornographic web sites
- Offers for software for collecting email addresses to be used in sending spam
- Offers for bulk email services for sending spam
- Stock offerings for unknown start-up companies
- Quack health products and remedies
- Illegally pirated software

A business that is strapped for cash can send an email ad to millions of potential prospects without buying an expensive direct-mail list and without the cost of printing, paper and stamps. So, the business or entrepreneur shifts the cost of

[1] Gates, "On Spam: Wasting Time On The Internet"
[2] SPAM Corporate Info, "SPAM and the Internet"
[3] CAUCE (Coalition Against Unsolicited Commercial Email), "The Problem"

advertisement to the recipient. Every business and every individual recipient of spam must help pay the cost of dealing with it.

The Problems and Costs of Spam

It is predicted that global email traffic will reach 35 billion emails in 2005, up from 9.7 billion in the year 2000.[4] While part of this increase will come from businesses and individuals taking advantage of handling goods and services on the Internet, a large part of the increase will be due to increasing spam mail. Anti-spam software vendors claim that approximately 40% of the Internet traffic in the United States is spam.[5] The National Security Institute says spam will cost organizations more than $10 billion this year in lost productivity and in efforts to combat it.[6] Spam now ranks with viruses and hackers as one of the costliest threats to organizations worldwide, and most of that cost is felt in the workplace.[7]

So why not just hit the "delete key"? That's how I handle my postal junk mail at home. I estimate that around 40% of the postal mail I get at home is junk mail. I can sort through my postal junk mail and throw it away before I even get in the house. Why not handle spam email the same way?

Unfortunately, the problems and costs associated with spam are much more complicated and cannot be addressed by simply scanning through your in-basket with your finger on the delete key.

So, what are these problems and costs?

1. Cost shifting

   A spammer with a simple dialup connection and a PC can send hundreds of thousands of messages per hour at a minimal cost. Imagine just how much postal junk mail you would receive every day if postage, paper and printing were basically free.

   Each email sent has an effect on bandwidth, memory, and available CPU cycles. When your Internet Service Provider (ISP) CPU is tied up processing spam, it creates a backlog on all the email in the queue. Each ISP must purchase bandwidth based on the projected number of customers they have. The cost of bandwidth is one of the highest operating expense items for an ISP.[8]

   When a spammer begins to consume the bandwidth of an ISP, the ISP has few choices: 1) let the customers suffer through slow response time, 2) take on additional operating costs by increasing bandwidth, or 3) pass

[4] GFI Software, "Dealing Effectively with SPAM"
[5] MSNBC, "Computer Spam Clogs E-mail Boxes"
[6] MSNBC, "Computer Spam Clogs E-mail Boxes"
[7] Trudeau, "Fighting The New Face of Spam"
[8] CAUCE (Coalition Against Unsolicited Commercial Email), "The Problem"

the expense on the customer by raising their rates. Again, the recipients bear the cost that the advertiser avoided.[9]

The costs are similar for businesses and organizations. Regardless of the amount of bandwidth an organization can afford, there is still a limited amount of data that an Internet connection can handle in a certain amount of time.

When an email comes into an organization, it passes through an Internet connection, through a firewall, and finally reaches the mail server. Just like the ISP, each email consumes a small amount of system resources such as bandwidth, memory, and CPU cycles. The impact of only a few spam emails is likely to go unnoticed. However, the problem is caused by the sheer volume of spam that flows into an organization.[10]

In my organization, we estimate that out of the 10 million emails received during a recent month, about 10% were classified as spam. That is 1 million unwanted emails that used our system resources and our time.

2. Fraud

Spammers are aware that the vast majority of recipients don't want to receive their messages. To deal with this issue, the spammers use tricks to disguise their email to look like anything but an advertisement. If you take the time to really look closely, you can usually identify spam messages. They usually contain subject lines with capital letters, exclamation points, and promises, promises, promises. Also, the senders generally falsify or hide their identity.[11]

My son recently got a message entitled "SEEING is believing!" It came from a sender that didn't exist. Turns out it was a spam message with links to pornographic web sites.

Some organizations use filters to block spam before it is delivered. However, spammers are becoming more and more creative and have ways to work around filters. A common trick is to relay their messages off of a mail server of an innocent third party. This process, in effect, doubles the cost because both the receiving system and the relay system are flooded with spam.[12]

3. Productivity of employees

[9] CAUCE (Coalition Against Unsolicited Commercial Email), "The Problem"
[10] Posey, Brian, "Combating SPAM Problems in a Corporate Environment"
[11] CAUCE (Coalition Against Unsolicited Commercial Email), "The Problem"
[12] CAUCE (Coalition Against Unsolicited Commercial Email), "The Problem"

Spam not only creates a drain on system resources, it can contribute to a reduction in productivity of your workforce as well.

Let's say that, on average, each of your employees receives 5 spam emails per day and spends 5 seconds on each. Now, 25 seconds does not sound like a lot of time. However, if you organization has 5,000 employees then collectively they would be wasting 125,000 seconds or 35 hours per day. This calculates out to 7,000 hours wasted each year (based on 200 working days). If you estimated employee cost is $50 per hour (including benefits) this results in a loss of $350,000 because each employee spends just 25 seconds per day dealing with spam.

There is also a good chance, that in the process of deleting spam, you will inadvertently delete an important message from a client or associate. This can also result in lost revenue (possibly even personal revenue if you deleted an important message from your manager!).

4. Disabling email

Email has become a critical business tool. The increasing amount of spam can degrade email performance and at times can render email useless.

This is very similar to the late 1980's when more and more businesses were using fax machines. Marketers would run scams to harvest fax numbers and begin mass faxing of advertisements. Many busy offices were overrun with advertisement faxes and could not effectively use the fax technology to conduct normal business because of the backlog.

The "fax" spam issue was eventually resolved largely through the passing of the Anti-Junk Fax legislation.

As spam continues to increase on the Internet and overrun our networking and processing capacity, was now face the same issues in our email environment.

5. Ethics and Morals

Spam is based on deceit, fraud, and basically stealing services. Aside from the business and economical ramifications, there are also moral and ethical standards being abused. Another responsibility that the spammers shrug off is who they target.

While researching this topic I ran across an article where a 7 year old (with the permission of his parents) opened up an email account so he could send email to his grandmothers.[13] Within a few months, his email had

[13] CAUCE (Coalition Against Unsolicited Commercial Email), "7 Year Old Gets Porn Spam"

been flooded with spam. He received as many as 30 spams per day, most pornographic. All were unsolicited, he had never signed up for anything on the Internet.

The parent was forced to abandon the account completely and set up a different one under a different name.

Combating Spam

In his book "The Road Ahead", Bill Gates writes that eventually we will be paid to read unsolicited email. You will tell your email program to discard all unsolicited messages that don't offer an amount of money that you have chosen.[14]

Now, I'll admit that Bill is much more of a forward thinker than I am. However, his prediction was written in 1995 and it still seems a long way off at this point. So, what do we do in the meantime?

Legislation has been suggested similar to the Anti-Junk Fax law. This legislation will attempt to put limits and restrictions on unsolicited email. Advertisements will be clearly marked so they can easily be deleted, and all email will be required to have a legitimate email address. Also, spammers will be required to honor requests to be taken off customer lists.

One such bill proposed by Senator Charles Schumer would initiate a national No-Spam Registry. This would be similar to the "Do Not Call" legislation recently put into law to address the problem of telemarketers calling us at home. While this sounds good, "Do Not Call" registers are effective because most solicitation calls are made from inside the country.[15]

The challenge with any legislation is that a majority of the spam is sent off shore before it comes back through unsecured, untraceable proxies. Secondly, a "Do Not Email" would consist of a huge list of email addresses. Think about it. How much would the spammers give to get their hands on that list? [16]

You can implement technology to assist your organization in addressing the issue of spam. There is filtering software available that can automatically block spam and undesired email. Microsoft Outlook has a filtering feature that you can tailor yourself to route spam messages directly to the trash or at least to a separate folder so they don't clutter up your inbox.

The problems with filtering software is that they are difficult to configure. And filtering spam does not completely eliminate it. Why? Because there is a fine

[14] Gates, "On Spam: Wasting Time On The Internet"
[15] Fogelson, Ben, "Spammed If You Do, Spammed If You Don't"
[16] Fogelson, Ben, "Spammed If You Do, Spammed If You Don't"

line between spam and legitimate email and marketing – and that line is basically in the eyes of the receiver.

My organization does receive legitimate emails that contain some of the same wording used in spam, such as financial quotes, medical references, and even sometimes "colorful" comments from our customers.

Filtering software can also cause delays in email delivery and they can become an administrative burden. Especially since the spammers are continually coming up with new spamming techniques meant to evade the filters.

Ultimately, a more advanced approach is needed that both analyzes the message content and message header as well as traces the email back to its sender.

Spam Education

As with most data security issues, you can significantly lower your risk by educating yourself and your employees. Here are some tips to remember:

- Never respond to a spam email. Even though many of these emails include an unsubscribe or opt-out for future emails, clicking on the link only confirms that you are a real user and will significantly increase your chances of receiving even more spam. Many times these links are simply a method of determining how many of their emails reached valid addresses. If you respond, your email will be marked as valid and likely added to other spam lists. The best thing to do is just delete it.
- Look after your email address. Be cautious of the websites where you post your email address on the Internet. Posting your email address on newsgroups, electronic newsletters as well as using bulletin boards and chat rooms increase your chances of be spammed.
- Check the address of incoming mail. Some emails look like they are from reputable sites such as Yahoo or Ticketmaster. They may ask you to re-enter your account or credit card info because they have misplaced it. Looking at the incoming address closer you notice it's not from www.ticketmaster.com but something very close like www.ticketmast**i**r.com.
- Read the privacy statements before you submit your email address to any web site. The policy should ensure that your email address will not be shared, sold or given to anyone else.
- Use the spam filters built into your mail program. Outlook has filters to keep out emails containing certain words or from certain addresses.

Conclusion

There few tools in history that are as powerful as the Internet. Communication and publishing of information is inexpensive and available to millions. Basically, the cost of sending an email is nothing. The core problem of spam is that junk

mail can be sent to tens of thousands of people – wasting system resources and our time – at almost no cost to the senders.

At this time, spammers have no incentive to limit the millions of emails they send and recipients have limited options for controlling the flood of spam. Until legislation is introduced, there is also no meaningful legal recourse.

With spam increasing steadily, it is important to take a proactive stance and educate your organization about the methods that spammers use and implement the proper strategies to mitigate your risk.

Using the Internet is a risk. It is unlikely we will see the complete elimination of spam. However, through continued advances in anti-spam software, increased pressure on legislators to pass strong anti-spam legislation, and educated users it will be possible to gain more control of spam and re-claim our email inboxes.

List of References

GFI Software. "Dealing Effectively with SPAM", May 19, 2003, http://www.secinf.net/anti_spam/Dealing_Effectively_with_Spam_.html Accessed August 13, 2003

SPAM Corporate Info. "SPAM and the Internet", August 14, 2003, http://www.spam.com/ci/ci_in.htm Accessed August 14, 2003

CAUCE Coalition Against Unsolicited Commercial Email. "7 Year Old Gets Porn Spam", May 30, 2001, http://www.cauce.org/tales/7_year_old.shtml Accessess August 13, 2003

Posey, Brien. "Combating SPAM Problems in a Corporate Environment", May 20, 2003, http://www.secinf.net/anti_spam/Combating_SPAM_Problems_in_a_Corporate_Environment.html Accessed August 13, 2003

CAUCE Coalition Against Unsolicited Commercial Email. "The Problem", August 14, 2003, http://www.cauce.org/about/problem.shtml Accessed August 13, 2003

Gates, Bill. "On Spam: Wasting time on the Internet", March 25, 1998, http://www.microsoft.com/BillGates/columns/1998essay/3-25col.asp

Fogelson, Ben. Eugene Weekly, "Spammed If You Do, Spammed If You Don't", August 14, 2003,

http://www.alternet.org/story.html?StoryID=16604
Accessed August 13, 2003

MSNBC. "Computer Spam Clogs E-Mail Boxes", April 9, 2003,
http://www.msnbc.com/local/kprc/a1568847.asp
Accessed August 13, 2003

Trudeau, Paris. Product Marketing Manager SurfControl, Inc. "Fighting the New Face of Spam", September 26, 2002