Understanding and Mitigating the Negative Impact of Unsolicited Email

John Armstrong
Mark Childs

CSCI E-170
Privacy, Security and Usability

Harvard University Extension School
Fall 2004

Contents

Summary

Spam is more than just a modern inconvenience. It is rivaling viruses and spyware as a disruptive force across the Internet and organizational LANs. Spam effects nearly everyone: home users, small businesses, large corporations, academic institutions, government agencies, non-profit organizations and community service groups. The impact should not be underestimated. The annual cost due to lost staff productivity, overloaded email systems, increased technical support and other displaced resources is estimated to exceed $20 billion worldwide. Another negative impact is the loss of legitimate email through aggressive filtering and the diminishing of email as a valuable communication tool. Now, credit card fraud and identity theft threaten to increase the toll Spam takes on society. New malicious concepts may be on the horizon.

There is also a substantial amount of crossover between anti-virus and spamming issues. Some of the techniques used by mass-mailer worms can also be used by spammers. And, many modern viruses are designed to facilitate the delivery of spam through zombie machines and mail relays. Finally, like virus protection; spam prevention requires robust systems spread across the enterprise, strong policies and processes and persistent monitoring and action. The resources utilized in deflecting Spam and mitigating its impact detract from other critical strategic technology projects, reducing the ability of technology to contribute to the organization's strategic plan.

The threat from Spam, the techniques used by spammers and the mitigation methods used to minimize negative impact are always in flux. The more information that technicians, system administrators, managers and executives can gather about unsolicited email, spamming techniques and spammers' motivations, the better equipped they will be to react and prevent unsolicited email.

Technicians and system administrators need to understand, prepare and respond to unsolicited email in order to minimize its disruptive impact on the organization.

Managers need to understand the scope of the threat, its ability to impact their operation and the need for policies, processes and systems to protect their resources

Executives need to look at the impact spam has on their organization: lost productivity, workplace disruption, resource allocation and the organizations ability to interact with their customers, stakeholders and the public.

In this article we wish to research, explore, deconstruct, and explain some of the contemporary techniques used by spammers in their quest to maintain their lead in the ongoing struggle over unsolicited email.

Terminology

Black List – blacklists are maintained by corporate spam-blocking software vendors or volunteer activist organizations. They contain a list of known addresses, domains, Internet Service Providers and others indicators for known sources of spam. Spam filters can use these lists to help identify known spam or suspicious senders. Also see white list

Ham – often miss-identified as spam – Ham differs in that it was sent as "solicited" commercial email and the recipient explicitly used opt-in (see below) to sign up for these emails.

Ignorebot – a script or email rule that sends soothing responses to complainants reassuring that the sender that the offender complies with all regulations

Mail Relay – a mail server that is configured to accept all incoming email and forward (relay) it to the recipient. Mail relays may be operated by ISPs that accept or encourage spammers or may be inadvertent as many early email servers enable relaying in their default configuration.

Mail Drop – a second email account that spammers use to receive email responses to their spam. A second "incoming only" email account is needed because the accounts that spammers use to SEND spam are frequently discovered and disabled by Internet Service Providers. Spammers respond by creating new "Outbound" accounts as fast as the old ones are disabled. (see whack-a-mole)

Opt-in – the only legitimate way to collect addresses for mailing lists and commercial solicitations. Be sure to read the fine print of the opt-in lists, because some opt-in lists share or sell their lists to unrelated third parties.

Opt-out – a scheme that spammers use to justify their unsolicited email. Spammers contend that they are entitled to send email to anyone, as long as they offer an opportunity for recipients to opt-out of receiving email. This is a false and ineffective argument because it places the burden of removing spam on the recipient.

Spam – unsolicited commercial email. The defining factor is that it is bulk mailed; often directed to huge blocks of addresses and the recipient did not explicitly request to receive this communication.

Spammers – people who send spam.

Throw-Away Account – also used in "whack-a-mole", it is an email account that spammers use only once for sending spam. When this account is disabled the spammer simply moves to a new account and repeats.

Web bugs - (AKA web beacons), are small chunks of HTML that are placed on a website or within an HTML enabled email. They usually are a small 1 pixel, invisible graphic file that will open a connection back to a particular web server for the purpose of tracking.

Whack-A-Mole – named for the arcade game where a mallet is used to hit pop up targets. Spammers use this technique to avoid detection by using 'mail drops' and 'throw-away accounts' to disappear after each spam assault – only to reappear somewhere else and repeat the offense.

White list – a white list usually maintained by a user or a system administrator. As opposed to a list of suspicious email, a white list is a list of trusted email addresses or senders. An email system that rejects all mail except for those on a "white list" may receive little spam – but may lose many legitimate emails.

Usenet - a subnet of the Internet that houses news servers, a bulletin board style listing of articles and discussion groups.

Zombie – a server or PC that has been taken over by remote control or proxy software. These devices are often used to launch spam so that the identity of the real spammer is obscured. The more offensive, egregious or illegal the spam is, the more likely the real culprit was hiding behind a zombie.

Brief History of Spam

Unsolicited mail is not a new concept. Chain letters have been around for over 100 years and bulk mail (junk mail) recently celebrated its centennial. However, the impact of email, its broad reach, its extremely low cost and its ability to be sent from anywhere in the world to anywhere in the world make unsolicited email the king of junk mail.

The first use of the term "Spam" pre-dates modern email systems. First appearing in Multi User Dungeons (MUDs)[i] the term referred to an attempt to overload the host system, its database or flood the chat session with text – driving out other conservation. The name is widely acknowledged as coming from Month Python's "spam skit" of the early 1970s. The term gained popularity in MUDs and chat systems through the 1980s – but it still did not apply to unsolicited mail. In the 1990s the term started to show up in Usenet postings – often paired with "cross-posting". This jargon, an inside joke originally coined by a small clique of early adopters (MUDers), followed them into the Usenet arena.

In the early 1990s, Usenet was a rough and tumble place. Often cliquish, churlish and ill-mannered due to the isolation and anonymity of a keyboard tending to erode what mediocre social skills many of its inhabitants had -Usenet still had rules of etiquette if not decorum. Spammers were held in particular disdain by the Usenet overclass. However, the growth of early mass-marketed BBS systems helped to swell the ranks of Usenet users and the appeal of a mass audience was too much for the spammers to ignore. The practice of sending mass, unsolicited email and the label for its application was now set.

Throughout the middle and late 1990s, driven by graphical-based web browsers, mass-marketed Internet access and inexpensive PCs, Internet usage boomed from less than 10% of the population to more than 30%. That growth has continued throughout the early years of the twenty-first century, reaching nearly 60%[ii] of the US population by 2004. That is a tremendous amount of growth and the potential of that large of an audience raised both the stakes and the pot for spammers. Techniques and methods were getting more sophisticated. HTML-enabled email allowed interactive graphic-rich advertising to be sent and sophisticated email harvesting schemes had been developed.

All of this growth has been built on top of protocols which have not anticipated some of the issue Spam has brought about. The email system is built on top of SMTP (Simple Mail Transfer Protocol), an easy to use and forgiving protocol which

only requires that the recipient's address be accurate. With no sender authentication required, header information designed to identify the source of a message can be falsified. This allows senders to be anonymous with little effort.[iii]

Negative Effects of Spam

Technology research firm Basex reports that Spam costs $20 billion dollars a year in lost productivity, clogged email systems, increased bandwidth usage, data storage costs, user support and the need for anti-spam software, hardware and administration to combat the problem.[iv] Its estimated cost is about $600 to $1,000 per user per year. Basex believes that over $600 million was spent on anti-spam software and other responses to try to mitigate the impact of Spam. That number is predicted to increase to $2 billion in 2005. This expense effects nearly all organizations: corporate, governmental and non-profit. Not only do IT budgets suffer, but the money spent on fighting Spam usually comes at the expense of other needs; strategic technology initiatives, operating expenses, profits, wages or capital investments. This is not just a corporate problem. Every dollar lost due to Spam has to come from other sources. This can hit cash-strapped charities, governmental agencies and community service organizations especially hard.

Technology-consulting firm Gartner Group reinforces these staggering numbers. Gartner estimates that an organization of 1,000 employees will lose $300,000 per year in lost productivity alone[v]. When you add in the cost of increasing your email infrastructure to handle the additional workload, additional software and hardware and technical support to deflect Spam, the Basex numbers seem reasonable. Independent research company Nucleus Research has estimated the annual cost of Spam mitigation at $874 per employee[vi]. They estimate that each employee loses about 1.4% of their productivity simply managing Spam. Jupiter Media Metrix estimates that each individual piece of Spam costs $1.00 in lost productivity. Not counted, but still critical, is the impact that Spam has on employee moral. The increasingly offensive, vulgar, pornographic and fraudulent nature of Spam can lead to increased employee complaints and even litigation.

In addition to lost productivity, Spam impacts both the Internet and individual email systems. It is estimated that by the end of 2005, up to 90 percent of all Internet email may be Spam. America Online and MSN report that about 80 percent of their incoming email is Spam - about 67 emails per user per day. This is a huge burden on any ISP's email system. For organizations that choose to tackle the Spam issue themselves the costs can also be high. The load placed on email systems due to spam can cause the hardware requirements to double. Spam filtering software can cost about $30 per user per year and usually requires

additional dedicated hardware. Spam management can easily consume 25 percent of an administrator's time.

Spam does not only impact productivity and drain resources, but negatively impacts the usability of email systems. In order to minimize lost productivity, Spam filtering has to be sufficiently aggressive to catch the vast majority of unwanted email, yet forgiving enough to avoid blocking legitimate email. Productivity may be lost due to Spam, but losing a legitimate email due to too-aggressive filtering can be worse. Email has become a vital tool in business, government and other organizations. Corporations cannot afford to lose communications, requests or product orders from their customers. Government agencies carry a responsibility to serve and respond to their constituents. With email a popular communication tool, effective organizations cannot afford to lose communication with their customers or appear unresponsive due to lost or filtered email. Spam filters need to be watchful for both errors of omission and errors of commission.

Spam also causes a subtler but important loss of faith in email as a communication medium. Email plays an important role in effective organizations and can improve communications, reduce expenses and reduce communication delays. However, if people lose faith in email as a communication tool, a valuable resource is diminished or lost. There is evidence that such a trend is emerging. Avoiding email is no longer the providence of the technophobe or luddite. Experienced, skilled users are starting to weigh whether the convenience and advantages of email are being offset by the negative impact of Spam, viruses, phishing and other malicious uses.

In "Spam: How it is Hurting Email and Degrading Life on the Internet"[vii], Deborah Fallows writes, "In large numbers, Internet users report that they trust email less and some even use email less because of Spam." Fallows' survey found that 25 percent of all email users have reduced their use of email because of Spam. Fallows' numbers are in line with other reports. Her survey discovered that about 12 percent of hone email users spend a half hour or more per day deleting Spam from their mailboxes. Other reports have demonstrated the huge financial impact of Spam, but Fallows also addresses the social costs incurred due to Spam. Fallows contends that the Internet was begun on a foundation of open access and that Spammers are taking advantage of this and "…ruining a good thing." Fallows continues, "Email was supposed to be efficient, reliable and trustworthy. Now, it's more often than not intrusive, misleading and disgusting." The stories users tell in this survey sound too familiar.

Attorney Sean O'Bryan gets about 100 emails a day through two separate accounts. In spite of trying several commercial filtering programs, he says that the vast majority of incoming email is spam. It has dampened his enthusiasm for email. The email messages he used to exchange with family around the country have all but stopped.

Public relations VP Matt Freidman, says that he is often unable to keep up with the inflow of Spam at work, so he often brings his laptop home and works off-hours just to delete Spam. He now describes email as "…an ordeal"

For some, email is beginning to feel like a walk through a seedy neighborhood at night. Basically, Spam pollutes email for everyone and we all suffer from the debris.

Motivations

The low cost to send Spam, and the effectiveness of it drives its continued growth. Compared to other direct marketing techniques, Spam's low cost to the sender is unparallel, costing just $0.00001 per message, as compared with $1.00 for telemarketing call, or $0.75 per postal mail message. [viii] In one survey in the United Kingdom, Forster Research found that 23% of Spam gets read[ix]. Fallow reports that 7 percent of survey respondents had actually ordered a product or service that was offered in an unsolicited email.[x] This is a huge number; because Fallows goes on to claim that due to the low cost of Spam, a response rate as low as 1 in 1,000 is a break-even point for spammers.

One of the first acknowledged Usenet Spams – Canter & Siegel's "green card lottery" was placed in order to advertise legal services[xi]. Since then, most Spam has been driven by commercial advertising. Spam was originally simple text messages. But as email systems grew and became more intuitive and graphic-based, Spam adapted. Now Spam tends to be graphic rich, with embedded context-sensitive links and often complex page layouts. In addition to goods and services, other marginalized ventures drifted towards Spam – attracted by its low cost and broad reach. Schemes, scams and scoundrels jumped into Spam in a big way. None of these activities were new; pyramid schemes, get rich quick, work at home, con men and other schemers have always advertised; often in the back pages of seamy publications. But, Spam enabled these swindlers to cast a much broader net for much less money. Technology had lived up to its promise of increased operational efficiency and greater opportunity – at least for the spammers.

If restrictions on telemarketing (the national Do Not Call Registry) have a substantial impact on sales for the companies that use this marketing technique, we may see more companies and organizations turn to Spam in order to reach their audience. Telemarketers know what level of response to expect from a sales pitch. All they need to do is use the reach of email to increase the number of prospects they canvas. Spam can be used to drive prospective customers towards the telemarketers. Displaced telemarketers can use Spam to generate sales leads and incoming phone calls and traditional telephone sales tactics to close the sales.

The global nature of the Internet has made Spam an international business. Spammers, located in the United States, can create solicitations locally and then use Russian proxies and viruses to create zombie machines to send the Spam

through email relays located in China, India or other countries[xii]. Spammers in foreign countries can target US citizens from nearly anywhere in the world and operate outside of the reach of US laws and regulations. Distance offers many advantages for the spammer and few (if any) disadvantages.

The impact of Spam has not escaped the attention of criminals and criminal organizations. In 2003 a derivative of Spam, "Phishing", surged in volume. Phishing scams, where often cleverly forged emails and social engineering are combined to lure victims to fraudulent, spoofed websites in order to steal credit card numbers, account and password information or other personal information have been amazingly effective. Gartner reports that as many as 30 million Internet users experienced a Phishing attack and that approximately 1.8 million people have fallen victim. In Phishing's boom, as many as 3 to 5 percent of the recipients were effectively fooled by the scam[xiii]. This is an enormous success rate – and it has been estimated to have been responsible for over 1.2 billion in fraud. ISPs have been getting better at responding to these threats by black-holing the IPs of offenders, but the Phishers have also gotten more sophisticated. In many cases organized crime, both domestic and foreign, have replaced the early "fly-by-night" Phishers.

Spam containing offensive, pandering and pornographic also continues to multiply. Fraudulent organizations, often overseas, use Spam as a way to drive traffic to their web sites, where dubious or illegal goods and services are offered. Not only is the risk of fraud higher on these sites, but the risk of credit card theft can also increases when you are dealing with merchants that seem to be turning to Spam. The rate of fraud, credit card theft and undelivered merchandise is substantially higher for many types of products. Credit card companies usually close the merchant accounts for these companies as their tactics become apparent – but the culprits often pop up under a new name and repeat the same practices.

Basic Spam Techniques

The first techniques used by Spammers to avoid detection were simple and unsophisticated. Surprisingly, they are still in use in some form. For instance, false subject lines are still being used as a form of social engineering – enticing the recipient to open their email.

Generic subject lines might simply be:

- Re: your attachment
- For your consideration

Or they may use a lurid or enticing subject line like:

- You gotta see this!
- Check out these pics!

A Federal trade Commission study found some interesting numbers[xiv]:

- 22% contained a false subject line – of which 42% claimed a personal relationship with the recipient
- nearly one-third of the false subject line messages were advertising adult oriented products or services
- 40% contained at least one false statement in the message body
- emails advertising business or investment opportunities contained up to 90% false claims
- 66% of all spam messages contained either a false From, false subject, or false claims within its text

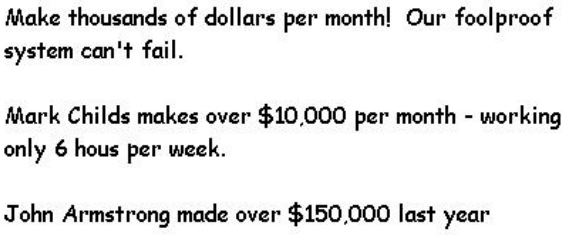
As organizations began to apply "word based" Spam filtering, spammers responded with simple tactics to fool these filters:

- alternative characters "0" for "o" "\/" for "v" (popular in Viagra ads),
- inserting or inserting characters or spaces between the letters "V`I`A`G`R`A" that the human eye "removed" but crude filters missed
- foreign or accented characters "Frěě mõnĕΨ"

As Spam filters became more sophisticated and adaptive, spammers developed more tricks. John Graham-Cumming, the author of a popular Spam filter, POPFile, has chronicled and named many of these tricks in "The Spammers Compendium[xv]".

The Big Picture

The big picture replaces the text in an email with a single jpeg graphic.



In an interesting twist – the graphic may contain only text. However, since it is not text – only a picture of text – there is no content to scan on. Adaptive filters responded to this by rating emails with no text high on the Spam scale. Spammers responded to this by combining this technique with other techniques – notably:

Hypertextus Interruptus

involves using non-displaying HTML tags to interrupt offensive or suspect words in a message. Examples would be:

Via<! —xe64 →gra

Viagra

This trick can be caught by instructing Spam filters to ignore all HTML before parsing and evaluating the email.

Invisible Ink

These tricks will place legitimate text into the email in an effort to fool the Spam filter. I frequently receive Spam formatted like this, so I suspect it is an effective tool and easy to implement. Examples are:

> You will never see this small, white text on a white background in an HTML enabled email
>
> <head>or by placing words into the email header – which is not displayed by most email clients</head>
>
> x-mime-key: You will not be able to see this text either – but it may fool your Spam filter into thinking this is a legitimate email.

There are many variations of invisible ink. Since spam filters may look for obvious matches between background color and font color, spammers may use near matches that fool spam filters but still hide the legitimate text from the human eye.

> <table bgcolor="#FFFFFF"><tr><td><font color="#FDFDFD">

Legitimate text can also be hidden within HTML spam by placing it within non-rendered HTML tags, such as:

> <style></style> or <title></title>

Legitimate text can also be hidden within hidden form fields or marquee tags

> <input type=hidden value=" Insert some legitimate text here!">
>
> <marquee height="2" width="2">Insert some legitimate text here!
> </marquee>

Script Writer

Script writer involves using a javascript program as the body of the HTML message**.** When the message is opened, the javascript runs – redirecting the user to an unexpected web site or loading an alternate email message. This technique should also work for virus, phishing attacks or as a tool to trick recipients into loading objectionable or malicious websites.

This trick can be coupled with enigma to further confuse Spam filters.

Daily News

Verbiage, often news articles or other legitimate text is placed between two false HTML tags. This text will not be rendered by the HTML mail client – but will be seen by the Spam filter – and is likely to reduce the Spam score of its email because a large amount of legitimate text will be recognized by the filter.

> <Not even wartime combat could prepare him for the shock of the tsunami devastation, Secretary of State Colin Powell said after inspecting the Indonesian island of Sumatra where giant waves washed away whole neighborhoods.
>
> Powell, commenting after a 30-minute helicopter tour, said, I've been in war and I've been through a number of hurricanes, tornadoes and other relief operations, but I have never seen anything like this.>

Enigma

Not all techniques involve hiding text to lower an emails Spam score. Some tactics use decimal, hex and octal encoding techniques to obscure the identity of the web site that the email links to. This can help Spam get around Black Lists or blocked sites.

http://7763631671/index.htm

http://0xCeBF9e37/index.htm

http:// 0316.0277.0236.067/index.htm

http:// 3468664375@3468664375/o%62s%63ur%65%2e%68t%6d

Slice and dice

Slice and dice is a clever trick that obscures the content from many Spam filters by breaking up the text into an HTML table – and then filing that table with text – from top to bottom in columns <td>. When the email client renders the HTML page it will look and read like normal text, but to the spam filter it appears like a string of unrelated characters.
The Spam filter sees:

AWOCOFTNF DENEROR WF U OL NL

The email parses this into:

ACT NOW
WONDERFULL
OFFER

The first column is filled with AWO, the second column is filled with COF, the third column is filled with TNF, etc.

The HTML would be:
<html><head></head><body>

```
<table cellpadding=0 cellspacing=0 border=0>
<font face="Courier New, Courier, mono" size=3>
<tr><td>

<table cellspacing=0 cellpadding=0 border=0>
A<br>W<br>O
</table></td><td>

<table cellspacing=0 cellpadding=0 border=0>
C<br>O<br>F
</table></td><td>

<table cellspacing=0 cellpadding=0 border=0>
T<br>N<br>F
</table>
</td><td>

<table cellspacing=0 cellpadding=0 border=0>
 <br>D<br>E
</table>
</td><td>

<table cellspacing=0 cellpadding=0 border=0>
N<br>E<br>R
</table>
</td><td>

<table cellspacing=0 cellpadding=0 border=0>
O<br>R<br><br>
</table>
</td><td>

<table cellspacing=0 cellpadding=0 border=0>
W<br>F<br><br>
</table>
</td><td>

<table cellspacing=0 cellpadding=0 border=0>
<BR>U<br><br>
</table>
</td><td>

<table cellspacing=0 cellpadding=0 border=0>
O<br>L<br><br>
</table></td><td>

<table cellspacing=0 cellpadding=0 border=0>
N<br>L<br><br></table></td></table></td></body></html>
```

Web Bugs / Beacons

Web bugs (AKA web beacons), when applied in spamming, are small chunks of HTML that are placed within an HTML enabled email that open a connection back to a particular web server for the purpose of tracking when an email is opened. This helps the spammer recognize and verify legitimate email addresses. These addresses have additional value because they demonstrate to the spammer that:

The email address is valid
The recipient probably does not have spam filtering
The recipient has demonstrated a willingness to "open" the email.

Opening up a spam with a web bug hidden in it will almost guarantee an increase in spam from the sender.

Web bugs work in different ways, and varying levels of sophistication. Some are linked to web servers that are able to extract email addresses from cookies placed there by associated sites. Some use javascript, Vbscript or activeX to trigger a response email. However, a simple method is to use a script that places the recipients email address as a cgi variable in the web bug. This returns the email address when the victim opens (or previews!) the email. Here is some actual code generated by a demonstration site - http://www.nthelp.com/OEtest/oe.htm

```
<img src=3D"http://216.144.1.23/oe.gif?=mgchilds@comcast.net"
 alt=3D"oe.gif (1024 bytes)">
```

Some responses to this exploit will be discussed later, particularly "disable your preview pane" and "disable html in your email."

Government Legislation

On January 1, 2004, the US government enacted the 'Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003', or more commonly know as the CAN_SPAM Act in response to the growth of unwanted commercial emails. Headed by the Federal Trade Commission (FTC) and the Department of Justice, but enforceable by other federal and state agencies, CAN-SPAN was not designed to outlaw Spam, but has guidelines for sending unsolicited commercial emails and penalties for those who break those guidelines. The key provisions of the act mainly attempt to address the false identities many spammers utilize, as well as provisions that would help consumers limit Spam. Summarized below are some of the key components of the act:

- False or misleading header information is banned.
- Deceptive subject lines are banned.
- An opt-out method to request that the mail not be sent in the future is required.
- Mail must clearly identify it is an advertisement.
- Calls for the study and establishment of a national 'Do-Not-E-Mail' Registry
- Future establishment of monetary rewards for help in prosecuting spammers.
- Additional provisions and penalties are specifically designed to address some of the strategies spammers have adopted as tools for sending email - namely the harvesting or dictionary attacks to get emails, automated creation of electronic email accounts and relaying or re-transmission of messages though unauthorized access of third-party computers.
- Allows for civil litigation and defines cost of damages.
- Defines criminal penalties, including ranging from jail time to fines.

This was the Federal governments attempt to criminalize deceptive Spam, but not Spam itself. Many critics complained that this was a fundamental weakness of the legislation, stating that law should be built around an approach that only allows emails that consumers have chosen to receive, or 'opt-in' approach, would be the best approach. [xvi] But not all criticism was negative, with CAN-SPAM act giving guidance to legitimate marketers on best practices and policies. Additionally, there was the first conviction of a spammer under the CAN-SPAM act in September of 2004.[xvii] Many ISPs have begun lawsuits, with Microsoft has filed over 40 alone[xviii] and the 'Anti-Spam Alliance' combine the resources of Yahoo, Microsoft, Earthlink and AOL to fight spammers in court.[xix]

CAN-SPAM Act called for a proposal to be made by June of 2004 to what would be needed to setup a 'Do-Not-E-Mail' Registry. In June, the FTC acknowledged

that 'Without authentication, a Registry will, at best, have no impact on spam and, at worst, result in more spam.'[xx] The FTC realized by creating a 'Do-Not-E-Mail' list, they would be creating a list of valid email addresses that would be highly prized by spammers. They concluded that there were no effective security measures to prevent the 'Do-Not-E-Mail' list from become a resource for spammers to identify valid email addresses and that the current state of email makes this approach impractical.

What did come out of the study into a 'Do-Not-E-Mail' registry was recognition of the main weakness of the 'CAN-SPAM' act – the anonymity emails allows and the lack of email authentication makes greatly undermines the enforceability of any anti-spam laws, as well as the effectiveness of some anti-spam filters. To respond to this, the FTC and the National Institute of Standards and Technology sponsored an 'Email Authentication Summit' in November of 2004. Several proposals came out of the summit to add authentication and fight spam[xxi]:

- Using sender domain verification which would involve checking the email source IP address against a list of approved email sending domains – an approach to minimize spoofing. Microsoft's protocol is known as Sender ID. Sender Policy Framework is an alternative, but similar approach.
- Using digital signatures in verification of the sender, as well as ensuring that the message hasn't been altered in anyway.
- Identified Internet Mail technology developed by Cisco, which uses a combination of both path-based and signature-based authentication.

The impact of CAN-SPAM is still under debate. AOL announced a significant amount of reduction of spam sent to its subscribers in 2004[xxii], but they seemed to be stressing the effectiveness of their filters, and not the reduction of overall spam sent to its users. There have been no other indications that CAN-SPAM has helped reduce the amount of Spam, but there have been some indications that spammers have changed their tactics to avoid identification and prosecution. Over 2004, the use of 'zombie networks', or hijacked computers, as sources of spam appears to have increased.[xxiii] According to Sophos.com, spammers have increased their average domain change from every week to every two days.[xxiv] Another new technique is to send spam from unregistered DNS, then registering the DNS a short time later. Meanwhile, in the time between the sending of the messages and the DNS registration, additional load and delays are created from the lookup of the non-existent DNS. This tactic, and the constant shifting and abandoning of DNS's to avoid detection has created even greater strains on DNS servers as they attempt to return the flood of undeliverable messages to non-existent DNS addresses.[xxv]

Practical Responses

For most organizations, the increased frequency of spam, its increasingly offensive nature and the increasing social and economic costs of spam warrant the investment needed to deflect spam away from the organization. Even individual users might find that the investment in spam blocking software pays dividends by improving their on-line experience. In early 2005, Internet Service Providers are heavily advertising their spam-blocking service as a major feature and differentiator of their service over another's. 2005 may be a turning point in the war against spam: a year where spam filtering and blocking becomes as vital as anti-virus software or patch management.

There are many different approaches and tactics to spam management, and like anti-virus systems it may take a layered approach and active dedicated systems administration to achieve effective spam filtering. Like viruses, the techniques spammers use adapt and evolve. System administrators and users will need to adapt and evolve their practices as well.

A good place to start on spam blocking and protection is at the email client. The client you use will depend on your organizational and computing environment. However, Microsoft Outlook and Outlook Express are still the widest-used email clients today. The techniques used to help protect against spam in these email clients can also be applied to other email clients as necessary. The concept will be discussed in a general format and specifics for Outlook and Outlook Express will be offered when applicable.

Disable Your Email Preview Pane

The first step we recommend is to disable any preview pane in your email client. A preview pane will display most or all the contents of the email message in a separate frame/window. In the case of an HTML enabled email, the message must be both parsed and displayed with an active HTML window. This allows malicious HTML to be activated before the message is officially "opened" by the user. This presents several risks, but regarding spam, it allows web bugs or beacons to activate before you "open" the email. Even if an email is recognized as spam (because of its subject line or sender) and deleted, the simple act of clicking on the email in order to delete it will cause the email to be previewed and any previewed – activating any embedded HTML web bugs.

In both Outlook and Outlook Express the preview pane is disabled by selecting 'view' from the tool bar and then de-selecting "preview pane"

Disable HTML In Your Email

This offers greater security from web bugs because any HTML is stripped out of the email before opening it. However, legitimate HTML enabled email will also be effected – often diminishing the value of legitimate email. This can be severe in documents that rely heavily on HTML for formatting – often rendering legitimate documents unreadable.

In Outlook Express 6 select 'tools' then 'options' from the toolbar. Under the 'read' tab, select 'Read all messages in plain text' and click 'OK' to save your changes.

Advanced users of Outlook 2002 can achieve similar goals through registry settings. A description is available here:
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q307594

Additionally, if you have Outlook Express and Windows XP-SP2, another tool is available, that offers more granular control. Select 'Tools' and 'Options' from the tool bar. Set Outlook Express to use the 'restricted sites zone' in the 'Security' tab. Select the option to 'Warn me when other applications try to send mail as me' and select 'Block images and other external content in HTML email'.

This will not block HTML and images that are included in the body of the email, but it WILL block HTML that is pulled from a remote site when opening the email – this blocks web bugs and beacons – but preserves other HTML content.

Protect Yourself from Email Address Harvesting

If your organization has a public facing web page you are a target for email harvesting. Organizations that require communication, feedback or responses from the public are likely to have numerous email addresses published on their website. These addresses can easily be harvested by automated programs (bots) and collected into spammer's email lists. Some of the Spammers tricks can be used against them to protect against spam, such as:

Drop Box – create a second mailbox for everyone that has an email address published on the website. This box will contain most of the spam and all of the public mail. The recipient's original mailbox will remain unmolested. The email in this drop box will still need to be sorted, but the recipient's daily work in their main mailbox will be much more efficient. Additional efficiency can be gained by small organizations by having these drop boxes managed by an ISP that offers spam filtering as a service.

Enigma – addresses that are published on public websites can use decimal, hex and octal encoding in the email address to confuse email harvesters.

Other techniques involve:

Webforms – customer feedback and comments are collected through web forms instead of <mailto> links. This stops address harvesting, but can have a chilling effect on customer feedback, as users may be leery of using these forms in fear of having their email address harvested themselves.

Encrypted Email Address - A clever technique that allows you to retain the convenient <mailto> tag is to use an encrypted email address and than runs a javascipt to decrypt the email address when the 'mailto' link is pressed. The email address remains encrypted and invisible to the harvester. For examples and additional information see:

mailto encoder http://rumkin.com/tools/mailto_encoder

Graphic Email Addresses – this scheme also uses javascript. A graphic that looks like the traditional 'mailto' link is placed on the web page. When the graphic is clicked a javascript runs that builds the email address and passes it into the mailto function. The javascript does not store the email address in a format recognizable by harvesting bots. For examples and additional information, see:

safemail http://safemailto.com/

"Good Citizen" System Administration

System administrators play a large role in spam abatement. Foremost is the importance of system administrators running a sound network and avoid having their systems misused as spam relays.

Disable Email Relays – best practices for email servers require that users authenticate before sending outbound email. Email servers should require authentication for mail relaying by users or restrict relaying to select IP addresses for system generated messages. This is becoming more common – but default settings on many older systems were OPEN for relaying. Networks should periodically be checked for mail servers because unknown (rogue) email servers can show up on many networks as a result of miss-configured servers or through applications deploying third-party SMTP servers as part of their installation. Mail servers should have logging enabled – and these logs should be periodically checked for suspicious activity.

System administrators should periodically run port scans or other diagnostic tools to locate unknown mail servers. All mail servers should be checked for proper configuration. Many network vulnerability scanners will check for open email relays.

Besides the good citizen perspective of disabling email relays, sound system administration requires it. An organization that has its email servers hijacked by spammers has its bandwidth and email server capacity stolen by the spammer. Additionally, the organization can be blacklisted as a spammer or face liability issues due to their failure to detect and stop this abuse.

Monitor and Secure Wireless Access Points – an easy and effective way to gain access to and hijack organizational email servers is to enter an organizational network through an unsecured wireless access point. The convenience and access of wireless networking is offset by an increased need to monitor and secure wireless access points. Unauthorized wireless access points (rogues) often appear on corporate networks due to their low cost and easy of installation. System administrators need to routinely scan for the presence of unauthorized wireless points and audit the security of their authorized ones.

Anti-virus Protection – any organization needs to have an effective, monitored and audited anti-virus system in place. Increasingly viruses are being used to facilitate spamming through the creation of proxies, zombies and email relay machines.

Spam Blocking Filters

The proliferation of spam, its demonstrated impact on productivity and organizational budgets and its increasingly offensive nature has made anti-spam efforts a big topic throughout 2004 and into 2005. Legal and legislative efforts are being explored and spam- blocking software is growing in relevance and importance.

Spam blocking software and appliances (dedicated hardware with pre-installed spam blocking software) are one of the leading growth areas of software sales. In a recent survey by InformationWeek, 70 percent of business-technology executives say "reducing spam to protect productivity is a top business priority this year[xxvi]."

Smaller organizations, that use a commercial Internet Service Provider (ISP) for email service, have few choices. ISPs are beginning to offer spam filtering as part of their email hosting or as a premium service. However, if spam blocking is not available from your ISP or the organization believes their ISP's spam blocking it is not effective, they will need to install client-based spam filters.

For organizations that operate their own email servers, there are several choices. Spam-blocking software can either be:

- installed on each desktop (plugging into most email clients)
- installed on existing email severs
- installed on additional servers
- installed as an appliance in front of the email server

The appropriate solution will depend on the size of the organization and the experience of the technical support staff.

Desktop Clients usually offer easy installation and allow individual users to customize their filters and settings. However, since they are unique to each desktop they are more difficult to update and maintain. Additionally, they usually do not share information with other clients, so they may not have as large of a "spam pool" to learn and adapt from. Desktop clients usually range from 20 to 30 dollars per client.

Server-based spam filters require more skill to install and operate. However they have the advantage of centralizing anti-spam settings and configurations and

usually allow for reporting so that email administrators can track their spam-blocking success. They will probably have a large "spam pool" to draw, learn and adapt from. If these spam filters are installed on your existing email server, performance of your email system may suffer if too many server resources are consumed by the filtering software. In order to resolve this issue, the Spam filtering software can be installed on additional dedicated servers – at an additional expense. Server-based spam filters will require additional system administration, but the cost of server-based software can be substantially less – usually running about 10 dollars per client. Ongoing software maintenance and updates will usually cost about 20 percent per year. As with anti-virus software – this ongoing support may be vital in order to enable the spam filtering software to respond to new and evolving threats.

Spam Filtering Appliances combine dedicated hardware and software in one package. Often the most expensive, they can provide easy administration and management combined with strong vendor support. Like a dedicated server and software, they usually sit in front of your existing email server. This offers robust blocking and removes the burden of spam before it reaches your email server.

No matter which spam filtering solution you choose, some key criteria to evaluate is:

- Ease of use
- Ease of Administration
- Filter should employ 'Bayesian' filters
- Ability to segregate incoming email for review
- Auto learning
- Add your own blacklists-block lists
- Vendor provides frequent updates
- Uses a reliable and tested blackhole list

Most software vendors offer trial versions of their software. This allows the system administrator, leadership, users and other stakeholders to test several different solutions in order to find the choice that fits their organization.

Involve your users

Even with spam blocking systems in place, a certain amount of spam is likely to evade your filtering system. An important part of your filtering/blocking system is to provide a way for exceptions (spam that slipped through the system) to be reported. An easy and effective way to accomplish this is to create an organizational "spamreport" mailbox. This mailbox allows organizational users a convenient way to report spam to their system administrator, remove it from their mailbox and return to more important activities. Simply train and instruct users to forward any suspected spam they receive to this single mailbox. This approach offers many organizational and technical benefits.

- It enables the users to get involved in spam prevention
- it demonstrates your organization is working seriously to block spam
- it helps reassure users that have received offensive spam that they are reporting the incident to the organization in a proper manner
- it helps give your objective numbers on the efficiency of your spam filtering - you can't measure a percentage of spam blocked without knowing how many "got through"
- it allows system administrators or security experts to examine the spam for new techniques and enables them to craft new responses and improve their filtering

Document Your Success

Finally, document your success. You need objective numbers to measure and evaluate the effectiveness of your spam blocking efforts. These numbers will be invaluable in many ways:

- Demonstrate to leadership that their investment in a spam blocking effort was sound
- Whether spam blocking and filtering is saving the organization money – celebrate that fact and let organizational leadership now
- Users that still receive spam may be frustrated - objective numbers will allow you to show how much worse the issue may be without blocking/filtering
- Spam blocking and filtering may be consuming an increasing amount of a system administrator's time – if additional resources are needed, objective numbers can provide proof

[i] http://www.templetons.com/brad/spamterm.html 12/27/2004 11:17:05 AM
[ii] http://www.pegasusresearch.net/metrics/growthus.htm 12/27/2004 12:06:04 PM
[iii] http://www.ftc.gov/reports/dneregistry/report.pdf
[iv] http://www.ecommercetimes.com/story/32478.html 1/3/2005 12:58:54 PM
[v] http://www.easylink.com/services_north_america/boundary_spam.cfm 1/3/2005 1:22:41 PM
[vi] http://www.nucleusresearch.com/research/d59.pdf 1/3/2005 1:31:50 PM
[vii] http://www.pewinternet.org/pdfs/PIP_Spam_Report.pdf 1/4/2005 11:07:03 AM
[viii] http://www.emailresults.com/article.asp?ContentID=6
[ix] http://www.theregister.co.uk/2004/12/10/spam_buyers_survey_bsa/
[x] http://www.pewinternet.org/pdfs/PIP_Spam_Report.pdf 1/4/2005 11:07:03 AM
[xi] http://www.wired.com/news/politics/0,1283,19098,00.html 1/4/2005 1:36:17 PM
[xii] http://news.zdnet.co.uk/internet/security/0,39020375,39157120,00.htm 1/4/2005 12:07:35 PM
[xiii] http://www.nwfusion.com/news/2004/0506gartnphish.html 1/5/2005 10:32:08 AM
[xiv] http://www.itaa.org/isec/pubs/e20035-04.pdf 1/5/2005 12:54:27 PM
[xv] http://www.jgc.org/tsc/ 1/5/2005 1:10:16 PM
[xvi] http://www.cauce.org/legislation/openletter.shtml
[xvii] http://www.usdoj.gov/usao/cac/pr2004/131.html
[xviii] http://www.clickz.com/experts/brand/capital/print.php/3447211
[xix] http://docs.yahoo.com/docs/pr/release1187.html
[xx] http://www.ftc.gov/reports/dneregistry/report.pdf
[xxi] http://www.theregister.co.uk/2004/11/16/email_authentication_summit/
[xxii] http://informationweek.com/story/showArticle.jhtml?articleID=56200528
[xxiii] http://news.yahoo.com/news?tmpl=story&u=/pcworld/20041228/tc_pcworld/119058
[xxiv] http://www.sophos.com/pressoffice/pressrel/us/20041208yeartopten.html
[xxv] http://news.yahoo.com/news?tmpl=story&u=/zd/20050110/tc_zd/142238
[xxvi] http://www.informationweek.com/story/showArticle.jhtml?articleID=17100348 1/9/2005 4:56:24 PM