mantra
COMPUTING, INC

233 Needham St.
3rd Floor
Newton, MA 02464

Ⓟ617.454.1310
Ⓕ617.454.1001

www.mantracomp.com

Spam, it's not just annoying anymore! What's happening, what to do about it and what's next for our venerable email system?

Spam is unsolicited commercial email, sometimes known as junk mail. Spam can appear to be nonsensical, contain sexually explicit material and impersonate email senders. Many people have noticed a marked increase in the levels of Spam in their Inbox over the last few months. Also, many people have reported problems with sending emails successfully, inexplicably disappearing emails, and fraudulent emails.

If you or your organization has been experiencing any of these problems, you are not alone!! The levels of Spam across the Internet have increased significantly beginning in September, with some email security firms and network administrators reporting an 80% rise.

Mantra Computing tracks its client Spam levels through its partnership with Mailprotector.net and has seen a significant rise in the levels of Spam for all its clients. One client receives over 3,000 Spam emails a week! With these volumes, Spam is no longer just a nuisance, it is a real problem overwhelming many mail systems resulting in delivery problems and information overload for many users.

How can this happen? Isn't someone responsible?

Unlike the United States Postal service, which has established procedures, rules and transactional fees (postage), the Internet's email system is based on a decentralized honor system with no transactional costs. Its rules were devised many years ago by academics that wanted to establish a simple communications system that would be available to all for the free exchange of ideas. It was never intended to support commercial interests.

When someone sends an email, the sender's computer uses a protocol called DNS (Domain Name System) to lookup where the email should be sent to, and then uses another protocol called SMTP (Simple Mail Transfer Protocol) to encode the email and deliver it to the intended recipient. The encoded email includes a return address similar to what is found on a regular postal letter, which tells the recipient where the email came from. Because there are no transactional charges and no way of authenticating where emails have come from (it is reliant on the recipient honestly and accurately including return information) the system is vulnerable to abuse.

Spammers have developed sophisticated ways of generating spam. Sometimes they use their own email servers, sometimes they hijack other people's email servers, and sometimes they hijack people's home and business computers and turn them into Spam generating "zombies" or "BotNets". Spammers hijack servers by opening up legitimate accounts with web hosting companies and then use those accounts to deliver as much Spam as possible before they are discovered. Legitimate email servers are also hijacked through unpatched security vulnerabilities. Personal or business computers are hijacked and turned into "Zombies" through Spyware. Spyware is software that is installed on a computer without the users consent and without the users knowledge. Spyware takes advantage of weaknesses in Microsoft Windows, Internet Explorer web browser, Outlook and Outlook Express email software. When a user visits a malicious website or opens a malicious email, Spyware can install itself. The Spyware software often creates "backdoors" that allow remote users to take control of a computer.

Spammers also generate Spam through computer viruses. Computer viruses use email to propagate themselves to other computers across the Internet. Once a computer is infected with a virus, the virus program scans the hard drive of the computer looking through many file types (Microsoft Office documents, the computer's address book, etc.) in search of email addresses. The Virus then compiles a database of valid email addresses and begins to generate large volumes of emails. The Virus falsifies the sender's address and populates the recipient's address using the database it compiled from your computer. These emails also include the payload to infect the recipient’s computers.

How did my email address end up in a Spammer’s database?

Spammers generate their email databases in many different ways.

First, Spammers can look up valid domain names from a public online list. A domain name is the second part of the email address (i.e. mantracomp.com from the email address garrett@mantracomp.com). Once they have a valid domain name, they can use an automated program to guess usernames such as john@mantracomp.com. Because Spam is free to send, they can afford to use a list of guessed emails and hope that one or two will get through. If one or two spams get through, the recipient may open the email, click on a link within the email and validate the email address for the Spammer.

Second, Spammers can setup automated programs called spiders or bots that search the Internet for email addresses. These automated programs work the same way that Internet search engines work. They go from website to website following the links and recording any email addresses they find. This includes Internet forums where users post questions and comments, corporate websites where they list company contact information and online articles. You can see where your email address is listed by going to google.com and searching for your email address. If it shows up in the search results, you can bet it is listed in a Spammer’s database.

Lastly, Spammers purchase lists of valid email addresses from marketing companies that collect personal information from online retailers, surveys and contests.

How do the Spammers make money? What motivates them?

There are three main ways that Spammers make money.

First, by generating huge volumes of emails with little cost they are able to “con” a few innocent people into buying or “clicking”; making their spam campaign worthwhile.

Second, a lot of Spam includes Spyware that installs itself on your computer without your knowledge or consent. Once Spyware is installed on your computer it is very difficult to detect and remove. Spyware collects browsing behavior and personal information and relays it back to marketing firms. DoubleClick (www.doubleclick.com) is one of the largest online marketing firms that collect data in this way. This marketing data is very valuable and can be sold to other businesses.

Third, Spammers use Scams and Phishing to steal personal data for identity theft, stock market manipulation, and other creative money making schemes. Phishing scams attempt to steal personal data including bank account numbers and PIN numbers by sending emails from what appears to be legitimate institutions with links to websites that also appear to be legitimate.

One example of a Phishing scam is an email from what appears to be your bank requesting you to logon to the linked website and update your personal information. The website you are linked to looks very similar to that of your own banking institution and asks you to confirm your account numbers, passwords, maiden name, etc. Once they have your information, they use it to steal your identity and your money. Another example of an online scam is an email from what appears to be a familiar person or an official sounding organization that lists hot pick stocks that are either “under valued” or “over valued”. This scam hopes to manipulate those stocks by artificially raising or lowering the stocks value so that the Spammer can then buy or sell them immediately after or before the Spam campaign thus making a profit!

The system seems broke! What can be done?, my business relies on email!

Unfortunately because of the way Internet email works, there is not a lot that can be done to prevent Spam on the Internet. The US Congress passed several laws in 2006 to legally define Spam and to provide consequences for generating it, but they have proved ineffective. The only option at this point is for individuals, ISPs and companies to try and filter out Spam.

Spam is generated by automated computer systems and as a result all Spam emails have detectable patterns. Many Spam filtering technologies try to evaluate these patterns to determine which emails are Spam and which are legitimate. Many Spam filtering technologies also use blacklists and whitelists to evaluate if emails are coming from legitimate sources. These blacklists and whitelists are updated by network administrators and automated systems that look for servers that generate large amounts of emails in short periods of time. Most filtering software rates incoming emails based on how likely they are to be Spam. Emails that are very likely get blocked and emails that are not likely get delivered. If the software is unsure, the emails may get blocked or tagged and delivered depending on the settings of the software.

Spam can be filtered on a recipient’s computer, directly on a mail server or by an ISP who provides email/Internet service (i.e. Yahoo, Comcast or Verizon). Filtering Spam on a recipient’s computer is less secure and less effective than filtering Spam directly on a server. The Spam still gets delivered to the end user’s computer and gets automatically filed into a local Junk folder. Filtering Spam on a server is usually more effective because the technologies employ more sophisticated filtering methodologies. If you filter on the server, software is installed on the server or on a machine in front of the mail server, which evaluates all incoming email and places suspect email in an online quarantine. Only legitimate email is forwarded to the end user.

Sometimes my legitimate emails do not get delivered! Why is this happening?

The growing problem of Spam has prompted many ISPs and network administrators to take action to limit the amount of Spam on their networks. Unfortunately in addition to limiting Spam, it also affects the reliable delivery of legitimate emails. A good example of this is Comcast. Comcast has opted to use a closed system of blacklists to limit who can send email on their networks. They blacklist computers and servers based on an undisclosed system for evaluating suspicious email behavior. Comcast does not publish who they have blacklisted or why they were blacklisted. As a result, many valid emails do not get delivered to Comcast recipients.

The Good News

The Internet is growing up! The Internet is based on an underlying communications and addressing protocol called TCP/IP (Transmission Control Protocol and Internet Protocol) version 4. The government and many colleges and universities have been developing a new version of TCP/IP called version 6. This new version has also been referred to in the media as Internet 2. The new version does not specifically address the problems with email but in general will support a much faster, more secure and larger Internet. The new structure of TCP/IPv6 will hopefully lead to greater accountability and improved email technologies.

Our Recommendation

Mantra Computing recommends using a hosted email security solution such as Mailprotector.net. A hosted solution provides a fixed monthly cost for a system that is always up-to-date and can handle the growing volumes of Spam and email without expensive upgrades and implementation costs. A good, hosted solution will constantly update their methods and technology to try and stay ahead of the Spammers’ evolving techniques. Good network managed Antivirus and Antispyware software is also critical to protecting one’s organization from the effects of viruses, Spam and Spyware.

Mantra Computing hopes this article provides a better understanding and appreciation for the Internet, how Internet email works and the problem of Spam. Mantra Computing will do its best to keep its clients apprised of the latest technologies and methods for maintaining your company's critical information technology infrastructure.

References:

Hosted Email Security Solutions:
-www.mailprotector.net (Available through Mantra Computing)
-www.postini.com
-www.spamcop.net

Local AntiSpam Solutions:
-CA Antispam 2007 (www.my-etrust.com) PC Only
-SpamSieve (www.c-command.com/spamsieve) Mac Only

Business Network Antivirus Solutions:
-Computer Associates eTrust r8 Antivirus
-Symantec Corp Edition Antivirus 10.1

Individual Antivirus Solutions:
-eTrust EZ Antivirus (www.my-etrust.com) PC Only
-Grisoft AVG Antivirus (www.grisoft.com) PC Only
-Avast Antivirus (www.avast.com) PC Only
-ClamXav (www.markallan.co.uk/clamXav) Mac Only

Business Network Antispyware solutions:
-Computer Associates ITM PestPatrol
-Webroot Spysweeper

Individual Antispyware solutions:
-Spybot Search & Destroy (www.safer-networking.org)
-Adaware (www.lavasoft.com)
-Webroot Spysweeper (www.webroot.com)
-CA Antispyware (www.my-etrust.com)