



Anti-Spam and Email Perimeter Defense

Updated June 2010

Anti-Spam and Email Perimeter Defense

Unsolicited Commercial Email (UCE), better known as “spam”, is an ever-increasing problem for all organizations that rely upon electronic messaging (email) for communications. Industry statistics show that over 80% of all emails transmitted over the Internet are UCE or spam. What this means to you as a user of email and to organizations worldwide, is that spam is not only a constant annoyance but there are real productivity and financial losses that occur because of spam. This document will highlight some of the primary causes of spam, techniques for filtering spam, best practices for managing email systems, and possible benefits of outsourcing email services for maximum protection and reliability.

What is “Spam”?

UCE or spam messages are primarily sent by both reputable and “less –than-reputable” organizations on the Internet for several reasons:

- 1) Advertising/selling of a product
- 2) Survey or gathering of survey information for legitimate use
- 3) Distributing computer virus, malware, or trojan software into your computer system for illegitimate use
- 4) Phishing or attempting to gather personal information or misdirect you to a web site posing as a legitimate company

The fundamental problem with UCE is that you cannot know which of the above motivations are behind each spam message, which messages are harmless, which are from a real company (such as your bank), and which messages are extremely harmful in some way to your computer or identity. For this reason, no spam or UCE should be trusted is the basic rule of thumb—no matter how much an email looks like it comes from your bank, as an example, you should not trust this and instead go directly to your bank’s web site via your web browser—and not by clicking on a hyperlink “conveniently” located within a questionable email.

Why Am I Receiving “Spam”?

In most cases, companies that generate spam messages purchased or “harvested” your email address amongst millions of other people’s addresses. Many of even the most respected web, social networking sites, product vendors, and online news sites share your email address with other companies who in turn may or may not have restrictions on who they share their lists with. Spammers purchase these email lists from legitimate companies or through illegitimate methods such as “harvesting” which may involve hacking a web site, watching or monitoring the Internet for email traffic that passes by, or by paying an employee of an other legitimate company to gain access to a customer email list.

Once your email address is “out there” and widely used by spammers, there is little you can do to stop the flood of spam so you need to look into filtering or stopping spam (see later section below). If it isn’t “too late” for you already, diligence on your part is necessary so that you do not to give out your legitimate email address to anyone you don’t trust. This means you should not use your work email address or even your primary home email address for anything you sign up for on the web—far too many legitimate companies capture and then share or sell email addresses. It is often best to have a secondary (or more) email address that you don’t normally check or read your emails. Whenever a web site requires you give them an email address, you this “non-primary” email address and let the web site send you their “confirmation email”. This way, you never really care who begins to spam you at this “throw away” email address—using a free email provider such as Yahoo or Gmail is a good choice for your “throw away” email account.

It is important to realize that even the most diligent person who “never” gives out their email address(es) can still get spam. One way this occurs is that spammers use a dictionary of words and common names. They basically send emails

to every John, Dave, Rickard, and Pamela hoping that someone with that email address will actually get the spam message and click on it.

Finally, spammers often “spoof” a legitimate email address so that they appear to be coming from a reputable company or person that you know—you may have even received a spam email before that seems to be addresses to you and was also *FROM* you as well. The reason spammers do this is that many companies or anti-spam filters often “always accept” messages that seem to be coming from known/internal users this the spam messages get right past any filtering.

Why Spam is Not Going to Stop Anytime Soon

Companies that make money by sending spam account for the majority of the “junk” emails you receive each day. These companies collect email addresses from web sites, surveys, and by purchasing lists from other companies. These companies live by the basic math that sounds something like this: if we send out 1 million spam messages a day, 3% of the recipients will open the spam email and 10% of those will click on a link within that email while 1% of the entire list will actually purchase something. These are not exact numbers but the point is that spammers can send out millions of emails per hour for just pennies yet there will be enough people opening, clicking on, and even purchasing the product to make it worth the spammers time and the company who hired the spammer to continue this business.

Spammers make millions upon millions of dollars a year in profit-and are often not located in the United States thus it is difficult to find and prosecute them. Though the United States and many other countries have improved laws banning UCE or spam, there are so many messages, each seeming to come from a different IP address on the Internet, that authorities can barely make a dent in the problem. Even more sophisticated computer systems are now being used by spammers so that the return email address, IP address, and country of origin are hidden, spoofed (fake), or just serialized so that “black listing” the spammer does no good since that email address/IP will never be used again.

How Do I Stop Receiving “Spam”?

This is the million-dollar question. There are a variety of software companies and services that promise to clean out spam or prevent it from reaching your mailbox. Most promise to catch 90-something percent of all incoming spam messages automatically but also have the ability for you to “white list” or “black list” messages or senders as you choose. White listing an email address ensures it will never get caught in a spam filter; however, be careful what you do here as white listing a national web site or newspaper (e.g. wsj.com=Wall Street Journal) which means that any email pretending to be from wsj.com, as in our example, will get through and this is also a common technique for spammers.

The most modern and sophisticated anti-spam systems incorporate three layers of security that is often labeled email defense.

- 1) **Email Perimeter Defense.** In this initial layer of defense, all incoming email data is scanned to determine which host server on the Internet is sending the email and if that server is a newly discovered system or a “trusted” source. If a new server or host comes online and begins sending emails identified as spam, worms, Trojan, viruses, denial of service attacks, or directory harvests, the perimeter defense system automatically throttles back the speed and number of messages accepted from this host. As the number of “bad” messages is maintained, the throttling back. The spammer sending emails will no longer be able to get their messages delivered and thus it is not economical for them to continue trying to send. Trusted servers or hosts that normally send legitimate email traffic are considered trusted and no throttling back of their data occurs. The key to success is that this trusted server list is shared across all other companies that use a particular email defense system so even if your individual network never saw spam from a specific host server, you are already protected as soon as another server discovered the harmful traffic.
- 2) **Anti-Spam Filtering.** Most anti-spam filtering systems use a combination of key words, heuristics, and behavior monitoring to determine what message are spam and what are legitimate. No system is 100% accurate and the higher the percentage of messages that are correctly identified as spam means you are also likely to have “false

positives” whereby legitimate emails get marked and quarantined as spam. More modern and advanced anti-spam systems don’t just look for key words anymore but instead have mathematical formulas to determine how many times a certain word is used, comparing this to the total number of words in the email, the “severity” of adult-oriented or inappropriate words, etc. Then a value is assigned to this “suspect” email which, depending on sensitivity levels, may or may not trigger the system to recognize this message as spam.

- 3) **Content Filtering.** Optional on some email defense services is content filtering. This is an additional layer that can be implemented to catch specific words, file types, or specific words found in an email or attachment. These content filtering rules can sometimes, depending on provider, be utilized for outbound message scanning as well to prevent internal users from sending sensitive corporate data containing certain words, phrases, watermarks, disclaimers, etc. Caution should be taken if you wish to use content filtering as these are simple rules—you may inadvertently block or mark legitimate email as spam.

Ultimately, messages marked as spam are either delivered to your email software’s “junk” email folder for your review, or are held at the anti-spam provider’s web site in a “quarantine” area for your review. It is always a good practice to occasionally review these emails to make sure legitimate email you have been waiting for isn’t accidentally caught in the spam filters.

Email Threats Beyond “Just Spam”

Beyond the annoyance, effort, and dollars spent trying to avoid spam, there are some threats to email systems even more heinous. These “perimeter” threats include computerized attacks and attempts to steal information from an email system by a spammer or hacker over the Internet. Computerized attacks can come in the form of a denial-of-service whereby the attacker sends enough data/traffic (often garbage or spam) at an email system that the anti-spam filters, network firewalls, or computers servers are just overwhelmed and are effectively put out of business/shut down. Other hackers can use highly-intricate attacks against firewalls or email servers to “harvest” or scan an email directory for valid names—by sending names into the email system and waiting for the system to come back with a positive or negative result if that email address actually exists or not.

Most casual or home computer users do not realize that every major corporation and email provider on the Internet spends tens of thousands, if not millions of dollars, each year trying to prevent and handle these types of “attacks”. These protections consist of one or more layers of networking hardware and software designed to catch, filter, or divert traffic at the perimeter of the network so that it does not get inside of the organizations internal network or computer servers. This “perimeter” protection is costly and requires constant monitoring; however, the potential damage caused by all of this traffic getting into the network is far worse.

Hosted Email and Anti-Spam Service Providers

As the quantity and complexity of attacks (spam or attacks against the perimeter network) increase, so does the cost and effort required to protect the networks, server farms, email systems, and ultimately the end-users. Most large hosted application and Internet providers leverage in-house and third-party companies that specialize in perimeter defense and anti-spam. The goal is to keep this complexity and “burden” away from the customer thus a hosted email service is often more about reliability and protection from threats and spam than just an email system by itself. As more and more corporations, small and large, use email as their primary means of communications, loss of denial of email services would be catastrophic for some. This is the reason for a continued increase in outsourcing corporate email systems to hosted messaging providers.

Hosted messaging providers have the network infrastructure, perimeter protection, firewalls, anti-spam systems, anti-virus systems, and redundant high-availability server farms capable of guaranteed email service availability beyond what an individual corporation could afford to deploy by themselves. The fact is that internal IT personnel within a corporation are just not specialized enough in messaging systems, email protection, backup/recovery, and ongoing high-

availability to keep up with the demands of a 99.99% always on and always ready email system. Due to the complexity of the leading enterprise email systems that now include group scheduling, collaboration, integration with corporate Intranets, and archiving/compliance needs, the need to outsource messaging systems to specialized hosted providers will steadily increase. The good news is that hosted message service providers are often less expensive than in-house email solutions but with far more reliability, protections, and features than most businesses can afford to install if they were to build an equivalent system in-house.

Finally, a key advantage to having an outsourced email defense/anti-spam provider is that over 90% of the email traffic sent via the Internet is spam or other unwanted traffic. By blocking this traffic at the outsourced provider, your computer network will only receive the 10%, in this example, legitimate data traffic which saves you hundreds, maybe even thousands, of dollars each month in bandwidth costs to your Internet provider.

Conclusion

There is no such thing as 100% accuracy with anti-spam systems nor will spam message stop being an annoyance anytime soon. The fundamental technology called SMTP (Simple Network Transfer Protocol) by which all Internet emails are sent includes the ability to spoof, fake, or hide the identity of a company sending emails to you—an average fifth grade student can probably do this on their home computer with little instruction/research.

We all need and use email systems and rely upon them more and more each day. Remember to keep your primary email addresses a closely guarded secret and always be careful what email you open on click on as it might not be from who you thought it was—it could even destroy your computer's data or lead to identity theft.

Always leave the protection of corporate email systems to the experts—whether your in-house IT staff or a third party hosted message provider, protecting email from attacks and spam is an ongoing battle with no true end in site. Laws and enforcement are insufficient to truly protect us so both the spammers/attackers and the legitimate users of email will be fundamentally at odds for the foreseeable future.

Best Practices

Finally, below are some best practices for both end-users and corporations to keep in mind on protecting your systems and filtering spam as best as possible.

- 1) **Use an anti-spam system or provider.** Whether an internal network appliance, software application, or hosted service, don't even think about using an email system for your organization without robust and proven protections in place.
- 2) **Don't forget perimeter protection.** Most anti-spam systems do not provide true "perimeter" protection at the edge of your network where it meets the Internet. If all the "bad" traffic enters your network and then you try to deal with it, you have already paid for the increased bandwidth/traffic and also likely overloaded your internal server farm trying to throw out bad traffic or potential denial-of-service attack. A third party hosted perimeter protection and anti-spam system is far better than anything most companies can afford to deploy internally in-house.
- 3) **Prevent your SMTP gateways and relay servers from accepting inbound email from the Internet.** If you can leverage a third-party hosted provider of perimeter and/or anti-spam filtering, you can then configure your email system SMTP gateways to accept email only from that provider. All traffic inbound to your network would be delivered (due to an MX record setting) to your hosted provider and the, after being filtered, forward to your SMTP gateways. You no longer pay for the 70-80% of emails that are spam or attempts at hacking that enter your SMTP gateways/network just so you can throw those packets of data away. That cost savings along may justify the price for the hosted perimeter/anti-spam or even completely outsourced email service.
- 4) **Never white list yourself.** Find alternatives to white listing your own company domain name and all your end-users within your anti-spam system. Most spammers "spoof" or fake the address of an email so that it appears

to come from your own company/email system—this is a technique to get past your spam filters.

- 5) **White list at user/department level only.** If you must white list an email domain to ensure that nothing gets quarantined, try to do so only at the end-user level or department level. This will keep the rest of the company from receiving potential spam from the email domain that the one user or department needed.
- 6) **White list any partner or marketing provider by IP address—not email domain name.** If you wish to guarantee emails sent from your partners or vendors skip your spam quarantine, you might be tempted to white list their email domain name. Instead, have them submit to you a list of their SMTP server IP addresses (e.g. 123.123.123.1) and program your anti-spam or perimeter defense systems to allow these. If you just allow their email domain name, spammers can easily (and often do) spoof that email address and would get right past your email protection systems.
- 7) **Prevent users from using third-party POP or IMAP email systems.** Whenever possible, try to prevent your end-users from using non-corporate email systems such as Hotmail, Yahoo, Google, etc. If they configure their local Outlook software to pull from these email systems, they are also pulling in spam and potential viruses, worms, etc. into your email environment and bypassing your perimeter and anti-spam systems. The same goes for users who program Google, for example, to forward a copy of their personal email to their corporate email system—they are exposing the corporate email system to additional traffic, spam, viruses, etc.
- 8) **Educate users on spam and using registering to web sites with their corporate email address.** The most valuable piece of Internet real estate, for a spammer to capture, is a valid email address for a real, live, human being. Corporations should remind their users to NOT use their corporate email address when signing up for web sites, subscriptions, etc. Many of these companies sell or share the email address which is then sold and traded all over the Internet. Using a secondary email address on a “free” system such as Hotmail, Yahoo, or Google, will go a long way to curbing the spam attempting to enter the corporate email environment.
- 9) **Not all Executive requests should be honored.** Users including Executives in the business, that demand an email domain name be white listed (or black listed for that matter) need to be informed that the ramifications of this change could affect the entire company. It is very common for IT personnel to “give in” to the requests of Executives demanding that “their emails” never get caught in a spam filter. Education (give them this white paper) is they key to helping them understand the ramifications of their request.
- 10) **Outsource email, anti-spam, and email protection.** The business of email protection, anti-spam, and provided enterprise class messaging systems is complex and yet continues to grow in popularity and criticality for most organizations. Certainly small but even large organizations can save money by outsourcing their email systems to a reliable hosted email service provider that has the 24x7 technical skills, customer service, network/perimeter security, anti-spam, anti-virus, and redundant/clustered server farms required for today’s modern messaging needs.