THE FIGHT

AGAINST SPAM

www.atmail.com

EXECUTIVE SUMMARY

Email is arguably one of the easiest ways to do business. Since the first email was sent on ARPANET in 1971[1], it's become the standardised working system. Email has been steadily increasing year after year, and in 1996 email had already overtaken snail mail in the United States. With this number increasingly on the rise, the days of criminals going through your mail slowly drifted away. However, they began targeting your email inbox instead of your mail box. These days, we refer to these types of attacks as spam or UCEs (Unsolicited Commercial Emails).

Spam is now growing faster than ever before. Email providers are racing to protect users from spam, while spammers are working out ways to get around the systems in place for to protect emails. Of the 196 billion emails sent every day, 64% are considered spam emails. This works out to be over 1,454,074 spam emails per second.

Although most spam emails are recognised by users, and either archived, deleted or reported as spam, quite a few users have believed spam emails to be genuine. A famous example was the '419' scam, where people were offered a large sum of money for a small up-front payment to obtain. Spammers target every inbox, regardless of who the user is. If you own an email address, you're going to get spam emails at some point

Phishing is also common among spam emails. What sets phishing emails apart is they will often be disguised as banking emails, PayPal emails or other service provider emails. These emails appear to be from a provider, but the purpose is to lure you to click on links to identify yourself or alert you of issues with your account. Once you click on these links you will be asked to fill in some personal details to confirm your identify. When you enter these personal details they will be sent to those running the phishing attack, giving them access to your Facebook login details, and larger issues like identify and bank fraud.

Spam is very damaging to both individuals and companies. Due to the increase in spam and phishing attacks, users are more exposed to receiving a virus on a device, becoming a victim of identify fraud or both. Although most people think of spam as the pesky ads that you sometimes see in your spam folder, the reality is often far worse and potentially a lot more damaging. spam and phishing attacks have become a business, where people are employed to trick users. They send spam in the hope that it lands in your inbox, that you click on the link, download the attachment or just open the attachment. Any or all of these things can lead to a virus, or worse. While spam also does contain pesky links that people usually ignore, they are increasingly more and more malicious as they can contain exploits aimed at infecting your computer and using your computer and email details to spread the infection to others.

With this in mind, it is absolutely critical that you configure your systems and utilise system tools to protect your business from spam.

1 http://en.wikipedia.org/wiki/Email#Email_networks

IMPLEMENTATION OF OPENSOURCE ANTI-SPAM ENGINES

Implementing anti-spam engines with your SMTP server is crucial in protecting your user base from spam and Phishing attacks. Anti-spam engines will reduce the delivery of spam as well as the chance that your accounts may be compromised and used to send spam. This means you're keeping your user base and business safe from potential attacks, and saving time and money in the process.

The use of anti-spam engines go beyond preventing spam from being delivered to your inbox or spam folder. They are a vital tool to protect accounts, devices and lots more.

IMPLEMENTATION OF OPENSOURCE ANTI-VIRUS WITH ANTI-SPAM ENGINE'S

More often than not if an anti-spam solution is in use, you will need an anti-virus engine to work with the anti-spam engine.

An anti-spam engine may stop you from receiving some spam. However, if spam is delivered with attachments, you may experience security breaches. These can be sent as attachments, links or within the email itself. Using an anti-virus engine to scan emails alongside an anti-spam engine allows you to reduce further risks to your business.

USE OF DNSBLS FOR ANTI-SPAM

DNSBL or RBL's (DNS Blackhole List or Realtime Blackhole List) are used to reject or mark emails as spam if the sending IPs or domains are included on these lists.

You can use DNSBL's within your SMTP daemon to reject/deny emails sent from servers that are on these lists or you can include DNSBL checks into your anti-spam engine to mark emails sent from servers on this list as spam.

The best practices for DNSBLs is to integrate them into your SMTP server's configuration during the HELO stage of SMTP. Doing so will reduce the load on your servers so that your systems don't have to process any more data from servers that are marked as.

Reliable DNSBLs should only be used for rejection at SMTP level. Reliable DNSBLs should be those that have no false positives, some of these include SpamCop, Spamhaus and Barracuda.

By using DNSBLs you're able to stop spam before it reaches your users, further reducing hardware usage overhead on processing emails. This frees your server up to process legitimate emails.

INBOUND & OUTBOUND SCANNING OF EMAILS

Scanning of emails internally is crucial to your daily operations as a business. This helps save time, resources and increases security.

A small but devastating issue, which is often overlooked by some mail administrators, is the scanning of outbound emails for spam.

By scanning your outbound emails, you reduce the risk of ending up on DNSBLs. If you're picking user accounts that are being compromised, by either a virus they have downloaded with a file by mistake or by weak passwords, you're minimising the risk of ending up on these lists.

Ending up on a DNSBL can cause a lot of issues for your own business when attempting to send emails. If you're on a DNSBL due to a compromised account, you will see many emails you attempt to send be rejected by the receiving server/s. Because of this, you run the risk of losing business and clients by not being able to reply to their emails or send emails to clients. While most DNSBLs will usually delist you for such things as compromised accounts once it is sorted out on your end, some may keep you listed for up to 4 weeks.

This is why scanning of emails should be done not only for inbound, but also outbound emails.

CUSTOMIZING YOUR ANTI-SPAM ENGINE'S RULES

You should update and customize your own spam rules in your anti-spam engine. You can do this by looking at the sort of spam you see in your own systems.

Customizations of spam filters are always a must, as anti-spam engines get smarter, so do the spammers. There will always be that one spam email that slips through your filters. Even with the improvements and modifications already discussed, you're bound to get some type of spam that may not end up being caught in your spam folder.

To get around this and aid yourself from being attacked with this sort of spam, that is often not yet picked up by global DNSBLs or spam filters, you're going to constantly need to have a customized ruleset to run on emails from your anti-spam engine. This can be as simple as including certain phrases to be marked with a spam score. This can be assessed by looking at the 'from' email, if the subject line contains a certain phrase, group of letters or all of the above.

In doing so you will notice that it picks up a lot of spam that not only was previously subverting your anti-spam engine but also increases the scores of a lot of emails that were already previously marked as spam.

Maintaining a customized anti-spam list can be hard at first, however, once you have it configured out it's unlikely that you will have to make many drastic changes more than once every few months.

COUNTRY BASED MAIL REPUTATION

While you're looking at creating, using or maintaining a customized anti-spam list you should consider country based email reputation.

For example, if your business is based in the United States and you only do business with companies or customers in The United States and Australia, the chance that an email coming to you from China or Russia being related to your business is very slim. This should be the first alarm bell.

If this is the case for your business, you can add rules that will mark emails originating from servers/IPs based in specific countries. This method should be used sparingly and not aggressively at all, if you score an email out of 10.0 where 10.0 and above is considered spam, consider setting the country based rules to 1.0. This will allow you to non-aggressively filter spam in ways that aid picking up emails as spam that may be new and unseen, meaning your anti-spam engine isn't looking for them.

CONTINUED IMPROVEMENTS

- Razor2, DCC, Pyzor. - Leverage global lists
- Auto banning scripts
- Mail queue monitoring

Although you've now set up your anti-spam engine, your Anti-Virus engine, DNSBL, implemented Inbound & Outbound scanning of emails, added a customized anti-spam list and added country based reputation filters, there's still always more to do.

Some continued improvements are to look at leveraging global lists such as Vipul's Razor (Razor2), DCC or Pyzor.

These lists collect spam that's sent and reported globally. Whoever is also running plugins can distribute updates and data they collect . These check phrases, URLs, sending addresses and sending mailservers that may not be on DNSBLs yet.

You can also consider using auto ban scripts to protect yourself. Using simple scripts to monitor your mail queues will help you spot suspicious activity on the system, and help you have the knowledge to ban or blacklist the account responsible. By blacklisting the account internally, these accounts will not be able to send emails from your servers, saving you a lot of time.

While you have your auto ban scripts set up and running, you can also leverage these to target inbound emails as well as outbound, creating your own sort of internal blacklist that can be dynamically updated by automated scripts running on your mail servers.

Using these tools in conjunction will greatly improve your arsenal in the war on spam.

IF YOU HAVE ANY QUESTIONS
OUR INBOX IS **ALWAYS OPEN.**

CONTACT US

GLOBAL HEADQUARTERS
atmail pty ltd
22/224 David Low Way
Peregian Beach, 4573
Queensland, Australia