

Email Security



Email is a critical communication component of almost every business. If you have any doubts, just turn off your email server for a couple of days and see how it affects **your** business.

If email is critical in your business then it's critical for you to protect your email system.

Protect it from what?

- SPAM
- Viruses
- Phishing
- Being Blacklisted

How can these be managed, monitored and rendered useless?

All security solutions must be monitored, modified and managed. Many security experts have made the statement, "*Security isn't a destination it's a journey.*"

What does the journey involve?

Let's look at each threat.

SPAM

The various methods used in The BOX to prevent SPAM are:

- Bayesian filtering
- List of valid email addresses
- Country of origin
- Invalid Reverse DNS
- Reported SPAM source

Many methods have been developed to reduce SPAM. The BOX uses "best of breed" in all open source code. Every client is different and therefore requires a custom package to suit their needs.

We incorporate **Bayesian filtering** in a managed mode. Bayesian filtering involves breaking an email message apart into "tokens". These tokens are words, groups of words, phrases and number of occurrences of each.

Statistical calculations are performed on these tokens for both SPAM and HAM (legitimate email) messages. The accuracy in identifying both SPAM and HAM is dependent upon how many messages in each category used in the calculations. We have each client's emails copied to our servers where we have people scan through the messages, move the SPAM into a separate folder from the HAM and then perform the Bayesian calculations on each.

This creates a database of tokens which is then copied to the client's appliance for further monitoring.

The BOX also uses a **list of valid email addresses** for the specific client. As each message is received it's first checked against the list of valid recipient email addresses. If the incoming message isn't addressed to a valid email recipient, why bother with further analysis? – it's not wanted and it gets rejected back to the sender. Many email servers will accept the message but have no where to deliver it so it sits in the undeliverable folder.

This specific filter doesn't catch a lot of SPAM but it is another affective use of an easily implemented method. In many cases, it also provides us with new sources of SPAM. If you don't have an email address for "info@" and you're getting email to that address, it could probably be someone trying to send SPAM to you. We record the origination of these messages and track them down. If they are "bogus" we'll report them and add them to your blocklist as well as the blocklist of all BOXes.

What happens when a new employee is hired or an existing employee leaves?

You call us. We'll make the changes for you.

The BOX blocks SPAM by **Country of origin**.

If you're a local business, one that does business with people local to you or just in your country of origin, do you need to allow emails from other countries? Or do you need to allow email from the entire world?

Many reports show that approximately 50% of SPAM originates in the US, but again, if you can block 50% of SPAM by not allowing email from other countries, why not?

The experience of our clients has showed different statistics than what many reports show. Our clients show that around 80% of SPAM is sent from countries outside the US.

Our appliance downloads updates of country IP addresses every night from the sources of these IP addresses. It is then sorted by what countries you want to receive email from and all others are logged and blocked.

Invalid Reverse DNS is a bit more tedious to manage. As each message is received by The BOX, the IP address of its origin is checked against the domain name. If they don't match, it's rejected.

A good example is if someone sends you an email and it appears to be sent from e-Based Security, LLC. The BOX will check the DNS record for ebasedsecurity.com to see what the IP address is for our mail server. If the source IP address of the email sent to you does not match the DNS records, it gets bounced.

This is more tedious to manage because there are many email servers out there with improperly configured DNS records. We can fix that, but it does require work on our part. We constantly scan your email logs. When we see an email that gets rejected by an Invalid Reverse DNS record, we manually review the message to see if it looks legitimate. If it is, we'll contact the sender and work with them to correct their DNS record.

If your BOX receives an email message from a "hacked" PC that is being used to send SPAM (very common these days) and it claims it's from eBay, the Invalid Reverse DNS checking will block that message.

Our philosophy is that this is such an effective method of controlling SPAM that it's actually worth the extra time and effort. In addition, imagine all the other email servers we're helping by getting their DNS records straight.

The last method used by The BOX is using **Reported SPAM source**. There are web sites that collect information from reporting sources all across the world on where SPAM is originating. As each message is received by The BOX, its origin is checked against these lists of reported SPAM. If the IP address of the origin of a message is found in one of these lists, the message gets bounced back to the sender. These blacklists are updated so frequently that it would be impossible to keep a list like this on The BOX. Each message is actually broken apart and the source IP address is checked against the list over the Internet. This does create some latency but we're talking seconds not minutes or hours.

The BOX contributes to these lists. As we positively identify SPAM we notify certain sites as to the source IP address and they update their lists.

If you receive a call from someone saying their message to you was bounced back to them, simply call us and we'll work with them to get it rectified. We may have to help them get their domain "unlisted" from one of these

blacklists, we may have to help them correct their DNS entries, or sometimes we just have to make sure they typed your name correctly. In any case, it's our job and we do it well.

VIRUSES

The second threat to email is viruses. The BOX relies on scans all emails coming into your email server for viruses and phishing emails.

As a small business, your email server is probably also on your main server – your only server. This means it performs other functions other than just providing email.

The more you ask of this server, the more resources it requires. If you can process the “nasty” stuff before it gets to your server, you'll save the resources for its other functions – providing files, buffering print jobs, etc.

The BOX uses ClamAV for all virus prevention. ClamAV is updated by the masses of open source supporters.

One critical area for any anti-virus software is the time between when a new virus is detected and when the software company releases a new signature. This is one area that ClamAV really shines.

It is typically considered one of the first to release new signatures after a new virus is detected. The BOX is configured to automatically check for new virus definitions every 15 minutes. You don't have to change a thing.

With The Box checking emails **before** they get into your network, the anti-virus software on your PCs will have to do very little work. They become the secondary line of defense rather than the one and only.

PHISHING

Phishing emails are designed to trick the user into visiting a web site where they'll be asked to provide bank login information, PayPal or eBay information or some other form of identification credentials.

The idea is that you receive an email that in every way appears legitimate. Even the web site you're directed to looks legitimate. It may contain a statement that suspicious activity has been detected on your account and you should login to verify the activity before they suspend your account.

The message will typically contain some sense of urgency.

If you were to login through their link, your information would be stolen and probably sold in the black market.

Because these emails are sent in large quantities to a variety of email addresses, they are also classified in many of the same methods as SPAM or viruses.

Signatures can be developed for phishing emails. We work with reliable sources for these signatures – they provide us updates and we provide them with samples of new phishing emails we've discovered through our network of clients.

In phishing scams there are two levels to protect against – blocking the original email luring you to the bogus web site, and discovering the web site and working with people to take it off-line.

All the techniques we use in filtering out SPAM also contribute to blocking these phishing emails in addition to the signatures we use.

Often times these emails are sent from already compromised systems – PCs under the control of the hacker. The websites they use are also often times a compromised system – many times right here in the good old United States of America.

That's right.

Small business owners often think these nefarious people operate exclusively in foreign countries however our research indicates that many of the attacks are from systems in the US. The attacker may be in a foreign country but the systems they've compromised are right here and that's where they launch their attack from.

BLACKLISTED

Being blacklisted results if one of your systems is used to send SPAM. If one of your PCs is compromised and used to send SPAM, it will be detected by someone and reported. Once it has been reported your domain will appear on one or more blacklists.

These blacklists are used by organizations to assist in identifying SPAM. We use them on The BOX.

When you appear on a blacklist, any organization using that blacklist will not be able to receive email from you. You can get your name removed however, it will require some time.

How long can you afford to be without email?

And what will your customers think of you when they realize you didn't take the necessary precautions to prevent being blacklisted?

By preventing any email out of your network unless it's from your email server, you will drastically reduce the chances of your domain appearing on any blacklist. That is how The BOX keeps you off of blacklists.

Now you see the dangers of each of these methods and how The BOX acts as your defense against them.

The BOX – designed specifically for small business owners.

Visit: <http://www.ebasedsecurity.com> to learn more. Or call, 1-866-838-6108