

# 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**

Why is SPAM a threat to the security of your small business?

SPAM uses system resources. We're not going to jam all sorts of non-applicable statistics down your throat. Many people quote the dollars wasted in manually handling SPAM – whether or not this applies to you as a small business owner is not our decision. Manually handling SPAM does waste time. What that time is worth to you is up to you to figure out. We do know that many of customers tell us they save at least one week a year by not manually handling SPAM.

SPAM is often used as a method of infection. If the SPAM message is clever enough to trick a user into visiting an infectious web page, or to open a "safe looking" attachment, it could very well infect that system. Once that system is infected it will try to infect all systems it can find – starting with the other systems in your network.

## **VIRUSES**

The second threat to email is viruses. The BOX 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.

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.

Viruses come and go in waves. Sometimes it appears as if they’re fading away and at other times they seem to be spreading all over the Internet. Either way, you need to be protected by more than one layer of virus defense. As a small business owner you could buy yet another anti-virus software package and have it installed on all your PCs or you could use a security appliance that is automatically updated every 15 minutes, monitored by us, and get back to running your business.

## **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