STOP SPAM.
SAVE TIME.

SPAM TITAN

SPAM FILTERING ESSENTIALS **CHECKLIST**

No matter which email server or spam filter you are using, the following should be helpful in reducing spam and related malware attacks on your network.

1. Use an RBL
2. Set your server to require correct SMTP handshake protocols
3. Use Recipient Verification (RV) to reject email to non-existent addresses
4. Block dangerous attachment types
5. Scan for viruses
6. Make sure that any urls in the email body are safe
7. Use a regularly updated spam pattern library
8. Use Baysian filtering
9. Set the appropriate spam score for your organisation
10. Enable end user spam feedback
11. Train your end users to prevent infections

1. Use an RBL

Your first line of defence, whether or not you have a spam filter, is to use a Realtime Block List (RBL) provider to reject any email from known spam servers. This alone will reduce spam email by 70-90%, depending on your industry. This will reduce the load on your email server or spam filter, as well as your network, as the email is rejected before it is downloaded. **This could save you significant bandwidth**. We recommend using zen.spamhaus.org as it is the most up to date, with best spam blocking and lowest false positive rate. Setting up your email server or spam filter to use an RBL should only take you a few minutes.

2. Set your server to require correct SMTP handshake protocols

If you make sure that only email using correct SMTP is accepted, you'll block most spambots. Ensure that you require HELO (EHLO) with a Fully Qualified Domain Name and preferably a resolvable hostname too. As with using an RBL, this check is done prior to accepting the email, so it will reduce load on your spam filter, email server, and network. This will only take a few minutes to configure in your email server or spam filter.

Note: Individual organisations may occasionally need to whitelist suppliers or customer with incorrectly configured email servers to allow their email to be accepted. This will work to significantly reduce spam for individual organisations, but may not be appropriate for IPS's and MSP's.

3. Use Recipient Verification (RV) to reject email to non-existent addresses

Spammers often send email to a range of possible email addresses such as admin@, info@, and may also use a dictionary of names to get email into individuals email inboxes. Reject email that is not addressed to genuine email addresses, by either uploading your valid email addresses as a csv to your mail server or spam filter, or using Microsoft Active Directory integration if possible.

Again, as with using an RBL and SMTP handshakes above, **RV prevents the email being downloaded, saving you bandwidth, and reducing load on your email server and network**. This may take a little longer to implement if you need to get your valid list of email addresses, convert them into CSV format, and upload them to your email server or spam filter, but it will be worth the effort due to the amount of spam it will block.

Note that all 3 of these solutions complement each other, and can be implemented on most email servers, even without having a spam filter. If you are not using these, you are wasting your bandwidth, opening your network to unnecessary risk, and causing yourself a lot of wasted time and effort dealing with the effects of spam - such as the cryptolocker virus for example. Make half an hour this week to implement these 3 and you will probably save yourself weeks of work over the next year.

The rest of the steps here are only relevant if you have a spam filter (commercial or open source, on site or in the cloud).

4. Block dangerous attachment types

Very few organisations ever need to have .exe files delivered via email. Block them, and in the few cases where they are required, create an alternative method of delivery that ensures safety with the minimum of bureaucracy. **Make sure that you are blocking by MIME type, not file extension, as very few spammers will use the actual exe file extension**, but will disguise the payload file as a pdf, image, spreadsheet or doc.

5. Scan for viruses

If you don't have a spam filter, you need to have very good end point anti-virus protection in place. If you do have a spam filter, **make sure you are using the anti-virus scanning, and that the AV engine and signatures are up to date**. Most spam filters will allow you to automate and set the update frequency. My personal opinion is that if you have AV in your spam filter; use a different AV for endpoint protection, to get the benefit of redundancy. No matter how small the benefit of having different engines is, it still beats having all your eggs in one basket. You need to have endpoint AV, and the market for spam filters and AV endpoint is diverse and competitive enough that you will not be paying a premium to use 2 suppliers. Of course, YMMV, so please feel free to share your opinion in the comments!

6. Make sure that any urls in the email body are safe ❑

Use URIBL and SURBL to check that urls in the body of the email are not known malware or phishing websites.

7. Use a regularly updated spam pattern library ❑

Most spam engines will have this built in, and usually not configurable. This is where a significant amount of spam is captured, based on a large database of recent and historical spam, provided by the spam fighting community. **Spam Assassin is an excellent resource for accurate, up to date spam signatures**.

8. Use Baysian filtering ❑

Most spam engines use a Bayes engine (Bayes was a statistician, and his methods are widely used for classification - in this case: spam vs ham) which is trained to recognise spam. **Incoming email is scored based on the spam pattern library, bad attachments, bad links, and end user feedback** (the "Spam" or "Junk" button in the email client). The Bayes engine then learns to recognise new spam, and also to forget old spam patterns that might now block legitimate emails.

9. Set the appropriate spam score for your organisation ❑

Most spam filters will give an incoming email a score, based on the content and attachments. It is up to you, the systems administrator, to decide the right spam score threshold for your organisation. This is something that takes a little trial and error to get right, but usually only needs to be done during the first week or two after deployment.

Your spam filter providers should give you a trial period to validate that you can get this right for your organisation, and help you configure their spam filter to get the optimum block rate and minimum false positive rate possible with their product. Make use of your free trial period to ensure your get this working - it will be your head that rolls if you go ahead with purchasing a license because of bells and whistles rather than actual spam blocking performance - that every member of your organisation will measure every time they open their email inbox. You have been warned!

10. Enable end user spam feedback ❑

Provide a way for your end users to improve your Bayes engine, by manually tagging any spam that gets through your filter as "Spam" or "Junk", and also for correcting false positives.

11. Train your end users to prevent infections ❑

A good email usage policy, that teaches and warns of the risks and consequences of spam, malware, viruses and phishing, gives your end users the knowledge they need to help catch the remaining few scams that get through. This alone could save your organisation from financial ruin - it is so important I almost made it #1 on the list, particularly because so many sysadmins give this little attention.

There is a lot of negative sentiment about "users" and how the sysadmin's job is to protect them from themselves. Instead of giving up on them as a lost cause, **equip them with the armour and ammunition they need to join you in protecting their data**. Use the big bad crytolocker virus as a scare tactic if needs be - but make sure that everyone knows the potential risks in clicking a link in an email, and to be suspicious of any email from the bank (or any other organisation critical to your business) asking for details they should already have (like usernames, passwords, account numbers, social security numbers, etc.).

If you provide the tools and they are not used, you at least have a leg to stand on when the crud hits the fan. "I told you so" is not much use once the business is bankrupt, but at least your career will not end with the company if you did everything you could reasonably be expected to do to protect the network and prevent intruders entry.

Good luck in your continued fight to end cybercrime!