SPAMHAUS
KNOW HOW
<DNS_blocklists/>

Spamhaus Know How eBook

Get to know DNS Blocklists

SPAMHAUS

Contents

DNSBL
IP
DOMAINS

1
0 1
1 0

rDNS
DKIM
DNSBL
SMTP
DNS
PTR
SPF

BLACKHOLE
DNSBL
BLOCKLISTS
REAL TIME BLACKHOLE LIST

Foreword

Written by Simon Forster

Foreword

Written by Simon Forster

Some say that email is losing its relevance. I don't deny that the way email is used has altered over the years. However, today I consider it an invaluable business tool and worth protecting more carefully than ever.

Fifteen years ago, email was used for the more trivial, sending jokes and pictures of cats alongside basic business communications. Fast forward to today, and email is now a serious business tool.

Frivolous and day to day online exchanges are increasingly shared via social media and instant messaging. However, these applications are ephemeral, whereas email is more "sticky"; there is greater proof of its existence.

I would go as far as saying that email has replaced the old fashioned letter as the preferred business correspondence. Consider how your bank, facility providers, and even solicitors communicate? Usually, it's via email. Business agreements and contracts, along with order confirmations, invoices, and of course, marketing materials, all use email as their preferred medium.

Email is a serious business application. This makes protecting your email traffic and data more critical than ever before. Protection isn't solely about rejecting email-borne threats before they enter your infrastructure. It is also about ensuring the data within your email stream is kept private and confidential, not open to any third party's prying eyes.

> "Email is a serious business application. This makes protecting your email traffic and data more critical than ever before."

With this in mind, email infrastructure decisions, including hosting, management, and security, are all key considerations to ensure this precious business asset continues to deliver successfully.

This eBook provides some considerations and helpful tips for those areas mentioned above.

Happy reading.

Simon Forster, CEO

Six advantages to running your own mail server

Written by Natale Bianchi

Six advantages to running your own mail server

Written by Natale Bianchi

Running your own email server is so 1995, right? Why would anyone go to all that trouble when you can outsource email to a third party and let them manage it? Let's STOP a moment, and before we (and our precious data) all merrily rush off to third party providers, let's consider some of the advantages of managing your own email infrastructure.

1 Your email stream can be customized to fit your exact business needs

No industry or company is the same. We all have different ways of working, and that includes different risk profiles. A medical facility will have an entirely different security posture to that of a high street retailer. One size does not fit all!

To meet the specific requirements of your company's risk profile, you can customize your email stream. For instance, you can adjust your spam filters to aggressively block countries from which you never receive email or guarantee acceptance for messages matching specific patterns, commonly known as whitelisting.

2 You bear the responsibility for keeping data private and confidential

You may be questioning whether you want this burden. Nonetheless, data is a precious asset, and your company's email stream is part of that asset. There have been plenty of stories over recent years of data harvesting, including the Facebook data privacy scandal.

> “We've observed cases in the past where a provider's terms and conditions allowed it to search the content of their customer's emails to aid in targeting adverts!”

When an email is in transit, it will have end-to-end encryption, no matter if you manage your own email infrastructure or outsource it to a third party. However, when that email is sitting on a server, having been delivered, it is unencrypted. This leaves it open to inspection by a third party, should they make it their mission to do so.

We've observed cases in the past where a provider's terms and conditions allowed it to search the content of their customer's emails to aid in targeting adverts!

A security breach excepted, if you're running your own email server, your emails' content can't be accessed by any other entity.

Six advantages to running your own mail server (continued)

Written by Natale Bianchi

3 You will have tighter control over your data

If you outsource your email, the data may become subject to the regulations of the country your provider is based in. For example, if your provider is situated in the USA, and the USA government requires your data to be shared, your provider will have to hand it over.

We're not saying that other countries' governments won't approach you to get their hands on your data if they require it, but you will have a greater awareness and control over what happens.

4 You are responsible for your own destiny… including service levels

Outages happen – it's a fact we're all aware of. Not so long ago, Microsoft suffered service issues that affected users across the globe for hours. Not having control of situations like this can be challenging. However, if you are directly responsible for your email infrastructure, you have direct control. You are in charge of your own destiny.

5 Other people's poor sending practices won't negatively impact you

Even if you have the best emailing practices in the world, if your email is being hosted on the same email server as an organization that is spewing out spam and other malicious emails, there is a chance that you may get listed on a blocklist.

This chance increases significantly if the provider managing that email server is slow to respond to abuse reports and allows dubious organizations to continue operating on their network, causing reputation to plummet.

> “At one point or another, we've all experienced frustration when trying to resolve a business-critical issue via a help or support desk. Either response times are slow or technical knowledge can be lacking.”

6 You won't be at the behest of a support desk when dealing with issues

“Hold the line, reader. We are currently experiencing high levels of calls. Your call is important to us and will be answered…in forty minutes.” At one point or another, we've all experienced frustration when trying to resolve a business-critical issue via a help or support desk. Either response times are slow or technical knowledge can be lacking.

If you run your own mail server, you'll be able to remediate failed message deliveries and other related issues rapidly. Particularly useful is the ability to look at the reasons behind false positives and fix them immediately.

Should everyone be managing their own mail servers?

No! We understand that managing your own email infrastructure isn't for everyone. Indeed, where email servers aren't correctly set-up, multiple problems can arise, including security and deliverability issues.

Six advantages to running your own mail server (continued)

Written by Natale Bianchi

However, we believe that IT teams and those at an Executive level need to make careful considerations as to how they manage their email, including the advantages of bringing it back in-house. If this is something you're looking to do, or already doing, read our top tips for running your own email server sharing simple actions to make this a success.

> “We're not saying that other countries' governments won't approach you to get their hands on your data if they require it, but you will have a greater awareness and control over what happens.”

Top tips for running your mail server

Written by Carel Bitter

Top tips for running your mail server

Written by Carel Bitter

There's much to be said for running your own mail server: privacy, flexibility and being in control of your own destiny; these are all good things. On the flip side, there's usually a bit more to it than just installing a software package and clicking the Go! button.

Have a valid reverse DNS set-up for your mail server

This is the most basic requirement to get your email accepted anywhere. Ideally the value of the reverse points back to the IP, so the DNS matches both forwards and in reverse.

Get a dedicated IP address for your mail server & limit the use of port 25

If you have end-user devices on your network IP which are compromised, spambots can spew out spam via your network to external sources. Having a dedicated mail server on a different IP with Port 25 restricted limits spam being emitted by these compromised machines.

Make sure potentially compromised end-user devices and regular NAT'ed traffic towards the internet do not use the same outbound IP address as the mail server, as this may negatively impact email deliverability.

Why restrict port 25?

Port 25 is the channel designated for sending email. By restricting this port, you force email to go through dedicated outbound mail-servers instead of direct-to-mx. Read how it helped Amazon Web Services.

Route ALL email traffic through your mail servers

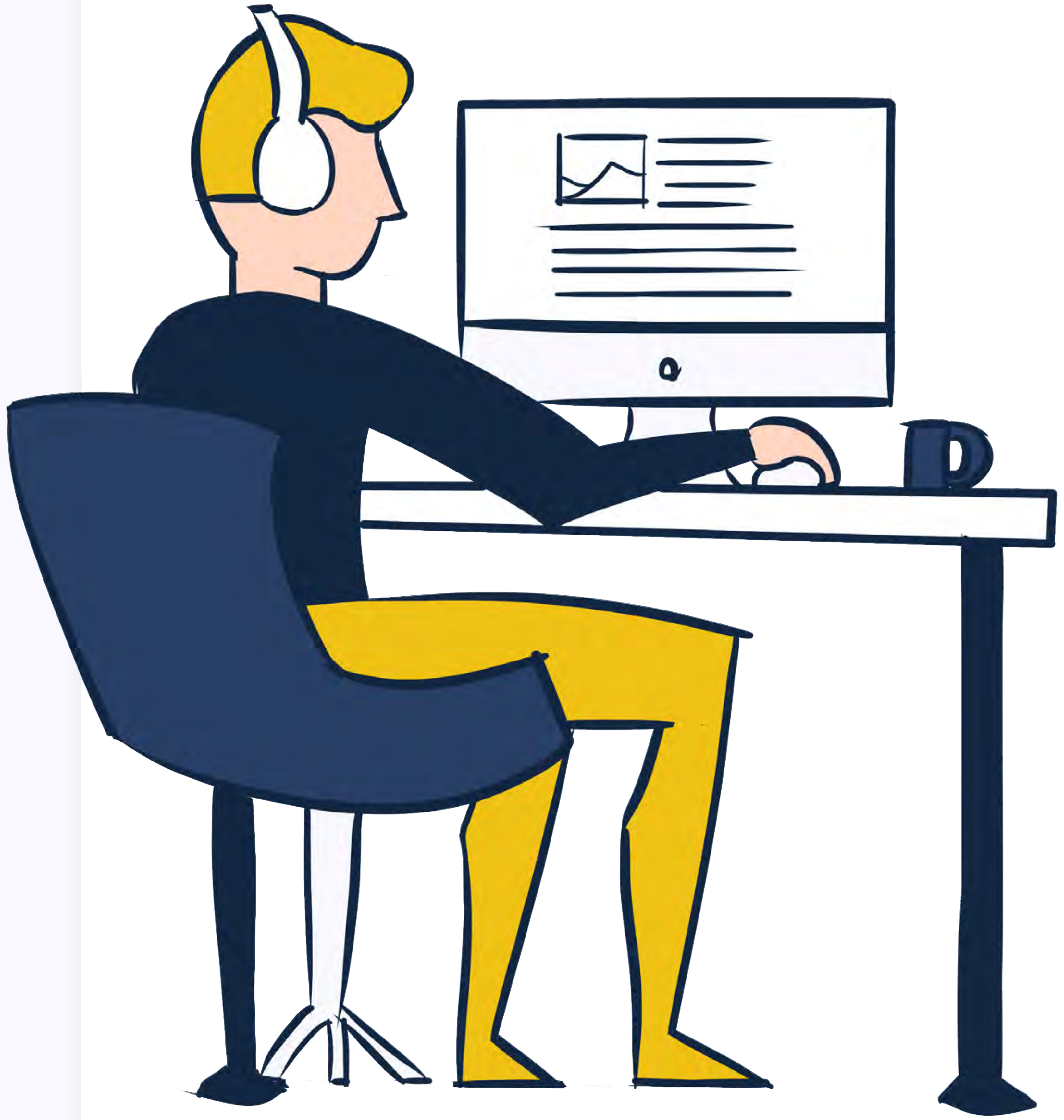
Email can come from servers or printers etc. in addition to email clients. Routing all of email traffic through your mail server means that you know what is being sent and where.

Reject as many malicious emails at the initial email connection and SMTP connect

Not only does this mean that the sender is immediately notified of a failed delivery, but you will stop vast amounts of spam and other email-borne threats before you download the header and body of the email. This saves on expensive content scanning.

Top tips for running your mail server

Written by Carel Bitter



Deploy email authentication

Miscreants can use domains they don't own, when they send malicious emails. To limit damage caused by this behavior, use Sender Policy Framework **(SPF)**, DomainKeys Identified Mail **(DKIM)**, and Domain-based Message Authentication, Reporting & Conformance **(DMARC)** standards

Sender Policy Framework (SPF) Set up this record in your DNS, limiting the IP addresses that are allowed to send for your domain.

DomainKeys Identified Mail (DKIM)
Through a DNS look-up to a public key, DKIM verifies that an email claiming to be from a domain is authorized by the domain owner to send from it.

Domain-based Message Authentication, Reporting & Conformance (DMARC)
Set this up to resolve issues for the receiver if SPF or DKIM don't verify.

Use the same domain name for forward and reverse DNS, and all authentication

Repeated use of the same domain name throughout set-up clearly shows the receiver that your communities are legitimate, and not those of an imposter.

Choose your domain wisely, correctly utilizing subdomains

Your domain's reputation will be taken into account when determining how a receiver treats a message, ensure you do everything possible to improve or maintain a positive reputation.

Always deploy robust email filtering practices.

Follow best practices for filtering email. Layer email filtering processes, using the most economical and effective process at the top of the stack to reduce as much unwanted email as possible, before using more expensive and resource heavy processes on the remaining emails.

DNS blocklist basics

Written by Matt Stith

DNS blocklist basics

Written by Matt Stith

You're running your own email infrastructure, or at least considering it, but how should email filtering be handled? What is your first line of defense against the spam and malicious emails that will bombard your mail server?

What is a blocklist?

The name gives it away; it's a list, or more accurately, a database containing IP addresses, domains, or hashes. These lists are compiled by specialist research teams, who have observed the listed internet resources to either be:

a Directly involved in malicious behavior, e.g., sending spam, distributing malware, hosting botnets, hosting phishing websites, etc., or

b Having a bad reputation associated with them.

Presented in a DNS zone, blocklists can be utilized by anyone managing their own email infrastructure. Fundamentally there are three stages where you should be using DNSBLs:

1. Initial set-up of an email connection against the connecting IP address
2. During the Simple Mail Transfer Protocol (SMTP) connect
3. Content filtering stage, once the email data has been transmitted.

What's in a name?

What's the right term to use? "Blacklists," "blackhole lists," "domain name system blocklists," or "real-time blocklists"? The answer is....all of the above (and probably more). We use the term DNSBL and blocklist.

How are blocklists compiled?

It all starts with data. Vast quantities of data. In fact, Spamhaus was dealing with 'big data' before 'big-data' became the buzzword we know it as today.

The industry and beyond shares data with Spamhaus, from hosting companies to Internet Service Providers (ISPs) and internet governing bodies. Of course, in addition to this Spamhaus runs its own spam traps and honeypots.

Through manual investigations, machine learning, and heuristics, our researchers analyze this data to see if it meets pre-defined policies for listing.

DNS blocklist basics

Written by Matt Stith

How much data is processed to produce blocklists?

Track
3 million domains assessed
18,000 malware samples processed

Analyze
13.4 billion SMTP connections analyzed daily

Score
100's of heuristics are used to identify the safe from the potentially malicious

List
12 million botnet nodes listed daily

Protect
3 billion+ mailboxes are protected

How are the policies defined?

Before curating a DNSBL, Spamhaus decides on the criteria the IP, domain, or email content must meet for it to be listed. These criteria are referred to as "policies."

Needless to say, these policies aren't plucked out of thin air. Instead, they are formed in consultation with the wider internet industry (both senders and receivers) to ensure they are fit for purpose and meet internet users' needs.

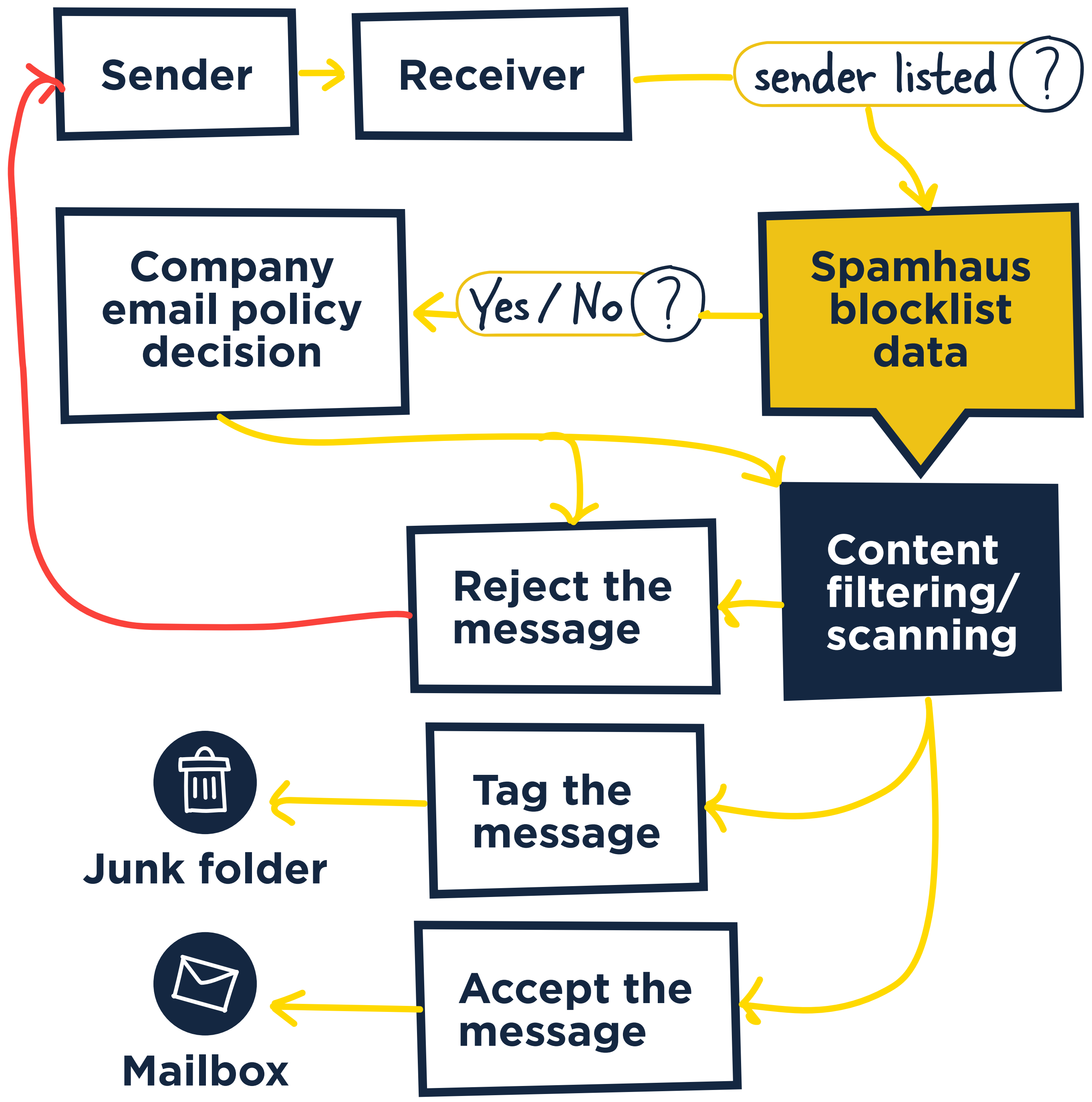
How blocklists work

The IPs, domains, or hashes associated with an email can be queried against a DNSBL to see if they're listed. As someone managing the email infrastructure, it's down to you to decide how to handle that potentially malicious email.
You can either:

a) Reject the email in real-time, with an appropriate delivery code, or

b) Accept the message and tag it for additional filtering.

Read Understanding the source code of a malicious email to understand why certain parts of an email's source code have specific blocklists applied to them. What blocklists are available?



DNS blocklist basics

Written by Matt Stith

What blocklists are available?

Here's a quick overview of the types of blocklists produced by Spamhaus:

Spamhaus Blocklist (SBL) – IP addresses observed to be involved in numerous activities including sending spam, snowshoe spamming, botnet command & controllers alongside hijacked IP space.

eXploits Blocklist (XBL) – Individual IPs (/32s) that are infected with malware, worms, and Trojans etc. This list prevents mail servers from accepting connections from compromised computing devices.

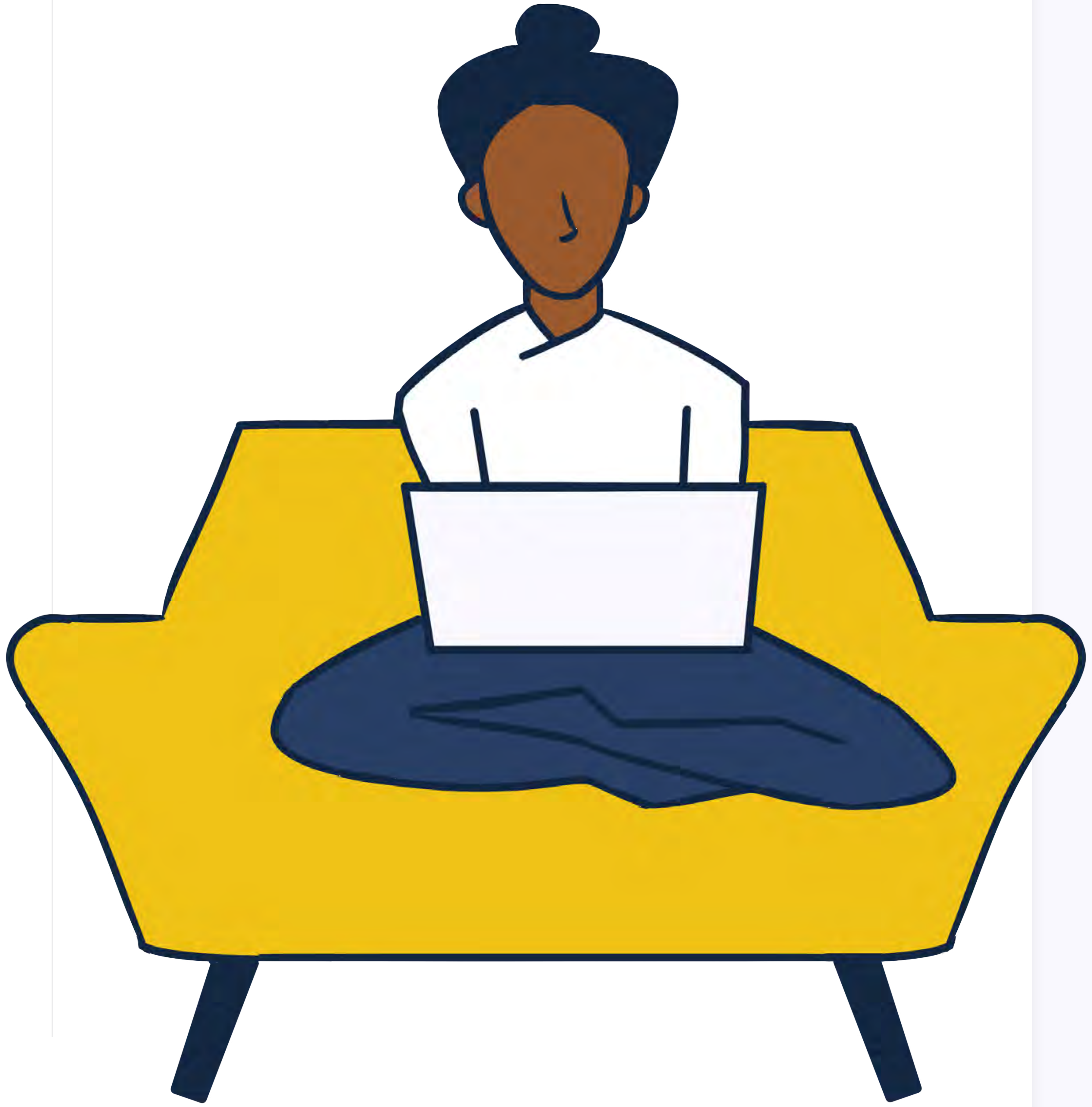
Policy Blocklist (PBL) – IP addresses that shouldn't be sending email e.g. internet of things (IoT) devices. Spamhaus works together with the industry, enabling IP owners to list and manage their own ranges for your safety.

Auth Blocklist (AuthBL) – IP addresses know to host bots using brute force or stolen SMTP-AUTH credentials to send malicious emails.

Domain Blocklist (DBL) – Domains owned by spammers, being used for nefarious purposes. We also list domains that are legitimate but have been hacked by bad actors and are being used with malicious intent.

Zero Reputation Domains (ZRD) – Domains that have been registered in the past 24 hours – helping you filter email from cybercriminals who register, and immediately use multiple domains on a daily basis.

Hash Blocklists (HBL) – A content blocklist that uses cryptographic hashes to list email addresses, cryptowallet addresses, and malware files.



Trial our DNSBLs for free

www.spamhaus.com/free-trial/free-trial-for-data-query-service/