guide

Our Email Deliverability Essentials Guide

spotler

Our Email Deliverability Essentials Guide
Introduction

HERE IN THE UK, WE ARE LUCKY AS EMAIL MARKETERS. ACCORDING TO RETURN PATH'S 2016 BENCHMARK REPORT, WE SAW OUR MESSAGES DELIVERED TO THE INBOX 88% OF THE TIME WITH ONLY A DIP IN Q4 OF 2015 AND Q1 OF 2016. BUT WHAT ABOUT THE REMAINING 12%? HOW CAN WE IMPROVE OUR EMAIL DELIVERABILITY EVEN FURTHER?

There are a number of elements that can affect your email's ability to get into the right inbox. For the purpose of this guide, we will focus on the essentials – IP addresses, domains and infrastructure considerations.

Contents

How your IP address & domain affect deliverability

Similar to a postcode, your IP address is a unique number listed in the domain name system that sends mail on behalf of your domain name. It exists to help identify each computer using the Internet to communicate over a network.

Why is your IP address so important?

The source of an email is one of the main considerations mailboxes take into consideration when filtering email messages. The two components that make up that source are the IP address and domain. So if the reputation of your IP address is damaged, chances are you won't make it to the inbox.

Types of IP addresses

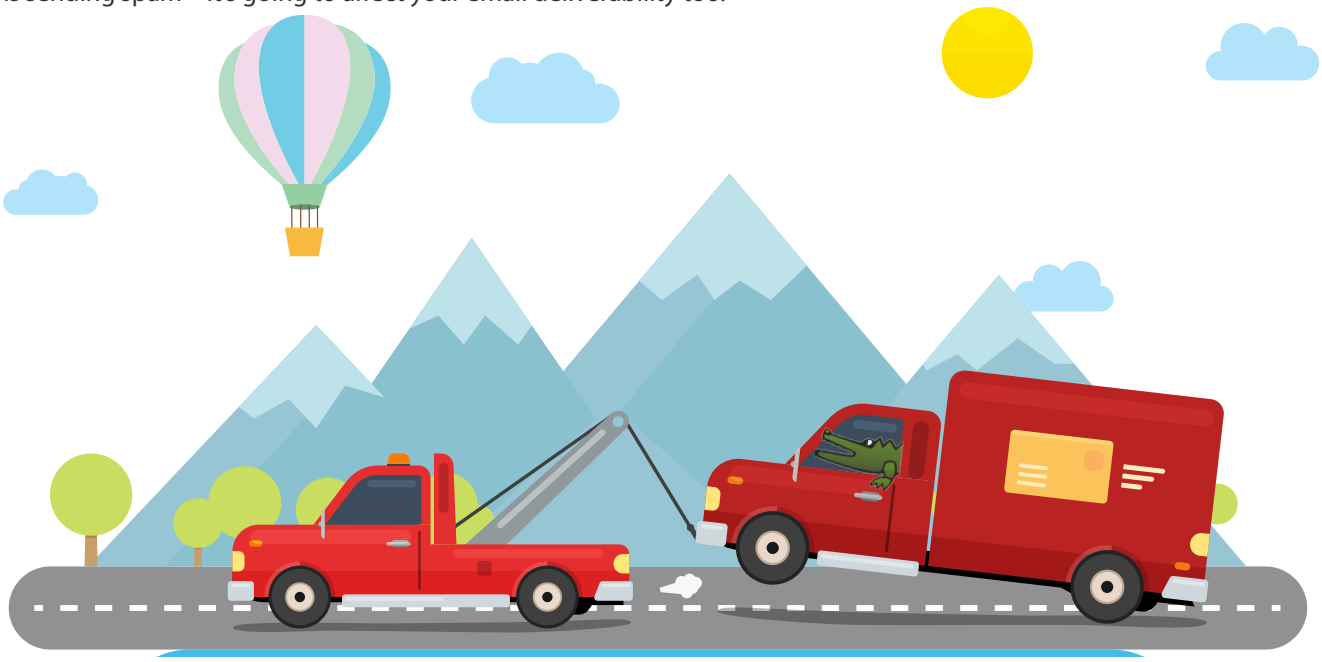
When it comes to email marketing, there are two types of IP addresses you should be aware of:

The Dedicated IP address

This is used by a single sender or company, which is what we enforce with our clients. With a dedicated IP address, no other company is sending email from this IP address. This means you, and you alone, are responsible for the reputation of your IP address.

The Shared IP address

This type of IP address is used by multiple marketers and companies to deploy email, which we would NOT recommend. The IP address reputation is based on all mail sent from it, so if another marketer from the same IP address is sending spam – it's going to affect your email deliverability too.



Your IP address & its Sender Score

Like a credit score, your email score places a numeric value on your email deliverability. The lower your score, the worse your IP address reputation. Of course, a high score does not guarantee you will get into the inbox as every mailbox provider has a different set of rules (much like banks and lending).

Your sender score relates to the mailing history of your IP address. That's why constantly changing IP addresses isn't necessarily a good idea. Things that can affect your sender score include:

- The length of time you've been sending from that IP address
- The volume of emails you are sending
- The consistency with which you are sending emails.

You're actually better off sending small batches of emails with a new IP address to engaged audiences to build up your credibility before batch-sending email campaigns to high volumes of email recipients.

*Our email deliverability expert can talk you through how to improve your sender score when moving to a new, dedicated IP address if you're using GatorMail.

What you need to know about your domain

So while the IP address is the number, the domain name is the registered name on the internet. For example, communigator.co.uk. As the second component of the email source, it's important that your domain reputation (sending rep for the domain name) is as clean as it can be.

Your domain reputation can be from the subdomain or the domain itself, but it is usually tied directly to the singing domain used in the Domain Keys Identified Mail (DKIM) authentication protocol.

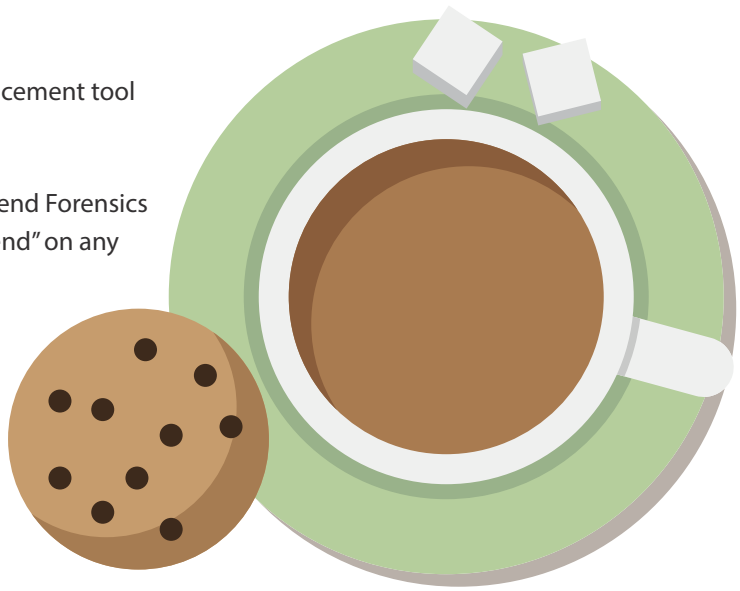
Here at CommuniGator, we also sort out your domain for you, though there are a few things you can do to keep your domain reputation as pristine as possible:

1. Keep your complaint rate low – send relevant, targeted communications.

2. Keep your bounce rate low – we have an inbox placement tool that can help with this.

3. Keep your spam folder placement rate low – our Send Forensics tool can help identify your score before you press "send" on any email.

4. Keep blacklist appearances to a minimum!



IP address best practice

Our recommendation and industry best practice is to use a dedicated IP address. That way, you can maintain your reputation without being influenced by any other email marketers. We would also suggest the following best practices.

Ensure your mail servers are secure

To keep spammers clear of your IP address, make sure you do not have an open proxy or open relay. If you are a CommuniGator customer, don't worry, we take care of this for you.

Don't IP address "hop"

If you have a poor reputation, hopping to a new IP address won't solve your problems. In fact, new IP addresses have almost as many problems as damaged IP addresses. Make sure you take the following steps to improve your current reputation and break in any new IP addresses the right way.

Steps to take to improve your IP reputation:

1. Secure your infrastructure
2. Authenticate your email streams
3. Monitor the emails you send
4. Send great content

Build up your reputation slow & steady

Slow and steady definitely wins the race when it comes to building up a sender reputation from a new IP address. We recommend you send out the first few emails to small volume groups to identify bounces and likely unsubscribes. This will show the mailing providers that you are attempting to send quality emails.

Then, increase your volume over time, making sure to keep your sends as consistent as possible. High-volume spikes are likely to attract attention, so you want to make the process gradual and timely.

Use a preference centre

A preference centre will allow your email recipients to request how they would like to receive email communications from you, making them less likely to unsubscribe or mark you as spam. Your preference centre could ask them anything from how often they wanted to receive your emails to the topics/products they would like information on.

Authentication & infrastructure considerations

Similar to a credit check, your authentication can be considered an ID check by mailbox providers. This way the mailbox provider knows it is you and not some spammer trying to impersonate you. In order to achieve this, you must have a solid infrastructure (foundation if you will) on which to build your email marketing platform, much like CommuniGator already have for their clients.

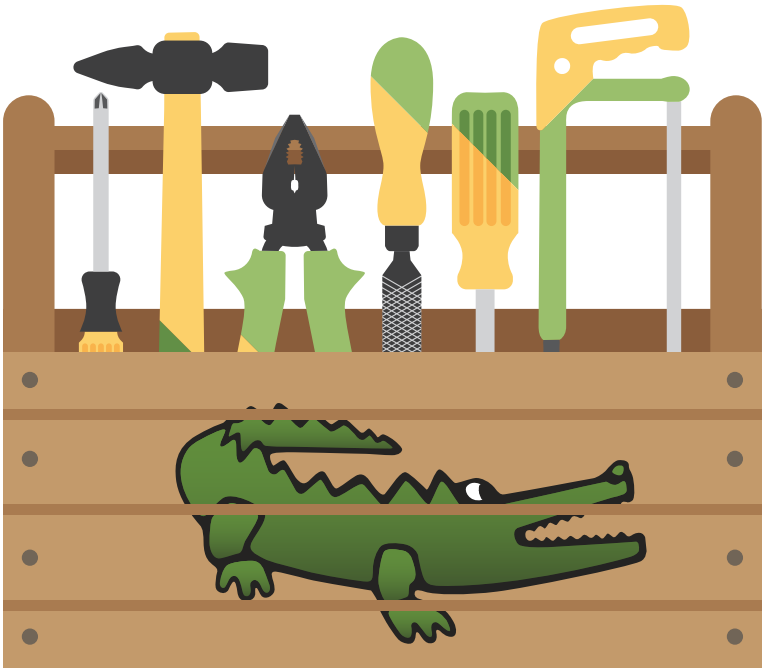
Your infrastructure will be comprised of three aspects:

- Accurate authentication
- Inbox placement testing
- Bounce Management

What happens if I don't have these three aspects in place?

Simple, your chances of landing in the inbox decrease significantly. Luckily, if you sign up to an ESP that manages your authentication and infrastructure, like GatorMail, you don't have to worry about building the foundation of your email programme.

Authentication isn't optional, it's essential to securing your brand and online email reputation.



Accurate authentication

Here at CommuniGator, we recommend three primary methods of authentication.

SPF (Sender Policy Framework)

SPF is an email validation system that uses IP address-based authentication to validate that the IP address that sent the message is authorised to send mail for that sending domain. In English, that means the mailbox provider can check that any incoming mail is from you and not forged from addresses at your domain by some spammer.

DKIM (Domain Keys Identified Mail)

DKIM is one of the most complicated email authentication tools out there. To put it simply, it allows you to validate your emails by using publicly available cryptographic authentication. By doing this, it signs each message is a way that is difficult to forge thus proving your message came from the correct sending domain.

DMARC (Domain-based Message Authentication, Reporting & Conformance)

The latest type of email authentication, DMARC builds on the SPF and DKIM protocols to make sure legitimate email is properly authenticated. It also has an additional reporting function that allows senders to monitor their domain from fraudulent email.

Inbox Placement Testing

When an email is sent from GatorMail it doesn't land immediately in the recipient's mailbox. First, it goes to our mail server where the email is queued for send. This way, we can monitor and check that emails will get to the inbox before they are sent, maintaining your sender reputation.

Each email that hits our mail server will usually have a delivery attempt immediately. But, depending on the response from the other side, it may remain in the queue for longer.

When we attempt delivery for an email, the remote site will do one of three things:

1. Accept the email.
2. Reply with a "soft" response telling us to try again later.
3. Reply with a "hard" response telling us to go away.

By default, we retry sending every 10 minutes until 5 days have passed, at which point the email will expire and we discard it. At best an email delivers within seconds of being sent. At worst the email does not deliver and is discarded. At any point from the first delivery attempt to when it is discarded the email can bounce. Despite what no.1 says, all three of these can result in a bounce.

Bounce Management

Essentially there are two types of bounces and two ways to get a bounce. The types are hard and soft. The ways to get a bounce are called local and remote.

Here we share our definitions of the bounce types and ways:

A local bounce – when a bounce occurs with the email never leaving our mail server. This is when we attempt an email delivery but get a hard or soft rejection. This type of bounce accounts for 90% of all bounces.

A remote bounce – when the email has been delivered to the recipient's network but later bounces back to us. This accounts for less than 10% of all bounces.

A soft bounce – occurs when the email does not deliver for the duration the email is on our mail server. This means every retry attempt to deliver was denied but not one of those denials was a hard response.

A hard bounce – occurs whenever the remote site gives us a hard response. This is an outright rejection of the delivery attempt and can occur after a soft response for 2 days or on the first delivery.

How bounces work in GatorMail

When a bounce occurs, GatorMail will add it to the results for the campaign and update the contact record. An important note to make is hard and soft bounces can equally update contacts to undeliverable.

We judge the contact update on what the bounce category actually is. For example, a bad-domain bounce is a clear sign of a bad email address and the contact would be marked undeliverable. But a blacklist-related bounce does not cause an immediate undeliverable even though that would be a hard response from the remote server.

In cases where we do not make a contact immediately undeliverable, we increment a count on the contact record. This is stored in the field called "BounceCount". Each bounce will increment it by 1 until we get the 5th bounce. At which point the contact will then become undeliverable, and the bounce count field is set to 0.

Types of spam filters and how they work

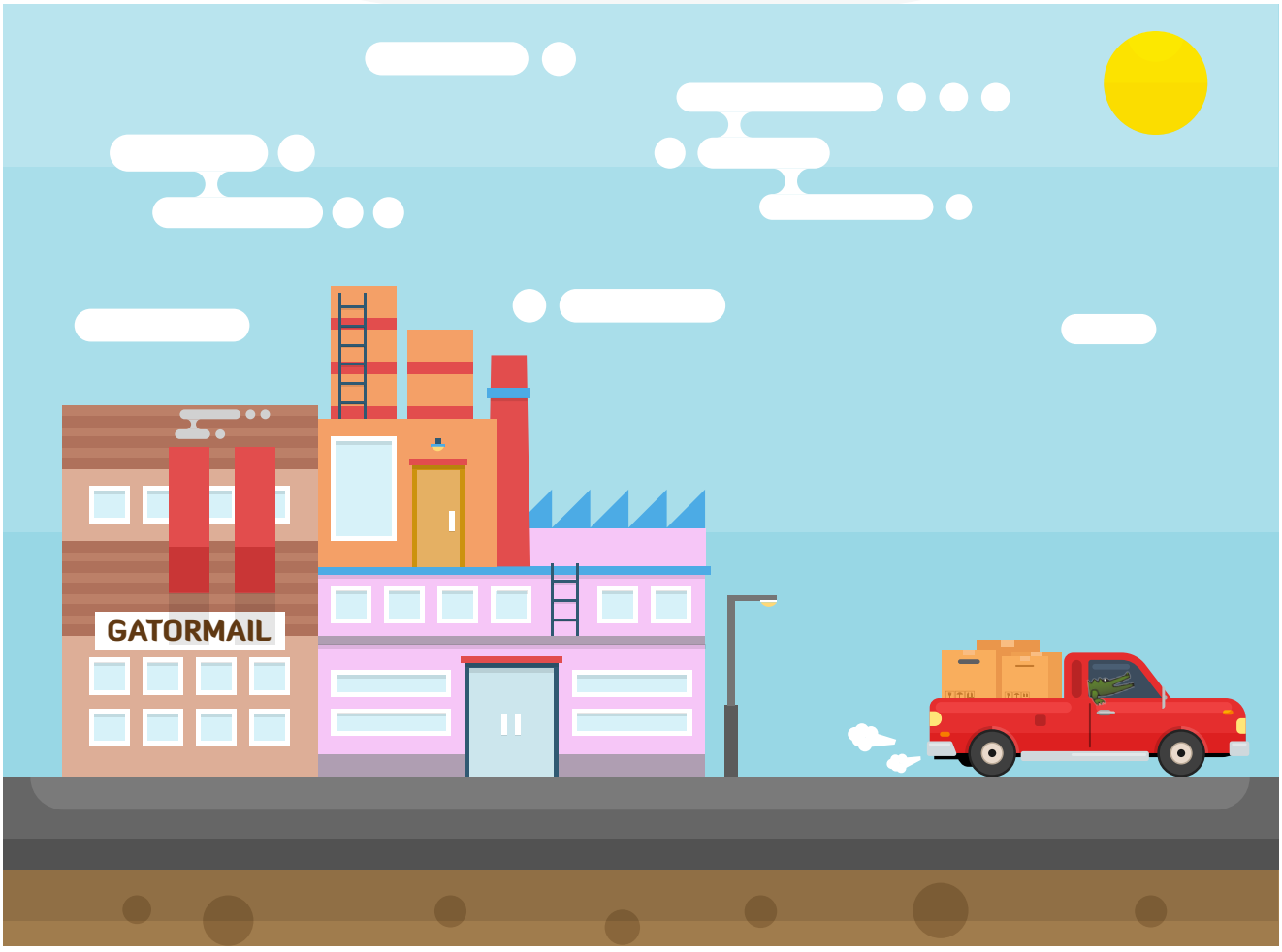
Even with the best practices and tools such as SendForensics, which are email deliverability and inbox placement tools, you can still find your emails subject to a spam filter. Each mailbox provider will have their own spam filter settings and search criteria, so it's important to understand what to look for and make sure you are complying to spam filter rules & regulations.

Gateway spam filters

These are physical servers that are installed at the border of a company's network. As the name suggests, all mail must pass through the "gate" before it can enter the system. It typically has less email data to learn from than a hosted spam filter because it is relying solely on the emails coming through to just the company.

Hosted spam filters

Hosted, or third party, spam filters have a much wider range of information to determine what qualifies a "spam" message because of the large list of clients using their service. They typically use content and reputation metrics to distinguish spam and can influence filters at the gateway or after the message has been accepted.

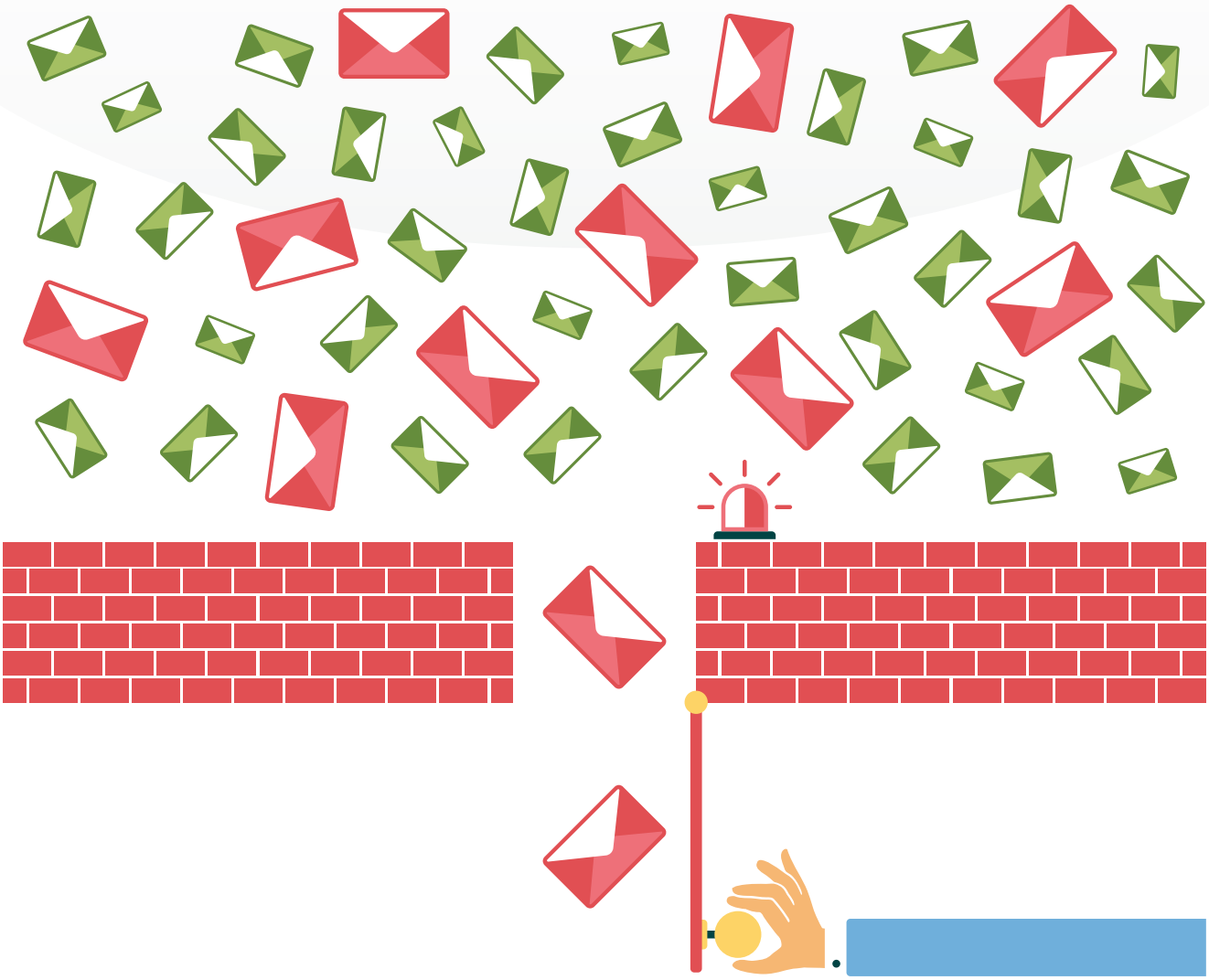


Desktop filters

These filters live on the end user's computer and are highly-customisable to the recipient's wants when it comes to their inbox, making it tricky to filter through. An example is Outlook, which obviously has the Clutter and Junk functionality, along with the anti-spam filter SmartScreen.

With spam filter algorithms constantly updating to predict marketer's movements, using tools which can pre-establish your "spam score" and reduce your likelihood of being rejected are useful to employ within your ESP. The best practice is, of course, to send relevant communications to the relevant person and employ permission based marketing principles where you can.

For more on our best practices in regards to spam filters, take a look at the CommuniGator Avoiding Spam Filters Guide.



Understanding blacklists

Blacklists are exactly as they sound, a bleak, dark place for any email marketer to find themselves. With over 300 public blacklists, as well as independent blacklists, it's important to make sure you follow the best practices given in this guide in order to never find yourself on a blacklist.

It's worth noting that companies and filtering systems often use a mix of public and private blacklists. There are two types of public blacklists you should be aware of.

IP address-based blacklists

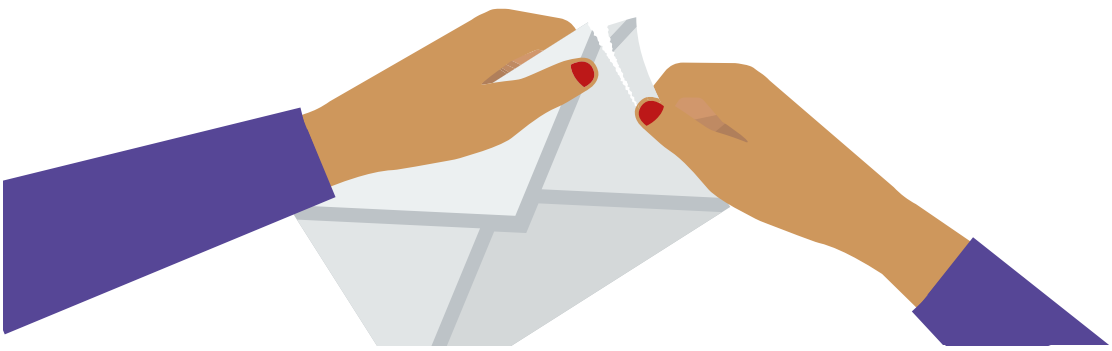
These lists focus on blocking anything from an IP address they deem to be a source of spam. If a remote site has put a complete block on receiving anything from that IP address, this is more like a global block (substantially worse than a domain block) and all email from this IP address will fail to get through.

Domain-based blacklists

These lists consist of domain names that appear within the email headers or email body itself. They will look for URLs within the email to see if it contains a domain that has been identified as a source of spam, whether an initial link or a redirect.

Common IP address-based lists include:	Common domain-based lists include:
Return Path Reputation Network Blacklist	dbl.spamhaus.org
Sbl.spamhaus.org (SBL)	URIBL
SpamCop (SCBL)	SURBL

The most important thing to remember is if you find yourself on a blacklist, discover why that is and try to fix the issue. Just hopping to another IP address won't improve your email deliverability overnight, and you're better off getting to the root of your problem so you avoid it happening again.



Email deliverability definitions & metrics

Here we round up a few email deliverability terms that you've probably heard but may not fully understand, as well as the metrics that are commonly used to measure email deliverability and performance.

Definitions

Email deliverability

Measuring your ability to get into the inbox through a number of factors including inbox placement rate, sender scores, domain reputations and surpassing spam filters.

IP address

Similar to a postcode, your IP address is a unique string of numbers separated by full stops that identifies each computer using the Internet Protocol to communicate over a network.

Spam

While in the eye of the email recipient for the most part, spam is technically defined by the intentions of the sender. If the intention is to send marketing emails to a valid prospect or customer, it's email marketing. If you hack a database and send to millions upon millions of randomly selected email addresses, it's spam.

Metrics

Delivered rate

A delivery rate measures the amount of sent email that were delivered, i.e. they weren't bounced or rejected by dividing the number of emails delivered by the number of emails sent. However, this doesn't necessarily mean the emails were delivered into the inbox (a common misconception).

Inbox placement rate

Inbox placement rate measures the percentage of sent email that actually lands in the subscribers' inbox. This is a much more accurate measurement than the delivered rate.

Bounce rate

The opposite of the delivered rate, this is measured on the messages that failed to get delivered for any reason.

spotler

SpotlerUK is one of the leading B2B marketing automation & lead generation software providers in the UK.

Offering an all-in-one inbound and outbound marketing software, SpotlerUK provides everything you need to launch effective marketing campaigns that generate leads and engages your audiences.

To read all the juicy details of what the platform offers and how we can help your business jump on over to our website: spotler.co.uk.

Or for more on all things marketing and sales related, visit our blog: spotler.co.uk/blog or sign up to our newsletter: spotler.co.uk/newsletter.

If you want to say 'hello', give us a call: +44 (0)1483 411 911

SpotlerUK
3 The Billings Walnut Tree Close
Guildford Surrey GU1 4UL

info@spotler.co.uk

Our products and services include:

Marketing**Automation** | Gator**Mail** | Gator**Leads** | Gator**Events** | Gator**Docs**
Gator**Survey** | Gator**Social** | Gator**Data** | CRM **Integration** | Managed **Services**