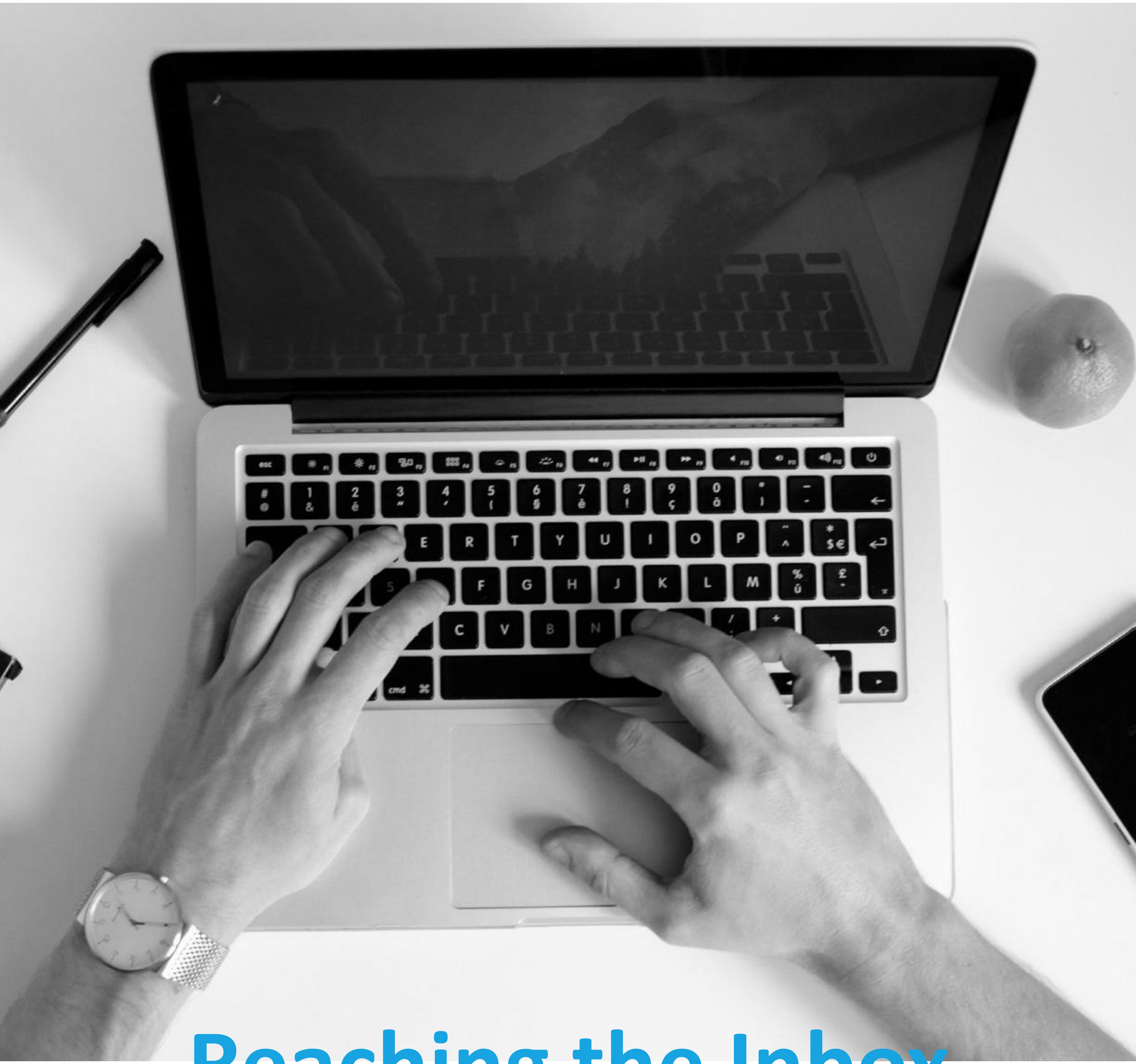
Rhetorik

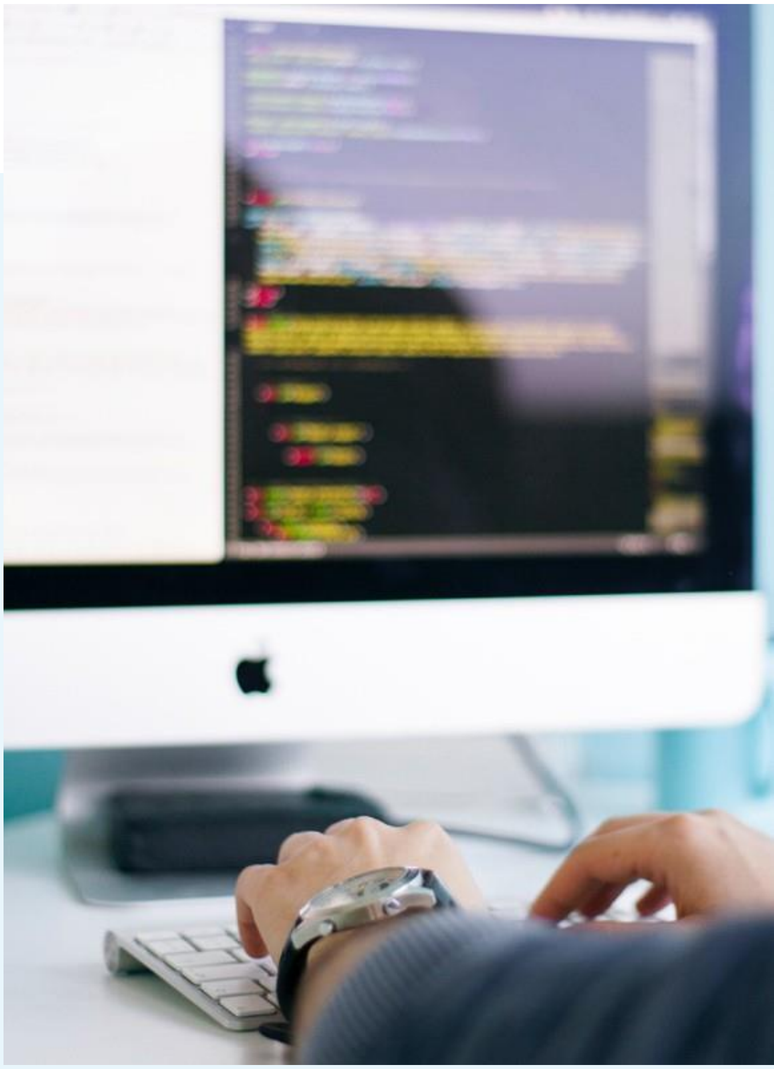


Reaching the Inbox

THE ULTIMATE B2B MARKETER’S GUIDE TO

EMAIL DELIVERABILITY

Contents



CHAPTER 01

How Email Works

What happens when you send an email? .

Introduction

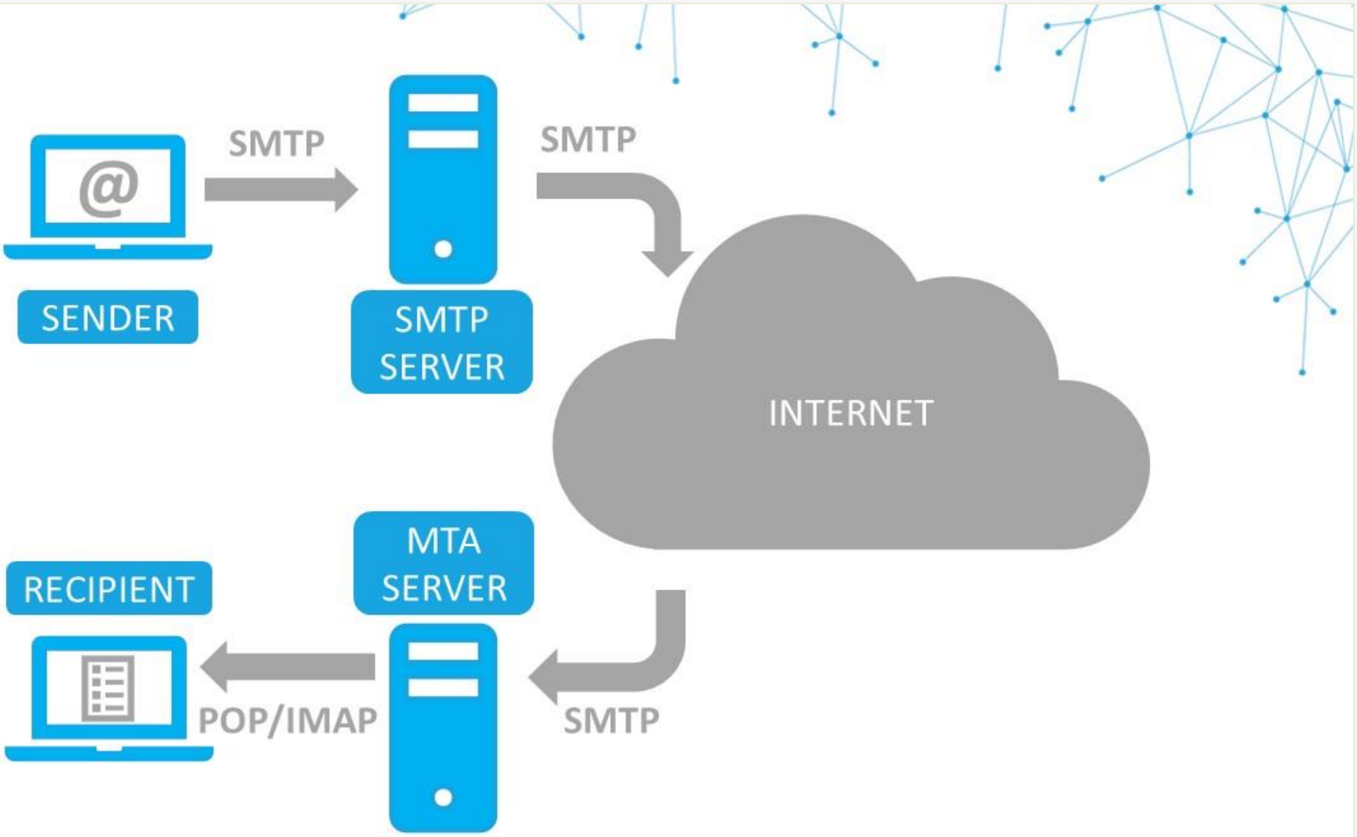
What happens when you send an email? Perhaps unsurprisingly, the process of electronic mail delivery is quite similar to physical mail: an organized system exists to take your mail and deliver it to the recipient.

The procedure to control this system on the internet is called Simple Mail Transfer Protocol (SMTP).

The sender connects to an SMTP Server (a computer running SMTP), which acts rather like a postman, picking up the mail from the sender and delivering it to the recipient's server.

The journey that an email takes from your computer to the recipient's looks like this:

- **Compose**: compose the message using an email client
- **Send**: send the message to an SMTP server
- **Relay**: relay the message to the recipient's server
- **Deliver**: deliver the message to the recipient
- **Read**: recipient reads the message



Send & Deliver

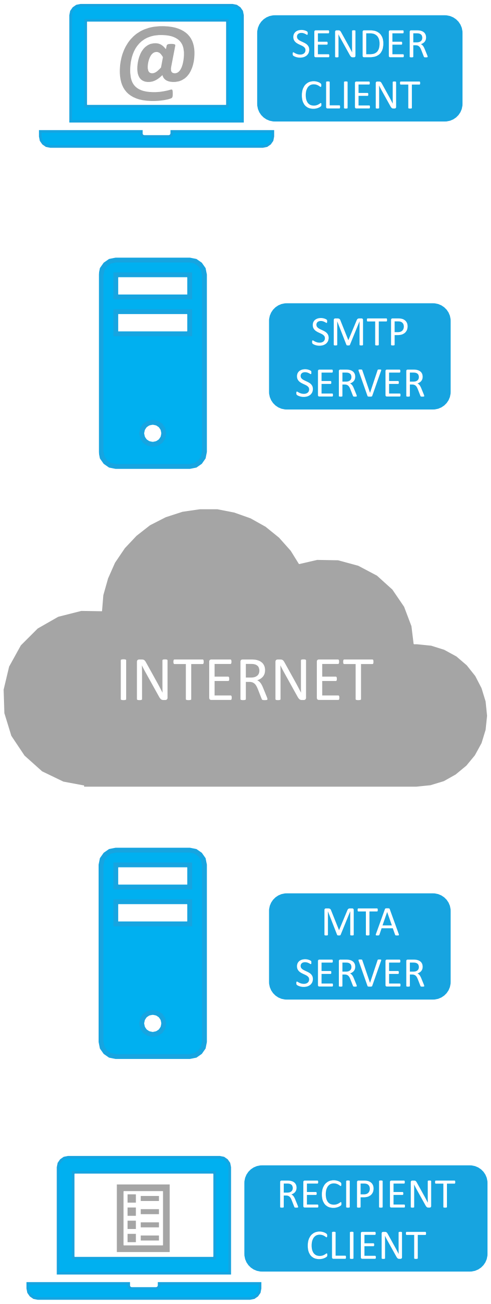
- **Compose**: Compose and send an email using a Message User Agent (an email client such as webmail or Outlook) from your address (eg, john@sender.com) to a given recipient (eg, jane@recipient.com).

- **Send**: The message is sent to an SMTP server (eg, mail.sender.com), which is given to your email client when you set it up. Client and server start a brief "conversation" enabling the server to check all the data concerning the message's transmission (sender, recipient, domains, etc.).

- **Relay**: If the recipient's email domain is directly connected to the server, the email is immediately delivered. Otherwise, SMTP 'relays' it to the incoming server, the Mail Transfer Agent (MTA), used by the recipient.

- **Deliver**: If the recipient's incoming server is down or busy, the SMTP host passes the message to a backup server. If no backup server is available, the email is put in a queue and delivery is retried periodically. After a certain period, the message is returned as undelivered.

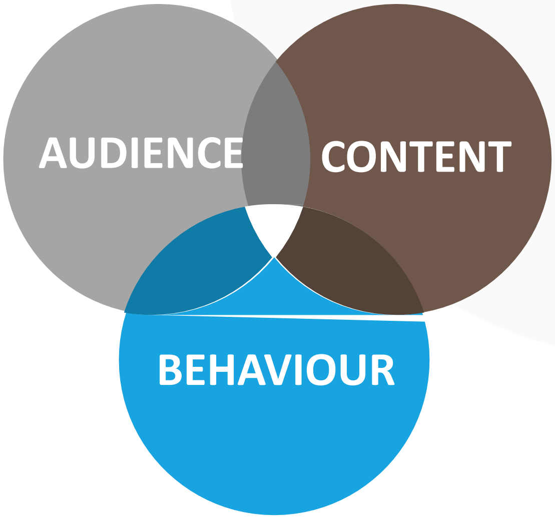
- **Read**: If there are no issues, the final segment is controlled by another protocol (POP or IMAP) that picks up the email from the incoming server and puts it into the recipient's inbox.

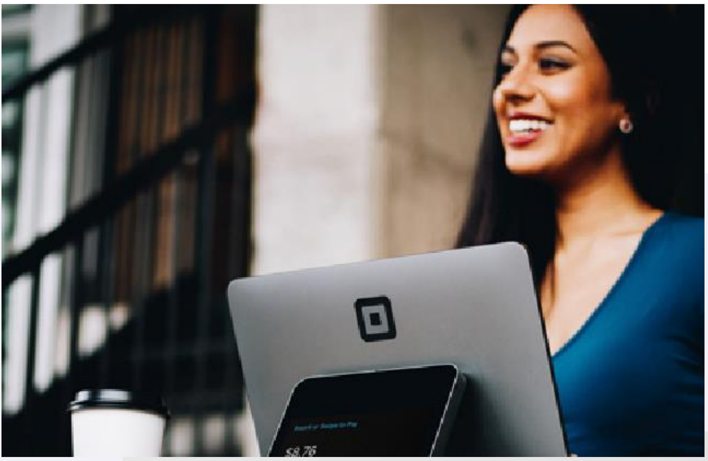


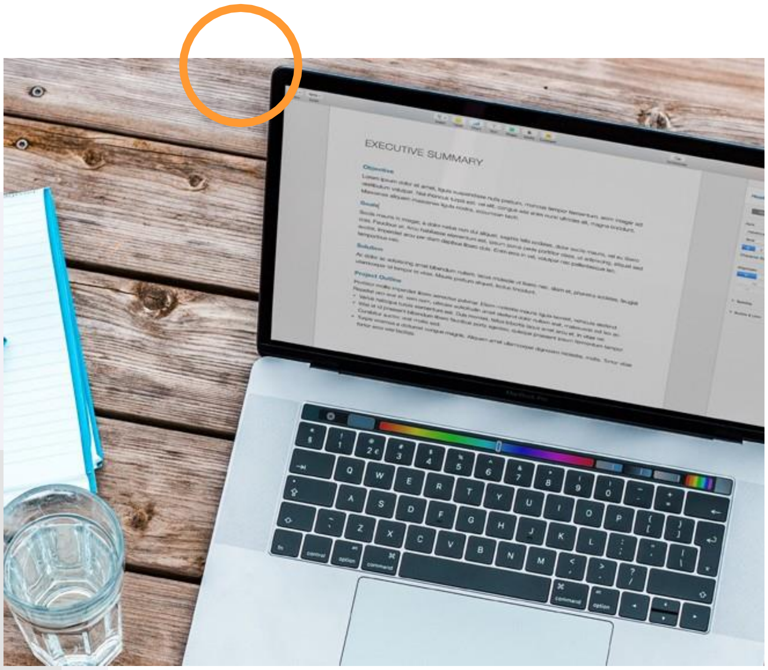
What you can control

SMTP is concerned only with the **process** of transmitting of the message and is largely beyond your control.

However, the quality of the **audience** list, the **content** of the message and the **behaviour** of the sender also affect deliverability, which are things you can control.







CHAPTER 02

Why not all emails get delivered

Audience, Content and Behaviour

Introduction

Your email is successfully delivered when your message arrives in the inbox of the intended recipient.

Unfortunately, even when you have the recipient's correct email address, delivery is never guaranteed.

The ways in which your message might fail to reach the recipient's inbox are many and varied - junk folders, anti-spam filters, firewalls, ISP (Internet Service Provider) blocking and more.

In fact, according to an Email Deliverability Benchmark Report by ReturnPath[1], more than 1 in 5 opt-in emails never make it to the inbox.

The three key factors impacting on email deliverability are **audience**, **content** and **behaviour**.

The good news is that you can affect all these factors to improve the chances of your emails being delivered successfully.

In a nutshell, you should aim to:

- **look after your list**
- **avoid spam-like Content** and
- **avoid spammer-like Behaviour**

These last two factors are closely linked, but it is worth looking at each separately.

[1] ReturnPath

How to avoid spam-like Content

Subject Line

The Subject Line will largely determine whether your email is read, filed or deleted.

If your subject line looks spam-like, then people, and the spam filters in place to protect them, will probably think it is spam.

- avoid using words that spam filters look for. There are plenty of online lists available to assist you.
- match the subject line to the email content. No-one wants to be promised a luxury cruise and end up on a pedalo.
- avoid the misleading use of “RE” or “FWD” prefixes if there has been no previous contact or email exchange.
- feel free to personalize and get creative with your copy, but be clear about what the email contains.
- be concise. Email clients may display a shortened subject line, so be aware what the recipient actually sees in their inbox.

Email Content

Subject line guidance also applies to the main email content. Avoid spam list words, be clear and concise. In addition, image to text ratio does carry some weight with spam filters and is worth getting right.

Spammy emails often contain lots of images and very little text, or just one large image. By creating similar emails, you risk your email being flagged as spam.

Many email clients do not display images by default, so design your emails with this in mind.

- Balance your images and text.
- Ensure your email “reads” well whether or not the images are displayed.
- Always use alt text for your images. This way, even if the images aren’t displayed, the reader will have some understanding of what they are.

Links

Marketers love their URL shorteners, but spammers do too. This means spam filters may block your emails, even when the links are genuine.

- avoid using URL shorteners. Replace them with clear call to action buttons to see higher click-through rates on your sends.
- insert a hyperlink on the relevant text rather than inserting the full URL (except text-only versions of the email).
- ensure all your links are functional, and that they go to legitimate domains.

How to avoid spammer-like Behaviour

Even if you get the content right, your behaviour as an email sender may determine whether your email makes it to the inbox or not.

Why? Because your behaviour determines your reputation, and reputation matters.

Senders with good reputations get delivered. Senders with poor reputations get blocked or their messages land in the "junk" folder.

As with personal and business reputations, your email sender reputation builds up over time – for better or worse.

To build or maintain a good reputation, you first need to know what your current reputation is and why.

We will look at what you can do about it in Chapter 3.

But first, what is it now and why?

It isn’t always easy to know what your reputation is, but there are signs – positive or negative – to look out for that will give indicate if you are on the right path.

Positive reputation indicators

Positive signs come with positive actions by recipients, and include:

- **Open** – If recipients frequently open your emails, this is a positive sign that they aren’t spam and helps your emails make the inbox.

- **Reply** – If people reply to your emails, this is also a good signal and helps improve your reputation with email providers.

- **Not junk** – If recipients move your email out of the junk folder, this is a very positive sign that your emails are relevant and deserving of the inbox.

- **Move to folder** – If people move your emails into other folders in their inbox, this is a sign they care about your emails and email providers are more likely to continue delivering them to their inbox.

- **Add to address book** – as with moving to a folder above, if users add your email address to their address book, this is a sign they care about receiving email from you, making email providers much more likely to continue delivering them to the inbox.

- **Add to white list** – users that add you to their white list, or select Never Block Sender, are sending a most positive signal that they want your email in their inbox.

- **Low bounce rates** – a positive sign is when only a small percentage of your emails are returned by the ISPs because the account is no longer active (hard bounce).

Negative reputation indicators

Not surprisingly, negative signs are linked to negative actions, such as:

- **Move to junk** – If recipients move your email to the Junk folder, this is a very negative signal suggesting your emails don't deserve to be delivered to the inbox.
- **Delete without open** – recipients taking a quick glance at the sender and subject line of your email, then deleting it, is a negative signal, though not as strongly so as moving to junk.
- **High bounce rates** - If a lot of your mail is hard-bouncing, it means you're not keeping your lists up to date. This makes your email look like spam to an ISP and your emails are less likely to get delivered.
- **Complaints** - Even a tiny increase in complaints by recipients can cause your emails to be blocked by the ISPs. Aim for a complaint rate below 0.1% of emails sent and accepted by the ISP.
- **Add to black list** – this is one you really want to avoid, as users that add you to their black list, or select Block Sender, are sending the strongest negative signal to email providers to keep your email out of their inbox.

Aim for consistency

High-volume senders are a red flag, more so when their sending behaviour is inconsistent.

Do you send a similar volume of emails each week or month, or are your sending patterns less predictable?

Consistency, based on typical recipient preferences and volumes, are a key factor for ISPs. When these elements are combined, you end up with not one, but two reputations:

1. Reputation with an individual recipient – If a particular recipient always opens your emails and moves them to folders, you build up a positive reputation with them.

2. Reputation with the various gatekeepers – For example, if the majority of Hotmail recipients open your emails and move them to folders, you build up a great reputation with Hotmail. On the other hand, if the majority are junking your emails, then even individuals who were engaged with you in the past may not receive your emails.

There is an additional level of detail to your sender reputation that is worth mentioning – you will have one sender reputation linked to the IP address you use, and another linked to your domain.

The key benefit to domain reputation is portability – if ISPs can track your sender reputation irrespective of the IP address you send from, then you are free to move between email service providers without impacting your reputation.

The downside, if you are unfortunate enough to have taken over responsibility for a domain with a poor reputation, is that it will be more difficult to start from scratch with a new domain.

Bottom line: Senders should focus on both domain and IP reputation in order to maximize email deliverability.

CHAPTER 03

How to get more emails delivered

The factors that impact email deliverability .

Reaching the inbox

Understanding the factors that impact email deliverability is a useful step to the primary objective – getting more emails delivered to recipients' inboxes.

The top things marketers can to do to help with this include:

I. **Be consistent**. Perhaps the best thing you can do to build and maintain a good sender reputation is to send a similar volume of emails on a regular schedule. Think of it a bit like a credit card – if you never use it then splash out on a big-ticket item, the credit card company might block the transaction. If you use it regularly, however, then that big-ticket item is seen as part of your wider purchasing behaviour and less likely to get red-flagged.

II. **Be personal**. Opening an email sends strong positive signals to email providers, which makes the 'From' name a critical element of your email campaigns.

Make sure the Sender Name that recipients see in their inbox is personal (eg, John Smith) rather than impersonal (eg, sales@sender.com), and is one that your recipients recognise.

III. **Be relevant**. Sending relevant and interesting content that people want to read is the basis of a great sending (and brand) reputation. Segment your audience and tailor your emails to each segment, rather than sending the same email to your entire list.

More relevant and engaging content will drive the kind of positive behaviour the ISPs (and you) are looking for. You'll increase the number of recipients opening your emails and decrease the number of people deleting them, sending positive signals to email providers about the validity of your campaigns.

Reaching the inbox - 2

IV. **Be open**. A key signal for ESPs is whether you receive replies to your emails. So make it easy for people to respond by using a real reply-to address in your emails.

Avoid using reply-to email addresses such as noreply@sender.com. Email addresses like this tell people you are not interested in hearing from them, which reduces the amount of responses you get, which in turn reduces your sender reputation.

V. **Be open (2).** Make it easy for recipients, email providers and ISPs to know who you are as a business.

When sending emails via an ESP, be sure to use a domain address owned by you and that your recipients expect to hear from, rather than a generic domain provided by the ESP.

This helps prevent ISP filters from blocking your emails, will also be recognisable to your recipients and help build your sending domain reputation.

Not all ESPs offer this facility, and the generic domain may be the default for those that do. Make sure your provider allows you to send from your own domain name (i.e. yourbusiness.com).

Spammers rarely do this, so you send a strong signal to email providers that you are a legitimate business sending legitimate emails.

VI. **Stay clean**. Using clean data is an obvious way to reduce reputational risks, so ensure your data is up-to-date data, remove unsubscribes and hard bounces.

Also, avoid spam traps – email addresses set up typically by ISPs to catch spammers. Sending to just one spam trap will impact your reputation and cause deliverability problems. Why? Because it suggests you or your list supplier harvest emails (scraping emails from websites), which may be illegal depending on your jurisdiction. Either way, it isn't good for your reputation and your email deliverability will decline.

VII. **Be authentic**. One of the surest ways to avoid being perceived as a spammer is to authenticate your emails.

Authentication is an "ID check" that determines the email is really from you, and not a spammer impersonating you. Authentication does not guarantee email deliverability, but helps ISPs to differentiate your legitimate business emails from other illegitimate ones.

While the precise details of authentication are not covered here, it may help you to know there are two main methods of authentication that you should implement:

- Domain Keys Identified Mail (DKIM)
- Sender Policy Framework (SPF)

CHAPTER 04

Understanding bounce-backs

The hard and soft options.

Introduction

If you have got this far, you now have more understanding how email works and that not all emails get delivered, even if the email address is valid.

You will also know the importance of content, reputation and other factors in improving your email deliverability.

You've authenticated your domain, segmented your audience, tailored your message and composed the most relevant and engaging email.

You hit Send and look forward to all those replies, click throughs and conversions.

But what else do you get? Bounce-backs!

A bounce-back means your email message has not been delivered. When this happens, the sender receives an automatic notification of the delivery failure originating from the recipient's mail server.

While there are numerous types of bounce-back, they are typically classified by your ESP as either a hard bounce or a soft bounce.

Very simply, if the ESP categorises the failure as a **hard bounce**, it believes it to be a permanent delivery failure and will not try to re-send the email.

A **soft bounce** is a temporary delivery failure which the ESP will try to re-send .

The bounce-back typically includes an SMTP code explaining why the message bounced (see Appendix). The ESP uses this code to classify it as a hard or soft bounce. Such information may appear in your ESP campaign report.

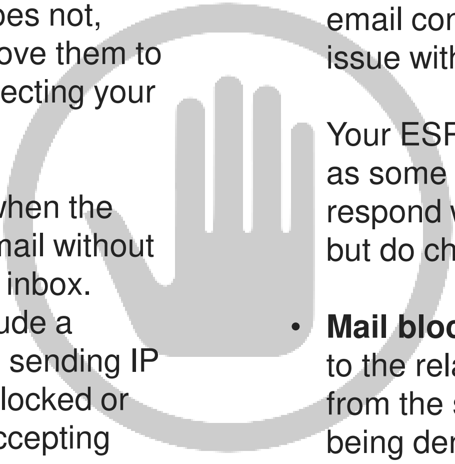
Unfortunately,

- **not all email servers use the standard SMTP codes**, so your ESP must guess how to classify the bounced message
- **not all ESPs use the same rules to classify bounce-backs**, so one sender might get a hard bounce, while another using a different ESP gets a soft bounce from the same email address
- **not all email senders are treated equally**, meaning one sender might see a hard bounce from a perfectly valid email, while another sender sees their email being delivered successfully

Hard bounces (mostly)

These challenges aside, there is much to learn from bounce replies, and plenty that you can do to reduce your bounce rates.

Hard bounce messages and what to do with them



- **Email address is mis-spelled or invalid**: a permanent error caused by an invalid email address. Most ESPs will automatically remove such contacts from future email sends. If yours does not, make sure you correct or remove them to avoid repeat hard bounces affecting your reputation.

- **General mail block**: occurs when the receiving server rejects the email without any attempt to deliver it to the inbox. Reasons for such a block include a blacklisted reply-to address, a sending IP or domain being temporarily blocked or blacklisted, or a server only accepting whitelisted senders.

  You might try resending if the bounce was caused by a temporary block or blacklist of the sending IP or domain.

- **Mail block - known spammer**: a security filter (at the local computer, company firewall, or ISP/data centre) has blocked your email. The address is valid, but the inbox can't be reached by you, perhaps due to poor sending reputation – previous emails from you to the mail server have looked like spam – or one of the sending IPs or domains is temporarily blocked or blacklisted.

  Managing your sender reputation and focusing on relevant content will help avoid this situation, but if it does occur, you'll need to ask the contact to whitelist your sending IP addresses and/or domains, then unbounce the contact with your ESP.

- **Mail block - spam detected**: The recipient's server has blocked your email as the content resembles spam. This may be triggered by something detected in your email content, but can be a reputation issue with your reply-to address or domain.

  Your ESP may treat this as a soft bounce as some mail servers and email providers respond with false or incorrect error codes, but do check.

- **Mail block - relay denied**: a bounce due to the relay (transmission) of your email, from the sending to the receiving server, being denied. This a temporary error, which could be on the sending or receiving side. It usually occurs when the sender's message is not authenticated, but it can also be due to a misconfigured server on the recipient side. Strictly speaking this is a hard bounce, but your ESP may categorise it as a soft bounce because it's often a result of user error, which can be resolved.

- **Mailbox is full**: likely a permanent error due to an abandoned inbox, but the recipient may have reached their storage limit. Some ESPs will classify this as a temporary soft bounce. Check how your ESP handles them.

Soft Bounces

Messages and recommendations

- **Temporary technical issue with the recipient's email**: recipient's server may be overloaded, timing out, or being re-configured and preventing it accepting the message. Re-send a copy email to the affected contacts at a later date.

- **DNS failure**: recipient's server is unable to deliver your email due to DNS issues at their end. An unreachable DNS host may be temporary or permanent, so your ESP will likely treat this as a soft bounce to allow time to rectify the problem.

- **Challenge response**: recipient's anti-spam software will only accept email from previously authorised senders. If the software doesn't know the sender, a challenge email is returned, requiring a specific action before the original email will be sent to the user. Your ESP will not know the requested response and will likely treat these as a soft bounce, but do confirm this.

- **Message too large**: your email, including all headers, text and images, is larger than the maximum size the recipient's mailbox allows. The bounce message doesn't give on the size limit information, but common advice is to stay below 500Kb.

- **Transient bounce**: recipient mail server can't deliver your email, but your ESP will keep trying for a limited period of time. This will likely be treated as a soft bounce, since the message could be delivered when the recipient mail server retries.

As well as these message-specific bounces, there are also a couple of other bounce reasons to be aware of:

- **Globally suppressed**: Contacts who have complained directly to your ESP in the past, or that are known spam traps.

- **ISP complainers**: Contacts who have submitted spam complaints to your ESP via their internet service provider.

CHAPTER 05

Appendix

SMTP Error Codes

What are they and what can you do with them?

SMTP Error Codes

For every email you send, the receiving email server will return a 3-digit SMTP code to your sending server.

The first digit defines whether the server has accepted the command, completed an action, identified a temporary issue or encountered an error. The second and third digits provide further information about syntax, connection status, mail transfer status etc.

The key ones to look out for in bounce backs are 5xx codes, especially the codes from 550 to 555.

Unfortunately, as mentioned previously, the situation gets rather confusing because:

- **not all email servers use the standard SMTP bounce reply codes in the same way**, meaning your ESP must guess how to categorize that bounced message
- **not all ESPs use the same rules when categorising bounce-backs**, meaning one sender might get a hard bounce, while another sender using a different ESP gets a soft bounce from the same email address

On the plus side, many error codes come with accompanying text to help explain the reason for the error.

Examples of side messages for code 550, the most common SMTP error code meaning simply the email could not be delivered, include:

550 Message rejected as spam

550 Mail from refused spam site

550 Unrouteable address

550 Message contained unsafe content

SMTP Error Codes

CODE	MEANING	HOW TO SOLVE IT / WHAT TO DO
101	The server is unable to connect.	Check the server's name and spelling, or the connection port.
111	Connection refused or unable to open an SMTP link.	Normally a connection issue with the remote SMTP server, depending on firewalls or misspelled domains. Check spelling and all the configurations.
211	System status message or help reply.	Comes with more information about the server.
214	A response to the HELP command.	Contains help information about your particular server, perhaps linking to a FAQs page.
220	The SMTP server is ready.	Everything is working.
221	The server is closing. May come with a message such as "Goodbye" or "Closing connection".	The mailing session is going to end and all messages have been processed.
250	Requested action has been completed.	Success: everything has worked and your email has been delivered.
251	User not local will forward	Recipient is not local to the server, but server will accept and relay the message to another.
252	Recipient cannot be verified.	Server cannot verify the user, but email account is valid and server will try to deliver the message.
354	Start mail input end <CRLF> <CRLF	Server has received the "From" and "To" details of the email and is ready for the message itself.
420	Timeout connection problem	Either your email has been blocked by the recipient's firewall, or there's a hardware problem. Check with your provider.
421	The service is not available and the connection will be closed.	Your or recipient's server is unavailable, and dispatch will be tried again later. May refer to an exceeded limit of simultaneous connections, or a more general temporary problem.
422	The recipient's mailbox has exceeded its storage limit.	Best to contact the user via another channel to alert them and ask to create some free room in his mailbox.
431	Not enough space on the disk, or an "out of memory" condition due to a file overload.	May relate to you sending too many messages to a particular domain. Try sending smaller sets of emails instead of one big set.
432	The recipient's Exchange Server incoming mail queue has been stopped.	A Microsoft Exchange Server error code, generally due to a connection problem.

SMTP Error Codes - 2

CODE	MEANING	HOW TO SOLVE IT / WHAT TO DO
441	The recipient's server is not responding.	There's an issue with the user's incoming server: yours will try again to contact it.
442	The connection was dropped during the transmission.	A typical network connection problem. Worth checking if it is due to your router.
446	The maximum hop count was exceeded for the message: an internal loop has occurred.	Ask your SMTP provider to verify what has happened.
447	Your outgoing message timed out because of issues concerning the incoming server.	This happens generally when you exceeded your server's limit of number of recipients for a message. Try to send it again segmenting the list in different parts.
449	A routing error.	Like error 432, it's related only to Microsoft Exchange.
450	Requested action not taken – The user's mailbox is unavailable.	Mailbox is offline or corrupted, or your email has been rejected for IP problems or blacklisting. The server will try to resend the message. Check status of your sending IP address.
451	Requested action aborted – Local error in processing.	Your ISP's server, or the server that got a first relay from yours, has encountered a connection problem. Normally a transient error due to a message overload, but can also be a rejection by a remote antispam filter.
452	The command has been aborted because the server has insufficient system storage.	Typically, too many emails sent or too many recipients, and the next try will often succeed. If a problem on your server, may have a side-message such as "Out of memory".
471	Error of your mail server, often an issue of the local anti-spam filter.	Contact your SMTP service provider to fix.
500	A syntax error: the server couldn't recognize the command.	May be due to a bad interaction of the server with your firewall or antivirus. Read carefully their instructions to solve it.
501	A syntax error in the parameters or arguments of the command.	Usually an invalid email address, but may also relate to connection problems, or antivirus settings.
502	The command is not implemented.	Command has not been actioned by your own server. Contact your SMTP service provider.
503	The server has encountered a bad sequence of commands, or it requires an authentication.	"Bad sequence" is usually due to a broken connection. If an authentication is needed, you should enter your username and password.

SMTP Error Codes - 3

CODE	MEANING	HOW TO SOLVE IT / WHAT TO DO
504	A syntax error: a command parameter is not implemented.	Similar to 501. Contact your SMTP service provider.
510/511	Bad email address.	An email in your To, CC or BCC line doesn't exist. Check and correct mis-spelled addresses.
512	A DNS error: the host server for the recipient's domain name cannot be found.	Check for mis-spellings as a domain name may be wrong, such as recipient@domain.coom instead of recipient@domain.com.
513	Address type is incorrect.	Usually an address misspelling, so check and correct. If not, and error persists, then likely a configuration issue - the server needs an authentication.
521	This host never accepts mail	A response by a dummy email server.
523	Total size of your mailing exceeds recipient server's limits.	Re-send the message splitting your list into smaller sets.
530	Usually an authentication problem, but sometimes may be an invalid email address, or the recipient's server blacklisting yours.	Configure your settings providing a username+password authentication. If error persists, check all email addresses and whether you have been blacklisted.
541	The message could not be delivered for policy reasons – typically a spam filter.	Your message has been detected and labeled as spam. You must ask the recipient to whitelist you. Not used by all servers.
550	The requested command failed because the user's mailbox was unavailable.	Usually caused by a non-existent email address. However, this code can sometimes be returned by the recipient's firewall (or when the incoming server is down).
551	User not local or invalid address – Relay denied.	Can be a clunky way to prevent spamming. You are unlikely to come across this issue if you use a reputable ESP.
552	Requested mail actions aborted – Exceeded storage allocation.	This indicates the recipient's mailbox has exceeded its limits and usually occurs when sending emails with big attachments.
553	"Requested action not taken – Mailbox name invalid".	Check all the addresses in the To, CC and BCC fields. There will likely be an error or a misspelling somewhere.
554	The transaction has failed.	A permanent error and server will not try to re-send the message. The incoming server thinks your email is spam, or your IP has been blacklisted.
555	The server does not recognize the email address format.	A permanent error and delivery is not possible. Server will not try to re-send the message.

How Rhetorik can help

Rhetorik is a global market intelligence company with 25+ years' experience offering data and marketing services to the IT, technology and telecommunications industry.

We offer a range of data acquisition, data hygiene and lead targeting services, specializing in international markets.

FIND OUT MORE

Rhetorik

www.rhetorik.com