SINCH Mailgun

HANDBOOK

Understanding email deliverability

What is email deliverability, and what can affect it? Unpacking the complexities of what causes your emails to land in the inbox.

Table of contents

PART 1

Introduction

The world of email is growing at an alarming rate. Today, there are approximately 4 billion email users in the world, and that's expected to grow to 4.3 billion users by 2023. With over half of the world's population using email, **mastering email is key to your business growth**.

Sending to a mailbox is easy, but sending to the inbox is another story entirely. This is where deliverability comes in.

> ***Note:*** *Deliverability is the rate in which your messages are being sent to the inbox of a given mail-box.*

In order to have great deliverability you need to have a great reputation, and that can only be done through a properly implemented email program.

Building an email program from the ground up is difficult even with an inhouse technical team dedicated to the effort. Many businesses opt for a little bit of help from email service providers to get the ball rolling with **email experts driving the implementation of the program**. Most of these programs only last a few months, and once everything is up and running your business is left to handle everything else from that point on. Easy, right?

Not exactly. While you might be sending fine out the gate, great deliverability isn't a set in stone metric.If your reputation starts to slip, it can land you on blacklists, in the spam filter, or worse – terminated.

So how do you stay on the right side of the deliverability equation? Here are common practices that you must do that affect your reputation and sending:

PART 2

Email lists

For starters, email lists aren't evergreen, in fact, **most marketing databases degrade by about 22% each year**. Degradation happens for a variety of reasons: employee turnover, lost jobs, full inboxes, death, and suspension of email services are just a few factors that play into your email list losing its quality. While it's easy to run your list through a validation tool and remove full mailboxes and misentered addresses, you can't account for people who aren't interested in your emails anymore.

Those uninterested users bring your engagement metrics down, which hurts your reputation as a legitimate sender. If your reputation falls below a specific threshold, **mailbox providers will move your messages directly to the spam folder or worse – block them entirely**. If either happens, your recipients are less likely to read your messages and convert over to your website, **decreasing the overall ROI of your email program**.

For those uninterested users, oftentimes the best move forward is to sunset them from your list. The question is – where do you draw the line? There isn't a one-size-fits-all solution to this problem, and it largely depends on how often you're sending to that given list.

Determining the best route forward for sunsetting inactive users is complicated, and several other core components should be visited before making any changes. Re-engagement campaigns and list segmentation strategies should be looked at before you remove any users, and these will largely depend on your business and sending needs. Regular **maintenance practices like these keep your engagement rates high and your email lists clean**. Be cautious about implementing any of these practices, as it's best to have an email expert who understands the intricacies of your email program aiding you in the execution of these clean up procedures.

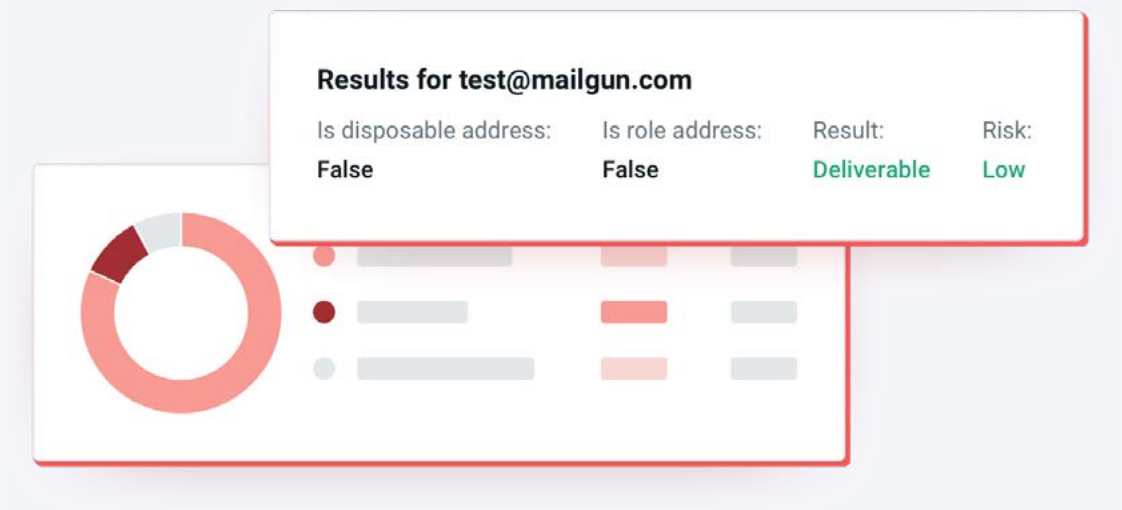
PART 3

Blacklists

DNSBL (DNS-Based Black List) and RBL (Real-time Black List) are **lists of IP addresses that are suspected of sending spam** and are used to prevent unwanted email messages from reaching unsuspecting recipients. It's important to mention that the blacklists aren't blocking your messages, but the mailbox providers themselves. These providers use this information from various blacklist services along with internal metrics to make decisions on whether or not to block a message.

Being listed on a blacklist isn't necessarily going to cause you problems with your deliverability, and while there are a lot of blacklists out there, not all carry the same weight to mailbox providers. Some providers are more important to Gmail, while others are favored more by Yahoo, it all depends on how mailbox providers view them.

That said, **requesting delistings is a delicate business**. Senders might believe that the reason for the block is trivial or a mistake and request a delisting without changing their habits. Requesting a delisting in this way hurts your chances of future requests being accepted in the future, and you might receive a permanent block if not handled delicately. Email experts tend to have existing relationships with these blacklists, and can help set you on the right path once they diagnose the issue.



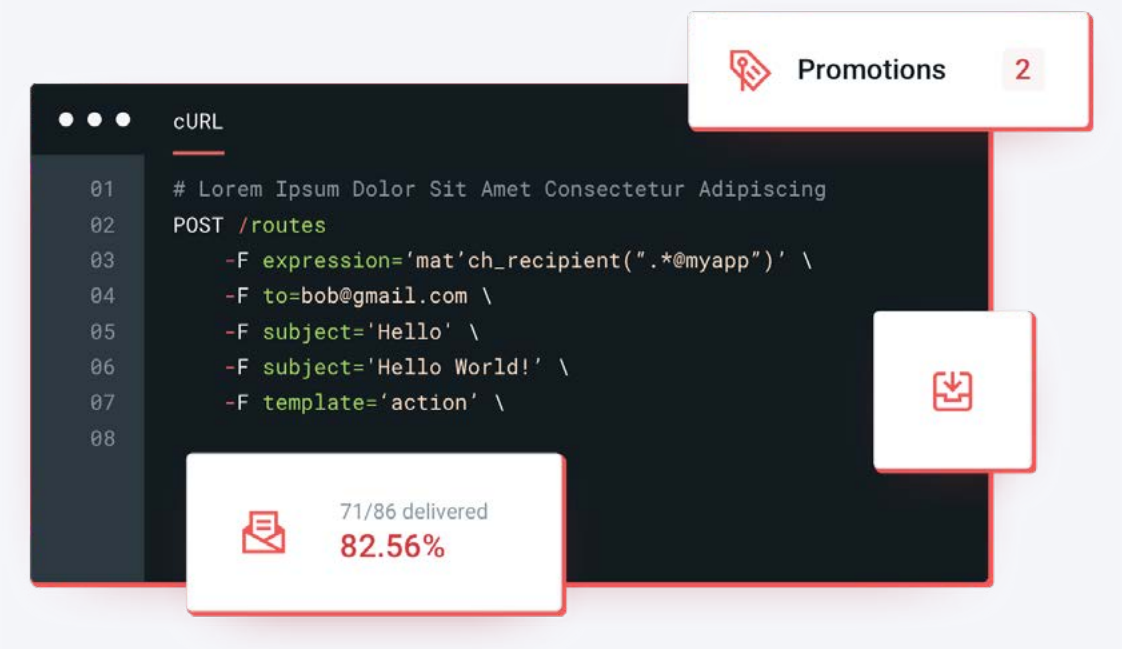
PART 4

Different mailbox providers, different tastes

Mailbox providers all have a different standard for legitimate email traffic, and they won't go out of their way to tell you whether or not you have met said standard. **Understanding specific needs for each mailbox provider takes a wealth of research and industry knowledge**, and goes beyond your standard authentication protocols.

For example, most mailbox providers check both your domain reputation and your IP reputation when your message reaches their servers, but each service provider weighs domains and IPs differently.

To add a layer of complexity, they won't tell you which one they weigh more, so it's difficult to know what to change if something goes wrong and all of your messages start bouncing or landing in the spam folder. If too many messages start landing in spam and hurting your reputation, entire subdomains and IPs can be tarnished for good, as building back that reputation can be a lasting effort on your part to fix with proper email best practice. It takes time to figure out what works and what doesn't, and all of that can change on a dime if they decide to change their filters.

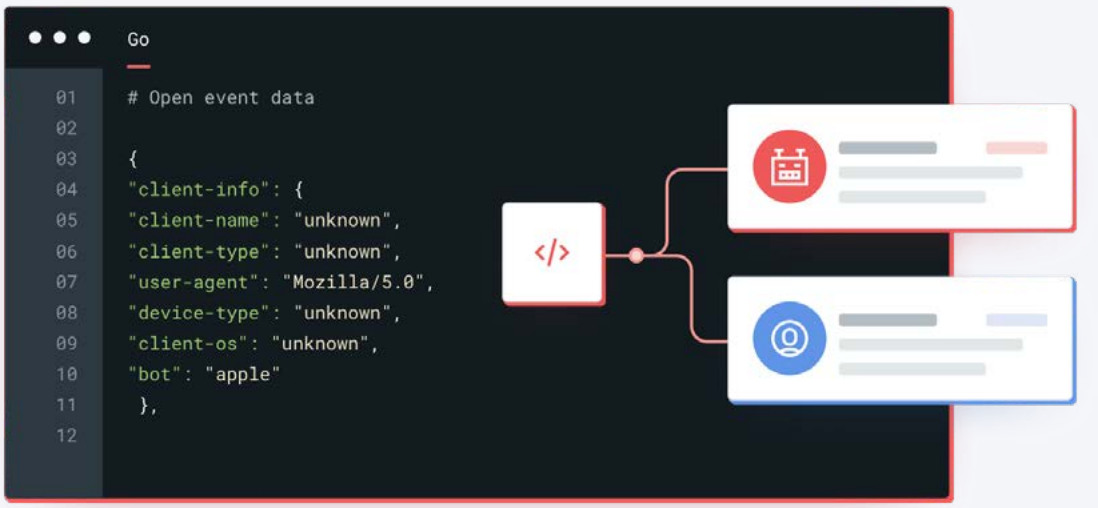


PART 5

Feedback loops

As a side note, most major mailbox providers provide feedback loops through which they give you information about spam complaints. **Signing up for these feedback loops is important to your overall deliverability** as they track the negative feedback you're receiving from your email recipients.

Signing up for these feedback loops can be time consuming, and it's important to be aware if your email service provider signs you up for these automatically, or if you need to do it yourself. While it is negative, ignoring this feedback causes your reputation to plummet, and will cause **your sending to be throttled or blocked completely**. If you're unsure about which feedback loops to sign up for, an email expert can help narrow down the list.



PART 6

Scaling accordingly

When you first construct your email program, your infrastructure is set up for your current volume at that time. As your business grows, so does your overall sending volume, and your overall traffic might need some IP and/or domain segmentation restructuring.

In theory, if you're sending over 100,000 messages a month you should be sending from a dedicated IP. Dedicated IPs are tied to one sender, rather than a shared IP that is linked to several senders at any given time. **Nobody else is able to influence the reputation of a dedicated sending IP besides the sender using it**, which in itself builds in a layer of reputation protection.

However, a fresh dedicated IP has no reputation tied to it whatsoever, and this plays into both your benefit and detriment. The benefit being that your reputation is protected from bad actors. If you were to send all 100,000 email messages at once from that brand new IP, mailbox providers will flag your sending as suspicious. Slow and steady wins the race in this case, but ramping up your sending will take time and measured effort.

PART 7

Adapting to a changing landscape

Outside of maintenance and adjusting your sending for growth, remember: the email landscape can change in an instant. If GDPR isn't evidence enough on that front, let's revisit the Yahoo and AOL merger. Two providers suddenly had to function under the same system and rules after Oath acquired both brands. The merger lead to a sizable group of senders being throttled by both providers, leading to hurt reputations all around.

In a similar vein, Gmail's filters are some of the most sophisticated on the market, and they're constantly changing their algorithms to combat spammers. While Google Postmaster Tools can inform a sender how their emails are performing, it's not enough. **It takes industry knowledge to truly set up your sending infrastructure** for each and every mailbox provider.

How many of your emails are bouncing, and which IP and domain are sending those emails in the first place? You've landed on a blacklist, but how respected is that blacklist by mailbox providers? Do you submit a delisting right away, or do you wait? Day to day deliverability care is imperative for continued success, and keeping on top of it all is a job in itself, but imperative to your sending success.

Mailgun's Deliverability Service is comprised of a team whose passion is understanding the intricacies of deliverability. Every day, **our employees show what it means to be an enterprise email partner**. We have the industry's most established, experienced team, and we all share a goal: helping you succeed.

> ***Note:*** *Within our deliverability service, our customers see an average of 97.4% delivery rates compared to the industry average of 85% and non-deliverability service customer average of 94%.*

Our team makes a point in understanding and learning about the changing landscape of email, and whenever changes occur, we're sure to make the changes necessary to keep nothing standing between your messages and the inbox. Your email program doesn't fit in a box, it fits in hundreds of thousands of mailboxes across the world, **let's work together to make sure you're landing in the right ones**.

PART 8

Resources

Can You Guarantee Better Email Deliverability?

Diving Head-First Into The Inbox: What's Impacting My Deliverability?

The Science and Art of Gmail Deliverability

How To Improve Your Email Deliverability In 2022

Email Authentication: Your ID Card For Sending

BIMI – More Than A Funny Name

Google Postmaster Tools: Understanding Sender Reputation

Yahoo And AOL Throttling – The Mailgun Festivus Airing Of Grievances Part Two

The Best DNS Blacklists – Not All Blacklists Are Created Equal

Well, This Is Awkward — Dealing With A Sudden Blacklisting

Email Statistics Report 2018- 2023

Over 100,000 companies worldwide use Sinch Mailgun to create elegant email experiences for their customers through world-class infrastructure. Brands like Microsoft, Lyft, and Etsy trust Mailgun's innovative technology and reliable infrastructure to send billions of emails every year. Built with development teams in mind, Mailgun makes sending, receiving, and tracking emails effortless for email senders of all sizes.

Mailgun was founded in 2010 as a response to the lack of developer-friendly, API-based email services. Since then, Mailgun has joined **Sinch**, a leading Communication Platform as a Service (CPaaS) provider, to become the developer-first email solution for their global customer base. GDPR, HIPAA, and SOC I & II compliant, Mailgun aims to provide the best email service possible with the utmost security and privacy.

For more information, please visit **mailgun.com**.