mailjet by sinch

EBOOK

Landing in the inbox: Deliverability basics

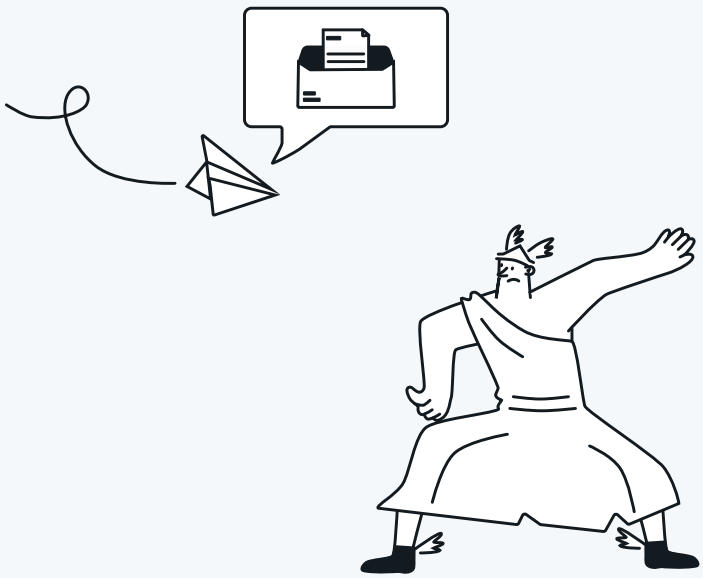
Table of contents

Welcome

There's nothing we hate more than seeing great email go to waste. Currently, one in every seven messages sent worldwide fails to land in the inbox, a number that can vary greatly by industry, country, and inbox. Email marketers are increasingly citing deliverability as one of their main barriers to effective marketing. Mailjet's Inbox Insights 2022 report found 28% of even the most-successful marketers call deliverability a concern.

There's no point spending time crafting great content if your messages never reach your subscribers' eyes. In this Deliverability 101 guide, we'll help you start off on the right foot and land your email to its intended destination. We'll also explore how to keep your subscriber engagement at the heart of your email strategy.

Fasten your seatbelts! We've got a bit of ground to cover before reaching destination success but don't worry, you'll enjoy the ride.



PART 1

First things first, what's deliverability?

Defining deliverability

Just how much goes on behind the scenes in the seconds between when you hit send to when an email lands in the recipient's inbox? A lot. In fact, as we mentioned earlier, one in seven emails don't even land in the inbox. They land in the spam folder, or sometimes even blocked by ISPs like Gmail and Outlook entirely. Deliverabiity is the umbrella term we use for issues that prevent an email from reaching its intended recipient.

Here are just some of the things that can happen that prevent email from reaching its destination:

- **Hard bounce:** A hard bounce is when an email is sent back to the sender because it couldn't be delivered for permanent reasons. It could be that the email address was typed incorrectly, or a fake one was entered because the subscriber was more interested in receiving the perk or offer for signing up than receiving your email. This is why it's always helpful to set up a double opt-in. We'll talk more about this later in the guide.
- **Soft bounce:** A soft bounce is when an email is sent back to the sender, but only for temporary delivery issues. This can be because the user's inbox is full, the server is down or the message is too big for the recipient's inbox.
- **Spam filters:** There are a lot of checks that happen when an email goes through the server ISPs (such as Gmail, Outlook, AOL) have filters set in place to protect spam or malicious email from landing in recipients' inboxes.

One thing to keep in mind is that deliverability rate is different from delivery rate. The two sound very similar, but shouldn't be confused. Deliverability rate is calculated as follows:

> ***Deliverability:*** *# of Emails that Land in the Inbox / # of Emails Sent*

Delivery rate actually includes all email accepted by the ISP, which includes email that lands in the spam folder, but doesn't include those that are blocked. You can have a 100% delivery rate, but if your deliverability rate is only 45%, you're missing out on a huge opportunity to communicate with your customers.

PART 2

Build the foundation for deliverability

Authentication

Making a good first impression with ISPs (i.e. Gmail, Outlook, etc) is very important since it will inform if and how they let you interact with your subscribers. But remember, they want the same thing as you: they want their users to have a stellar inbox experience. Here are some steps to win over those ISPs the first time you meet them.

There are many factors ISPs take into account when determining your sender reputation. Authentication is just one of those, but it's the first step to take to ensure you're headed in the right direction.

There are several authentication protocols you can use to signal to ISPs that you're one of the good guys:

SPF (Sender Policy Framework)

Haven't we all received spam email that's eerily similar to the look and feel of a reputable sender? It's surprisingly not very difficult to mimic the 'from' address to send spoof email. But fear not, this is where SPF comes into play!

SPF is one of the oldest forms of authentication, developed over a decade ago, along with DKIM. Did you know that prior to SPF outgoing addresses could be forged? It's still a common practice among spammers. SPF is a way for domain owners to take control over their own domain reputation by authorizing others to send email on their behalf. This automatically rules out anyone not on the approved list of addresses as spoofers. To learn more about setting up SPF, check out our handy guide here.

DKIM (DomainKeys Identified Mail)

This is a method the ISP uses to check that no phishy business has occurred in transit.

It allows you to add a unique signature to your email. The receiving server can check the domain signature to confirm the message really comes from where it claims to, and that the contents have not been tampered with along the way. Here is a guide to learn how to get your DKIM configured.

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

This is an added protective measure against domain spoofing. If SPF and DKIM methods ever fail, DMARC tells the recipient's domain what to do either reject the message or divert it to the junk folder.

Domain owners can use the **"p=" policy setting** to tell receiving servers what to do with email that doesn't pass DMARC validation.

In 2014, AOL and Yahoo announced a change in their DMARC policy, to p=reject, in response to ongoing security threats, and Google made a similar change at Gmail in 2016. Email will be rejected if the domains for the 'from' address and sender don't match. It's now no longer possible for ESPs to use sender address ending in @yahoo. com, @aol.com or @gmail.com to successfully deliver email on behalf of companies. Senders need to use their own domain because the ISPs increased their authentication measures. This helps prevent email forgery.

WHOIS

This lists all the contact information related to a domain name (i.e. the technical contact, the domain host, as well as the full name, email address, postal address and telephone number of each reference).

Setting your WHOIS to private is characteristic of spammers, so steer clear of providers who allow you to do this. This is one of the first things Mailjet will look into if a problem emerges.

Forward and reverse DNS lookup

Forward DNS lookup is when a domain name is used to locate an IP address. When you type a URL in your browser, the address is transmitted to a router nearby, which then finds the IP address. A reverse DNS lookup is simply the same process, backwards.

ISPs and email clients frequently use these processes to confirm your identity. If you're sending through Mailjet, we'll handle all of this configuration for you.

> *Suffering from acronym overload? Having trouble with set up? Our technical team is standing by 24/7, ready to help you out.*

Once you've figured all of this out, you should move on to reviewing your sending speed.

PART 3

Email delivery at a safe speed

Throttle your sending

Most people have a natural tendency to think that going as fast as possible is the best way to reach your destination quickly. Whether it's driving on a highway or sending emails, traffic police and speed bumps can cause serious issues. Ultimately, sending too much too soon, can mean more resistance on your journey.

Most ISPs monitor sending history to help them determine a sender's reputation. If the ISP filter catches any spike or deviation in volume, it can seem suspicious, and can lead ISPs to thinking the user's IP has been compromised. This can lead to a temporary block (or throttle) being put up against the sending IP (or domain) to protect end users and their inboxes.

The key is to take it slow and steady send at a consistent volume and frequency. When you're just getting started and you're looking to increase your sending volume, slowly ramp up so you don't raise a red flag with the ISPs.

Is a shared IP right for you?

SPs usually look back over your activity 30 days prior to your send. If you're an **infrequent or low-volume sender**, your reputation might be non-existent, even if you've been sending for a long time. This means you'd basically be rebuilding your IP reputation from scratch every month.

Luckily, with a shared IP, you can rely on other users to collectively uphold the reputation and volume history. The responsibility isn't all on your shoulders.

You'll also **save time and money**. A shared IP allows you to send larger volumes when needed, no warm up required. It is especially perfect if you're a seasonal sender, with high fluctuations throughoout the year. It's also less expensive than a dedicated IP.

At Mailjet, we monitor all our shared senders to check they're following deliverability best practices, as well as our Mailjet's Sending Policy. If a problem does arise, we use our trusted relationships with ISPs to address and correct the issue as soon as possible.

We can't always catch everything, though. There may be times when an email sent by someone using the same shared IP as you will affect the deliverability of your messages. As a result, if you're a large sender, we'd recommend a dedicated IP (a unique IP address dedicated exclusively to a single hosting account).

Owning a dedicated IP

Hey there, big sender! Using a dedicated IP allows you to isolate your reputation from other users, meaning that:

- You have more responsibility and control over your reputation
- We can more easily and quickly pinpoint the cause of any problems

Do you deploy over 10K emails each send? And, are you a frequent and consistent sender?

> *The dedicated IP option is available in our plans sending more than 150K emails per month and above.*

Warming up your brand new IP

If you're starting out with a brand new IP, you'll have no prior sender history for ISPs to go off. During your first few sends, they'll try to figure you out, judging the quality of your email and monitoring how recipients react to you.

To be on your best sending behavior, you'll need to **warm up** before sprinting ahead. Build up your sending volume consistently and gradually. A sudden spike in sending volume looks suspicious, so slow and steady wins the race. As we mentioned in the previous page, the warm up period isn't necessary for users sending emails from a shared IP. Find out how to warm up your IP using Mailjet

Separating your transactional and marketing email

Another important point to consider is to separate your transactional and marketing email to better identify and manage any deliverability problems.

Marketing email, by nature, is more likely to be marked as "spam" or generate unsubscribes. The reason behind this is that marketing email is sent in bulk to many contacts at once, often with little targeting or personalization. Transactional emails, on the other hand, are one-to-one communications sent to a particular recipient, typically after a specific action has been taken (i.e. a password reset, a purchase...), so it's important to keep your transactional messages separate to ensure their reputation isn't affected by this.

Still not sure where your needs stand? The Mailjet Crew can work with you to find or build a solution that best fits your specific sending behavior. Reach out to our support team if you're interested in learning more.

> *With Mailjet, you can create sub-accounts to easily separate your sending.*

PART 4

Your deliverability depends on your subscribers

Keeping ISPs & your recipients happy

As the old saying goes, "the customer is always right". Putting your customer first, making it a priority to be transparent and delivering what you promise ensures your subscribers stay engaged.

Authenticity and quality content are key in an increasingly competitive digital space. ISPs keep the inbox experience user friendly by tracking what types of content users are interested in receiving and which they don't care so much for (a.k.a. spam). Because of this, email senders with high engagement are inboxed more and those with low engagement often land in the spam folder. You can gauge your engagement levels with your contacts by looking at your open and click rates.

In order to win ISPs and your customers over, you want to appeal to your consumers with quality content. Be honest upfront, deliver what you've promised when they first opted-in and keep users engaged by connecting on an emotional level.

To ensure your content resonates with your recipients over time, make sure you segment your emails and use smart personalization to make them more relevant. Also, don't forget to clean your contact list regularly to remove inactive contacts and invalid email addresses that could harm your deliverability.

> *Head on over here to learn more about earning permission and keeping it over time.*

Opting-in & telling users what to expect

Establish explicit consent from your subscriber for the use of their personal data in all email communication.

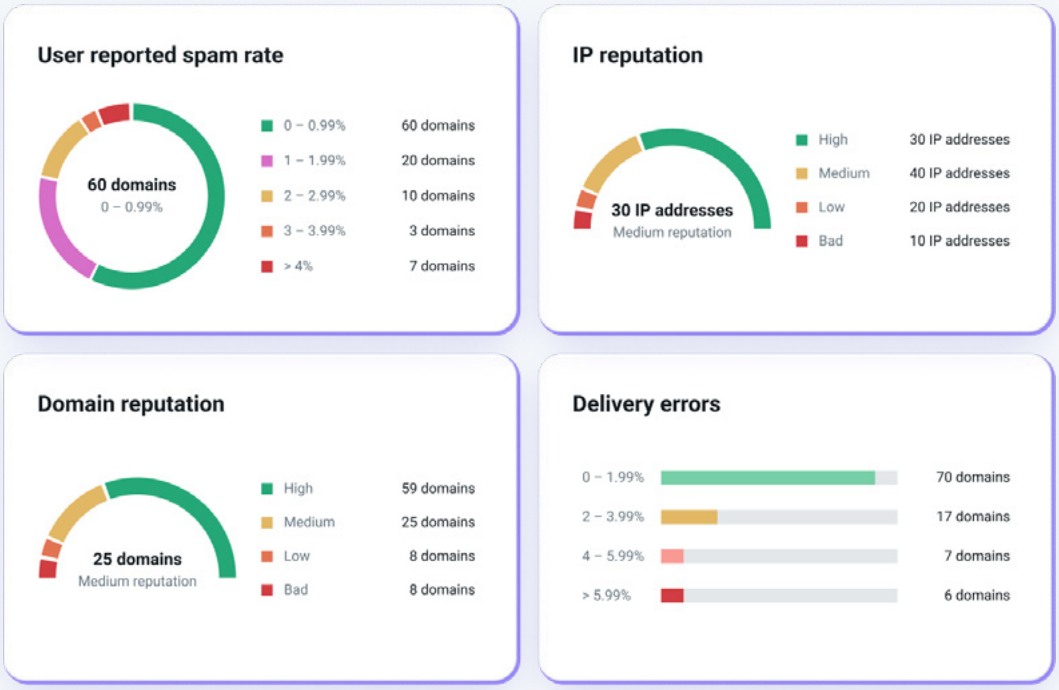
Being clear at opt-in ensures you have a cleaner list of contacts down the line. You'll want to tell your customers exactly what they are signing up to receive and how their information will be used. This builds trust and leads to higher opens and clicks and lower unsubscribes and complaint rates once subscribers start receiving your email.

Going back to the topic of double opt-in, which we mentioned earlier in this guide, sending a user a confirmation email with a validation link right after they subscribe can help to ensure that the email address given is correct, active and the user is excited about your content.

Empower your subscriber. The user has the right to be forgotten.

Make it clear that they can unsubscribe, and also ask you to erase their personal data records completely. Respond to these requests and promptly remove them from your list.

With policy reforms (such as the GDPR) ensuring that users have more say in what happens to their data, allowing your subscribers to easily manage their email preferences and handle their personal information has become even more important.



PART 5

Extra measures to increase your credibility

Use a domain name linked to an active website

Intentionally or accidentally using a domain name that links to a non-functional website makes you seem less credible, to both the user and ISP. It's something that many spam or phishing email senders do. It affects the legitimacy of your message (and sender reputation), which makes it harder to be verified by your contacts' servers.

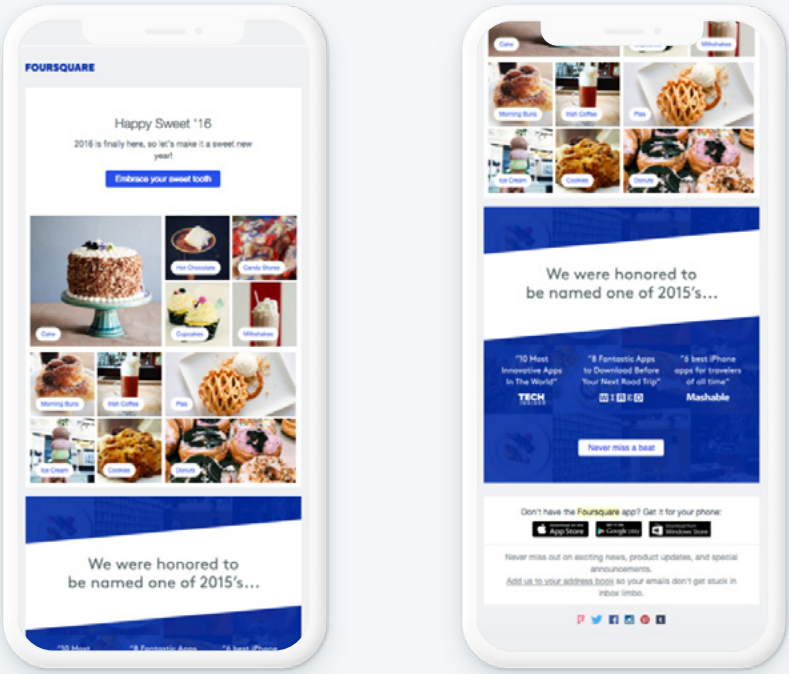
Make sure your domain name:

- Is recognizable and matches the brand you are promoting. For example, if you're sending on behalf of an ecommerce site for dogs, you might not want to use the sender domain "catsrule.com".
- Is linked to a website that's crawlable by search engines.
- Contains, at a minimum, an About Us page, a Privacy Policy page and detailed information on how to contact the company, either through a contact form or listing the company's contact email address, postal address and/or phone number on the website.

Configure abuse@ and postmaster@ email addresses

The abuse@ and postmaster@ addresses are used to receive consumer complaints and errors in processing, respectively. If these addresses aren't configured for your sending domain, these issues return an error to ISPs showing email clients you're not monitoring these messages. Needless to say, this doesn't help your credibility.

Beware, if our abuse@mailjet.com address is solicited, our team will be alerted and your practices may be put under the microscope. Also, note that these addresses are required for some whitelisting procedures, so if you want your reputation to be squeaky clean - go configure.



Get in your subscriber's good books

Users add senders they trust to their contacts. Invite your subscriber to add you to their address book this proves to spam filters that your recipients actually want to hear from you. Here's an example from Foursquare. They include a line at the bottom of each email providing subscribers a link to easily add them to their address book, so that emails don't get stuck in "inbox limbo".

PART 6

Some final thoughts for the road

The legal lowdown

Global spam laws are always changing. It's important to stay clued in on them so that you don't do your email an injustice.

Are you sending to or within:

- **The EU?** Be sure you are compliant with the GDPR when it comes to sending, and list management.
- **The US or Canada?** You'll need to be up-to-date with CAN- SPAM and CASL regulations, respectively. Also, make sure you're aware of any local data protection laws that apply in different states, like the California Consumer Privacy Act (CCPA).
- **The UK?** The Privacy and Electronic Communications (EC Directive) Regulations law made it illegal to send a subscriber an automated marketing message without prior consent. There are a few 'soft opt-in' exceptions though, where consent is considered implied. Read up on them here.

Spam laws may differ from country to country, but we've whittled them down to some universal, actionable takeaways:

Use a double opt-in as your first campaign, to gain user consent straightaway. A user may have provided the wrong address during signup or might even have signed up maliciously. Confirm that your customers are excited to receive your content and make sure you're not messaging an inactive account.

Include a clear unsubscribe link. Your sender name and unsubscribe link should be clearly identi able in all email sends not just for legal purposes, but also to honor your subscribers' rights.

So you've authenticated, found the right IP for you, and know how to keep your sender reputation fiying legally high.

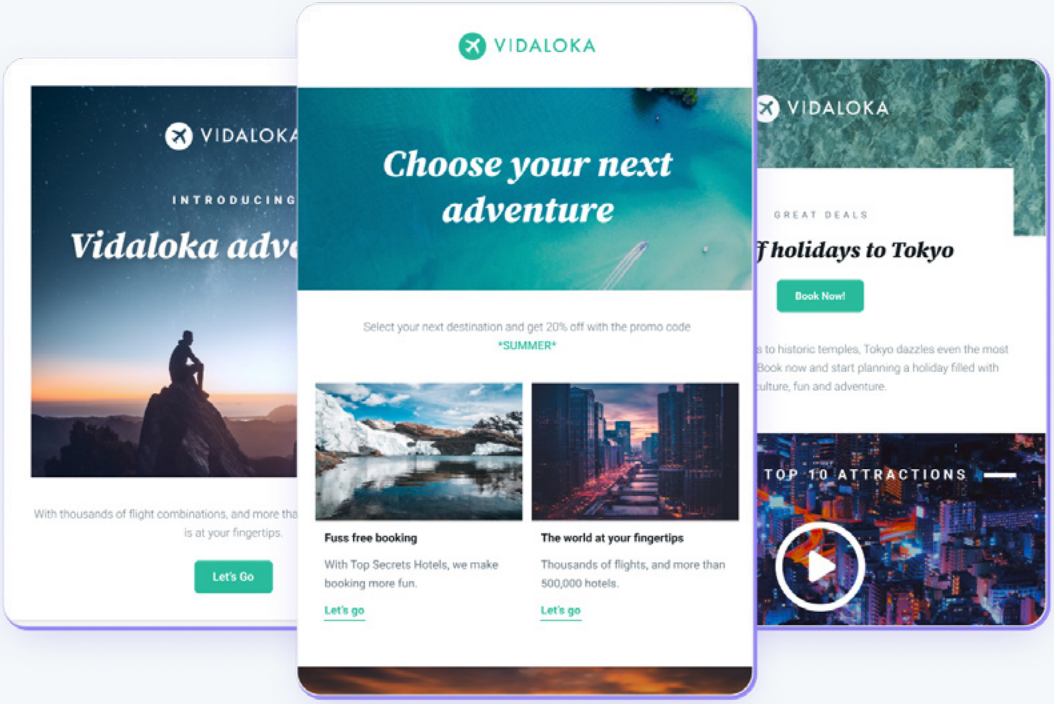
But maybe there's still something strange happening with your metrics? There's one more factor that may be affecting your deliverability failing to finetune your email to individual ISP requirements.

How to win over the most popular email clients

Nowadays, the most important metrics all email clients consider for inbox placement is user engagement (open, clicks...). All webmail providers have their quirks. You may have to tweak your tactics slightly to please their different personalities.

Gmail likes to categorize. Email continues to evolve into a more customer-centric experience. Most recently, Gmail introduced the tabbed inbox, which sorts messages by categories, including Primary, Social, and Promotions. The sorting algorithm is based on reported feedback from users. Give Gmail a helping hand and separate your transactional and marketing messages (as previously mentioned). This will also make sure your message gets in with the right crowd.

Hotmail, Outlook and Yahoo prefer to keep things simple. Hotmail and Outlook advise not to spread your email over too many IP addresses to keep your volume low. For Yahoo, plain and simple is the way to go. Don't include HTML forms, JavaScript, or embedded objects such as Flash or ActiveX.

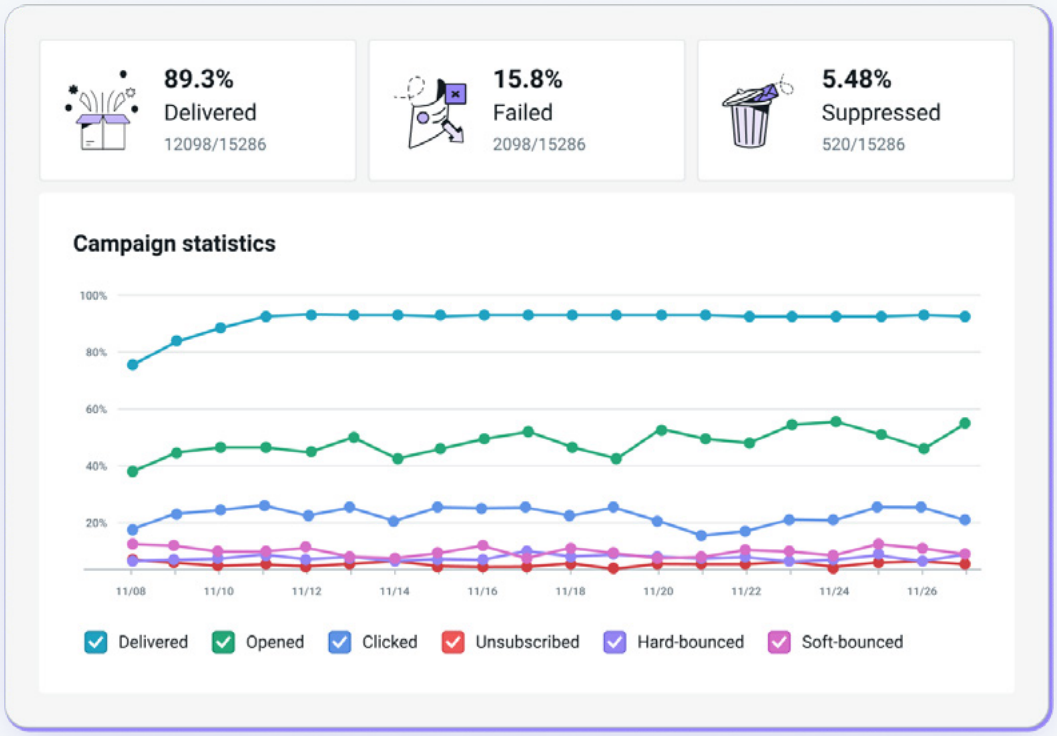


PART 7

Putting deliverability into action

Start putting these tips to work today. Don't let your hard work and budget go to waste by letting another email fall prey to the spam folder.

The Mailjet team prides itself in working to make deliverability one of our major strengths. We work closely with ISPs and email clients to take some of the weight off your shoulders, so that you can spend more time crafting awesome content.



PART 8

How we can help

At Mailjet, our mission is to help brands build better connected experiences, and the holiday season marks one of the most important times for brands to connect with consumers. Mailjet simplifies complex communication problems for more than 100,000 customers with these unique solutions:

mailgun by sinch

Mailgun by Sinch is the world's leading email delivery service. Developers and businesses use Mailgun's powerful API to send, receive, and track emails with a focus on simplicity and compliance to standards.

mailjet by sinch

Mailjet by Sinch is an intuitive email marketing platform that includes an easy-to-use email builder for beautiful designs, a contact management solution, and campaign analytics. Use Mailjet to drive results with meaningful emails.

email on acid by sinch

Email on Acid by Sinch is a leading email readiness platform that lets teams test and preview campaigns before hitting send. Take advantage of unlimited tests to address issues with client rendering, email accessibility, inbox display, and more.

inboxready by sinch

InboxReady by Sinch is a suite of applications that empowers marketers to optimize campaign performance and deliverability. Powered by Mailgun's reliable email infrastructure, InboxReady is a complete deliverability solution.

Use Mailjet's suite of tools to make sure your Black Friday emails and other holiday campaigns look amazing and get delivered. Find out why so many brands choose Mailjet.

More than 40,000 companies around the world use Mailjet by Sinch to strengthen connections with customers and subscribers while building their businesses through email marketing. Brands like Microsoft, Kia Motors, and Toast trust Mailjet to send billions of emails every year. Mailjet combines an intuitive, drag-and-drop email campaign builder with easy-to-use deliverability features to help businesses create and send beautiful emails without touching a single line of code.

Founded in Paris in 2010, Mailjet has offices in tech hubs around the globe, including the UK, US, Spain, Germany, and France. Mailjet is proud to be part of **Sinch**, a leading Communication Platform as a Service (CPaaS) provider, offering messaging, voice, and video communication solutions to a large global customer base. Mailjet is both ISO 27001 certified and GDPR compliant, offering its clients the highest levels of data security and privacy.

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