SINCH Mailgun

RESEARCH REPORT

State of email deliverability 2023

Industry benchmarks and expert advice on inbox placement

Table of contents

The journey to the inbox **3**
Key takeaways from the survey 4

1. **Email deliverability basics** **7**
Email infrastructure and deliverability 9
Transactional vs marketing emails 12
Delivery rate benchmarks 14

2. **Deliverability challenges and measurement** **17**
Top email deliverability challenges 17
Measuring email deliverability 18
Exploring the inbox placement rate 22
What's your reputation? 24

3. **Blocklisting and its impact** **31**

4. **Email authentication** **38**
Email authentication essentials 38
SPF and DKIM usage 39
DMARC implementation 41
DMARC policy options 42
BIMI adoption 45

5. **List building and hygiene** **50**
Bad list building habits 50
Good list building habits 52
List hygiene processes 56

6. **Best practices for better deliverability** **62**

7. **Deliverability: Why IT and marketing need to team up** **66**

How we can help **67**

About this survey **68**

INTRODUCTION

The journey to the inbox

To many people, it seems so simple. Hit send and an email shows up in the inboxes of intended recipients. The truth is, there's a lot that happens before and after an email reaches its final destination.

Email deliverability can be a misunderstood topic. That's partly because there are so many factors involved in determining where emails end up. Every sender wants to avoid the spam folder as much as possible, but you also have to worry about getting blocklisted or bad actors spoofing your brand.

At Sinch Mailgun, we're lucky to have teams of people who are experts on the ins and outs of email deliverability. We also have access to thousands of senders around the world, including customers from our sister brands, Mailjet by Sinch and Email on Acid by Sinch.

In the first half of 2023, more than 1900 senders took part in a survey so we could learn more about their understanding of what it takes to make it to the inbox and how they approach email deliverability. We also asked our in-house deliverability experts to offer insights on the survey results and advice based on their experience.

To sum things up, what you don't know about deliverability could hurt you. **Not making it to the inbox can have significant effects on everything from business operations to brand reputation.** But when you invest in improving and maintaining good email deliverability, you're going to see a positive return.

"Email is a channel that is often celebrated for its high return on investment. However, that ROI decreases as email deliverability issues increase. Email is a great source for revenue generation, but when messages end up in spam, people are extremely unlikely to take action. It doesn't matter how cost-effective email is. If your campaigns aren't reaching people, your ROI is zero."

Kate Nowrouzi, VP, Deliverability and Product Strategy, Sinch Mailgun

Key takeaways from the survey

When we reviewed the survey results and looked at the big picture, a few themes emerged:

1. A lack of email deliverability knowledge is common.
2. Senders are missing major opportunities to improve deliverability.
3. Getting into the inbox supports a better customer experience.

Here's more on these three key takeaways:

Lack of email deliverability knowledge

While more than 1900 senders from around the world completed the survey, many started answering our questions and didn't finish. We heard from people who told us they abandoned the process because they simply didn't know enough to answer everything. That lack of knowledge led to lots of uncertainty.

Deliverability experts are a rare breed. **Just 4% of survey participants claimed to hold the job title of Email Deliverability Specialist.** That's one reason why we offered an **Unsure** option with certain technical survey questions. The option was often selected around 25% of the time:

- More than 27% of senders are unsure of their delivery rate for marketing emails.
- Another 27% could not describe their organization's email sending infrastructure.
- Among senders using DMARC for email authentication, 40% were unsure of their policy.
- 24.5% of senders in the survey were unsure if they'd been blocklisted in the last two years.

The uncertainty isn't exactly surprising given the variety of businesses, email program complexity, and send volumes. Still, all these things are important to know, especially if you place importance on getting to the inbox.

Missed opportunities for businesses

The failure to follow certain email deliverability best practices was another sign of the need for more knowledge. These are major missed opportunities that could greatly improve the chances of landing in the inbox:

- 38.7% of senders say they **Rarely** or **Never** practice email list hygiene.
- Another 38% admitted they are **Not monitoring sender reputation**.
- More than 50% of senders are not yet automating the list-cleaning process with helpful tools.
- Nearly 60% said they have not implemented a sunset policy to identify and properly manage non-engaged contacts.

Throughout this report, we'll explain why these factors and others are important best practices that lead to a healthy email program.

Supporting the customer experience

There is good news for those who focus on improving email deliverability. Senders who prioritize inbox placement say it's about more than getting a higher percentage of messages delivered. **Better email deliverability supports a better customer experience.** And those who've had problems with deliverability learned the hard way.

- 40% of senders who prioritize deliverability say the biggest benefit is **Improved customer satisfaction**.
- Among senders who've been blocklisted, **Delays for important messages** was the biggest negative impact at 33.5%.
- Another 22% said the biggest impact of getting blocklisted was **Dissatisfied customers.**

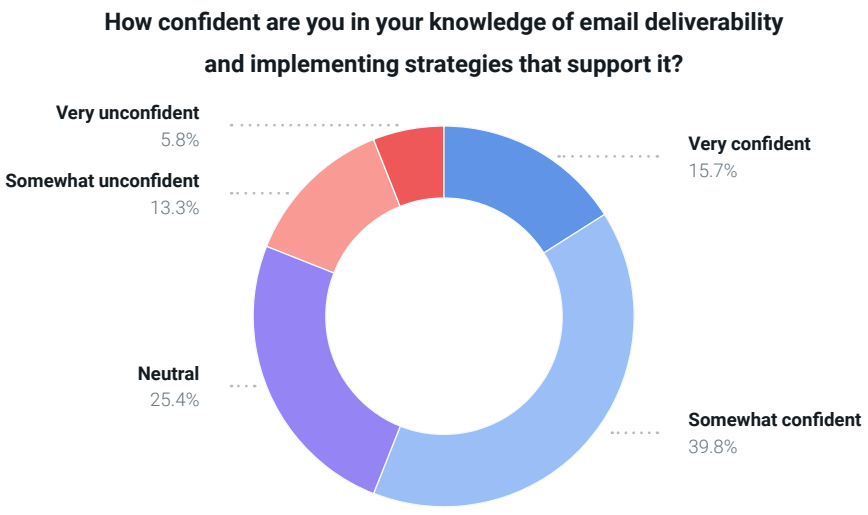
From password resets to special promotions, valuable information is delivered via the email channel every day. Many of your contacts are expecting and anticipating the arrival of those messages. When they get delayed, land in spam, or never show up, it erodes trust, causes frustration, and could easily reduce your revenue.

That's why focusing on deliverability is an excellent way to increase your return on investment (ROI) from the email channel. In fact, a 2023 Forrester Consulting Total Economic Impact™ study on Sinch Mailgun found that a composite organization would see a **264% ROI after just three years.** That's thanks in no small part to hundreds of thousands of dollars in incremental revenue from improved deliverability.

> *Focusing on deliverability is an excellent way to increase your return on investment (ROI) from the email channel.*

What do senders really know about deliverability?

We asked the senders who took our survey to rate their knowledge of email deliverability and their propensity to carry out practices that support inbox placement. Results show that close to half of respondents feel at least **Somewhat confident** in their abilities while less than 20% admit to lacking confidence around the topic.



But it's possible that some of that confidence is overstated, and other results in our "State of email deliverability" report reflect that possibility. **When you don't know what you don't know, it's easy to feel like you've got all the knowledge you need.** So, let's take a closer look at how email senders around the world are addressing deliverability. Watch for our deliverability experts to clear up confusion and add advice along the way.

"I know people spend a lot of time strategizing and building the email itself. When they send it out, if it goes to the spam folder for half their list, they're probably left wondering why. I think it's unfortunate, but it's the result of not understanding all the things that could impact email deliverability."

Nick Schafer, Sr. Manager of Deliverability and Compliance, Sinch Mailgun

PART 1

Email deliverability basics

A common misconception is that email deliverability is simply about getting messages delivered. But it's much broader than that. **The true definition of email deliverability involves following a set of practices, processes, and protocols that increase the likelihood of messages getting delivered to subscribers' inboxes.**

"Delivered to subscribers' inboxes" is the key phrase here. When an email is delivered, it means the receiving mail server has accepted the message. What happens next is still up in the air. Mailbox providers filter delivered mail, sending some to the inbox and some to spam. Messages may also land in other folders that are part of the main inbox, including promotions, updates, and social media.

For most legitimate email senders, reaching the inbox and avoiding the junk folder is a big deal. We asked survey participants to rate how much of a priority deliverability is to their companies. It's clear that inbox placement is an important business objective.

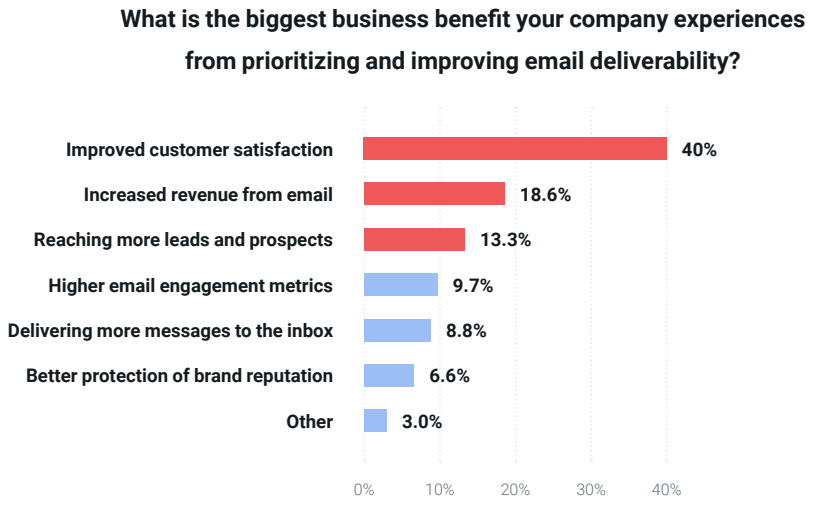
The question is, how is the goal of high deliverability achieved, and what does it look like? First, realize that many things can affect your ability to land in the inbox:

- Email sending infrastructure decisions
- Levels of engagement from subscribers
- Email authentication protocols
- List building and list hygiene practices
- Unsubscribes and spam complaints
- Sudden changes in send volume
- New sending IPs or domains
- Your reputation with major mailbox providers
- Changes in mailbox provider spam filtering technology
- And more...

Some of these factors are highly technical and others are connected to email marketing strategy. Most are in your control, but sometimes deliverability issues aren't even your fault.

So, what's the payoff for investing time and resources into improving email deliverability? We asked senders who rated the importance of deliverability at 60 or higher to choose the biggest benefit to their business.

Senders selected the benefit of **Improved customer satisfaction** (40.1%) most often. That more than doubled the next most popular option, **Increased revenue from email** (18.6%). Rounding out the top three benefits of prioritizing email deliverability was **Reaching more leads and prospects** (13.3%).



Remember that there are different types of emails. People *expect* to receive **transactional emails**. They usually *sign up* to receive **marketing emails** from brands they trust, and they *hate* getting unsolicited **spam emails**.

If an important transactional email never shows up, that could certainly create a dissatisfied customer. Yet even a missing marketing email can be disappointing. Imagine missing a promo code from your favorite online store or that a newsletter you look forward to reading gets lost in the spam folder.

"With transactional messages, recipients obviously do not want to wait for a password reset email, or for an MFA/2FA email. Or worse, for those emails to not arrive at all. They would expect those specific emails to come to their mailboxes almost instantly. Any transactional email that is delayed, or not delivered at all, could be quite problematic to your end-users."

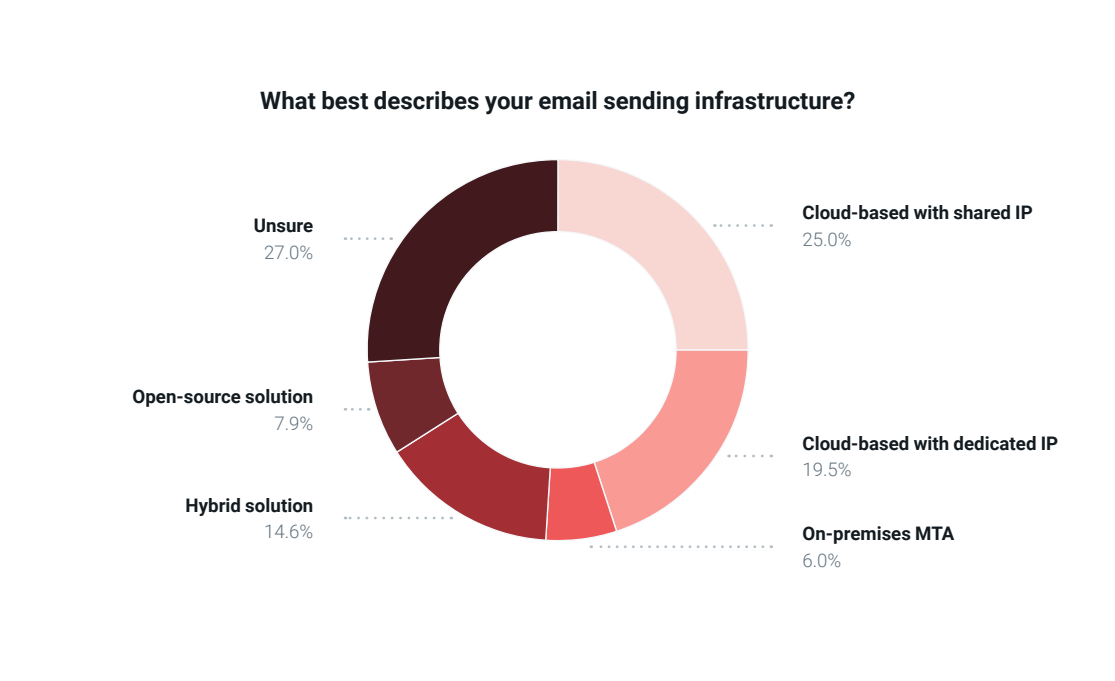
Alexandre Zibrick, Compliance and Deliverability Engineer, Sinch Mailgun

Email infrastructure and deliverability

Let's take a step back to the beginning of an email's journey to the inbox. Emails pass through a variety of servers, mail transfer agents (MTAs), filters, and rendering engines before recipients ever look at the message.

Bulk email gets sent from a particular domain and IP address. The IP address may be shared with other senders, or it could be a dedicated IP for a specific sender. There are senders who have their own email servers on premises, those who use cloud-based platforms, and those with a hybrid solution for email sending.

Here's a breakdown of email infrastructure among the senders who took our survey. As you can see, the two cloud-based options are a bit more common than others, with 25% sending from the cloud on a shared IP and 19.5% using a dedicated IP. Only 6% have an **On-premises MTA** and 14.6% use a **Hybrid solution**.



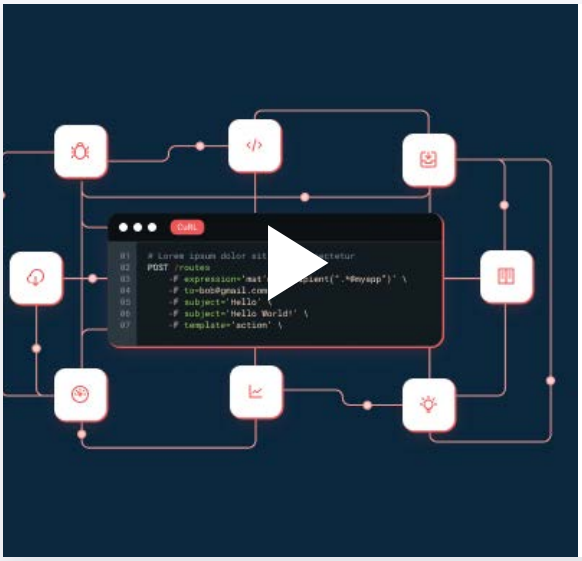
Many organizations have launched large-scale digital transformation projects in which they've migrated to the cloud. Email sending infrastructure (as well as secure data storage) is one of the biggest opportunities for taking advantage of what the cloud has to offer.

Perhaps the biggest advantage of a cloud-based email infrastructure is what you *don't* have to do. Putting email infrastructure in the cloud takes a lot off your plate, including many upfront expenditures and ongoing pressures involving upgrades, security, and compliance. Check out the comparison table for more on cloud vs on-premises email infrastructure:

Main characteristics of on-premise	Main characteristics of cloud-based
Large upfront cost	Pay-as-you-go subscription
Hardware/software installation and licensing	No installation, fast onboarding
Full control over your infrastructure	Third-party hosting
Responsible for all compliance	Cloud-provider responsible for compliance
Larger ongoing costs (maintenance, on-site staff, etc.)	Not responsible for server maintenance

Main characteristics of on-premise	Main characteristics of cloud-based
Responsible for physical and cyber security	Provider responsible for meeting security standards
Support your own infrastructure	Providers offer dedicated IT staff, support, and additional services
Limited to the devices you use for installation	Access on a large number of devices, supports integration with other tools, and securities like single-sign on (SSO)

Choosing cloud-based email infrastructure reduces a sender's concerns, obligations, and overhead costs. In the end, that contributes to increased email ROI.



WEBINAR

Everything you need to know about dedicated IPs

Find out more about email infrastructure when you watch a webinar recording featuring Sinch Mailgun experts. They answer all the toughest questions about using a dedicated IP for email sending.

Watch Now

"When you pick a cloud-based email service provider like Sinch Mailgun, we do all of it for you. You don't even have to think about it. You don't have to worry about security updates, vulnerability patching, or hardware updates. We handle all of that, and it reduces costs associated with email in the long run."

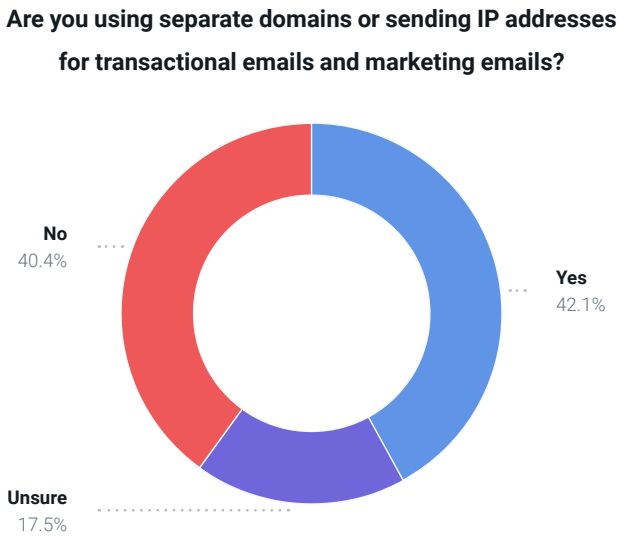
Natalie Hays, Product Marketing Manager, Sinch Mailgun

Transactional vs marketing emails

A smart email infrastructure decision for many senders with higher volumes is the separation of transactional and commercial messages on different IP addresses or subdomains. Better deliverability is the reason why.

Transactional messages *are not* bulk email. Password resets, two-factor authentication, invoices, shipping updates... these types of time-sensitive, automated messages are sent to individuals – not a huge list of contacts. But grouping transactional emails with mass marketing messages could cause deliverability problems.

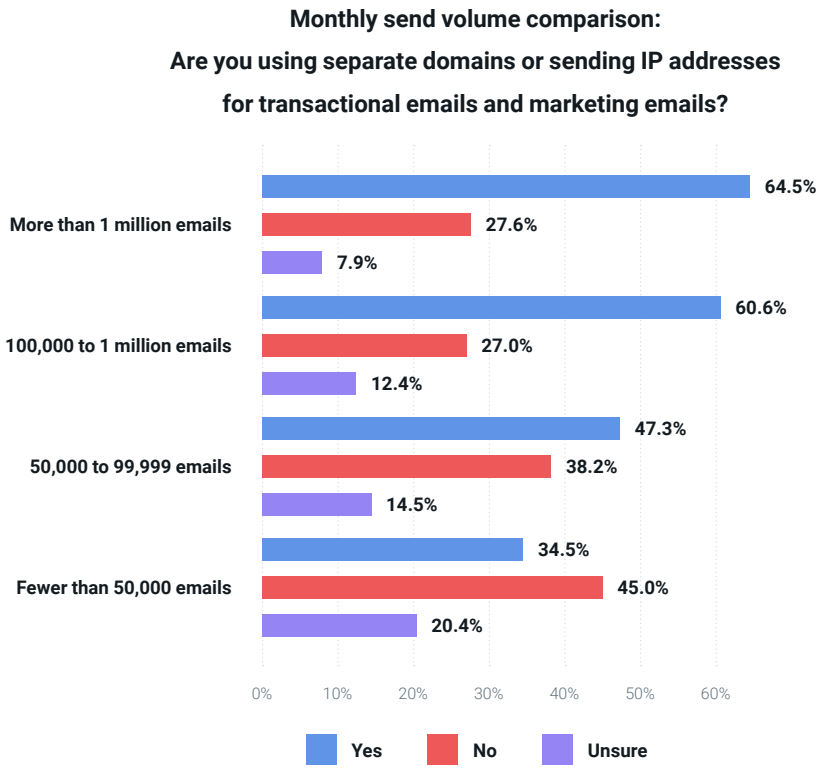
Mailbox providers are monitoring your sending practices. You don't want them to get confused and lump transactional emails with marketing messages. **That's why more than 42% of senders in our survey use separate subdomains or sending IPs for transactional and marketing emails.** However, another 40% of senders say they are not separating transactional communication from email marketing messages.



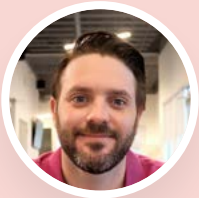
The reason for the separation is straightforward. Marketing emails are more likely to be marked as spam, have a higher number of unsubscribes, and have lower engagement rates. As a result, mailbox providers are also more likely to filter marketing emails into junk/spam.

Separating transactional emails from marketing sends a clear message to mailbox providers that your transactional communications are to be treated differently.

The practice of separating these two types of email communication is more common among high-volume senders. While more than 60% of senders with a volume of more than 100,000 emails per month are isolating marketing email traffic from transactional, far fewer senders with a volume below 100,000 emails per month are doing the same.



There are also situations in which senders separate emails even further. For example, high-volume senders with more complex email programs may have different subdomains for abandoned cart emails, win-back campaigns, or unsolicited cold emails from sales. **This strategy ensures you have better control over deliverability for your most important messages and campaigns.**



"It's a smart move to separate mail streams. If you have cold sales emails going out from the same sending domain as your marketing campaigns, that's not a good idea. I don't recommend sending unsolicited emails at all, but I know it happens. Cold sales emails have a bad reputation, and they'll get marked as spam. You don't want any chance of that bleeding over to your transactional or marketing messages."

Nick Schafer, Sr. Manager of Deliverability and Compliance, Sinch Mailgun

Delivery rate benchmarks

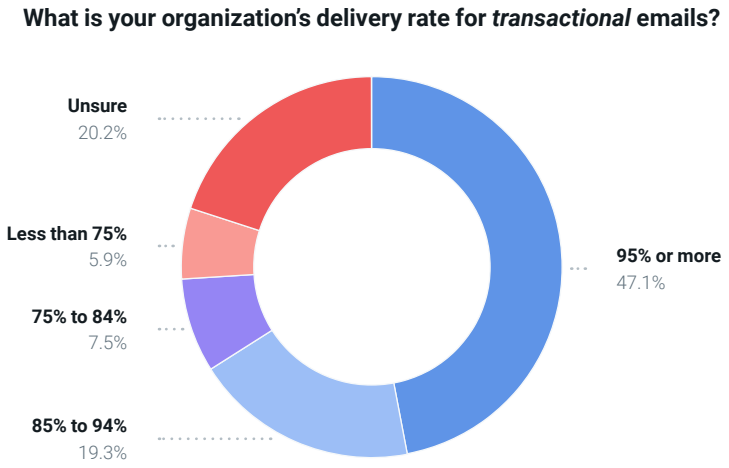
The delivery rate is the metric most often associated with email deliverability. While it doesn't tell the entire story, it does let a sender know the percentage of emails that are received and accepted by mailbox providers. **One of the biggest misconceptions among senders is that email deliverability is all about the delivery rate.**

It's important to understand that the delivery rate metric only measures the number of emails that mailbox providers accept, not where emails ultimately end up. The simple equation for the delivery rate percentage is:

```
(# of messages delivered ÷ # of messages sent) X 100
```

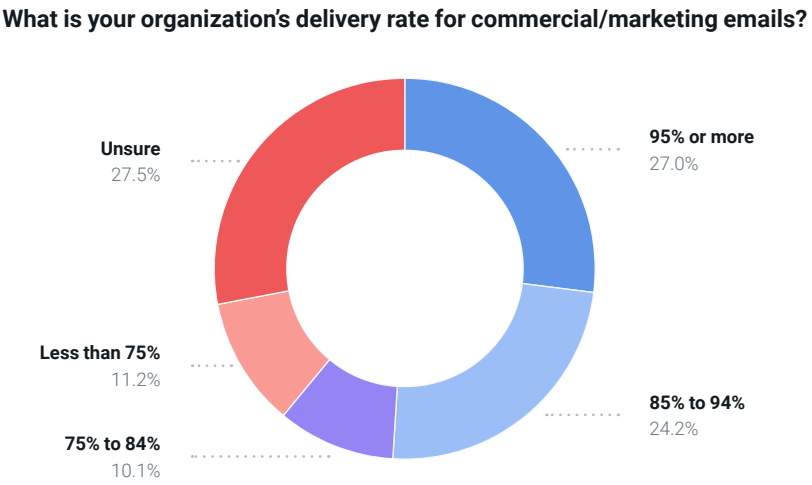
This excludes messages that bounce because of an invalid email address or a full mailbox, for example. It also excludes messages that mailbox providers reject or block for any reason. So, to be clear... **if emails are landing in spam, they still count toward the delivery rate.**

For this report, we asked senders to select from a range of delivery rates for both transactional and marketing emails. **Just over 47% of respondents reported a delivery rate of 95% or more for transactional emails.** However, a combined 13.4% reported delivery rates below 85% for transactional messages.



A delivery rate below 85% means 15% or more of transactional messages never get delivered at all. If more than 1 out of 10 transactional messages never arrive, that could definitely be an issue. In fact, separate research from Mailjet by Sinch suggests **93% of consumers would consider switching to a rival brand after a bad experience with transactional emails.**

Reported delivery rates for marketing emails are noticeably lower than transactional emails. **The survey found that only around 27% of respondents have a delivery rate of 95% or higher for marketing emails.** More than 21% of senders reported delivery rates below 85% for marketing emails. These findings further support the strategy of separating transactional and marketing messages for deliverability purposes. When sent from the same IP or domain, the poorer reputation of marketing emails may carry over to your transactional communications, which can drag down their deliverability.



Lower delivery rates are a sign of deliverability issues such as emails getting blocked or having lots of invalid contacts on your list that are bouncing because they are fake, non-existent, or had a typo in the email address. Mailgun experts say that even a 95% delivery rate for transactional messages is reason enough to take a closer look at the situation.

"For pure transactional email traffic, I would expect a 99% delivery rate and never much below that. For marketing emails, I think you should always aim for at least 95%. If you aren't achieving that, you need to take a closer look at your program and practices right away. If I were to see a transactional delivery rate below 75%, I would be very concerned."

Alexandre Zibrick, Compliance and Deliverability Engineer, Sinch Mailgun

PART 2

Deliverability challenges and measurement

As we've already established, a lot goes into email deliverability and plenty of things can keep emails from landing in the inbox. We asked senders in our survey to identify their biggest deliverability challenges.

Respondents were given a list of common challenges and asked to identify and rank the top three. The results reveal that the three biggest challenges are avoiding spam folders, increasing delivery rates, and staying off email blocklists.

Top email deliverability challenges

(Respondents selected and ranked their top three options)

1. **Staying out of the spam folder**
2. **Getting more emails delivered**
3. **Staying off email blocklists**
4. **Reducing email bounces**
5. **Maintaining list hygiene**
6. **Low subscriber engagement**
7. **Improving sender reputation**
8. **Complying with regulations**
9. **Setting up email authentication**

Interestingly, more complex topics such as compliance and email authentication placed lower in the ranking of challenges. **Our in-house experts note that the top three deliverability challenges represent ongoing frustrations for senders.** The second half of the list includes challenges like authentication, which is highly technical but doesn't need much attention once it's set up.

This ranking of deliverability challenges was the same for both high-volume senders with more than 100,000 emails per month and low-volume senders with under 100,000 emails sent per month. So, it's clear that keeping messages out of the junk mail folder is a top priority. But even legitimate emails end up in spam for various reasons. That's why deliverability needs to be a focus if you want to experience higher email ROI.

"I absolutely agree that staying out of spam is the biggest problem for senders because most people rarely check their spam folders. Deliverability is all about getting to the inbox. You need to follow best practices to achieve a higher inbox placement rate."

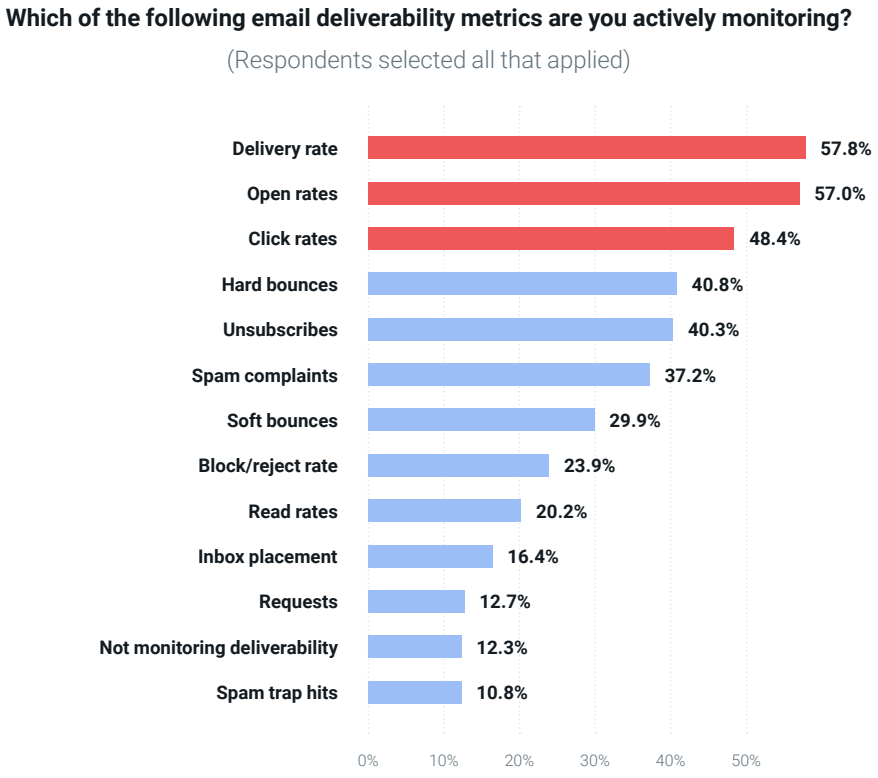
Kate Nowrouzi, VP, Deliverability and Product Strategy, Sinch Mailgun

Measuring email deliverability

It's tough to track email deliverability. There's no easy way to look into the inboxes of every subscriber on your list to find out how mailbox providers filtered your message.

That's why part of tracking email deliverability involves monitoring metrics that indicate signs of potential trouble. There are also email metrics you want to keep high because they show that you're sending to a healthy, engaged list of subscribers. Measuring engagement matters because it's one way that mailbox providers judge the reputation of senders, helping them decide whether a message should go to the inbox or spam.

Our survey asked senders around the world to identify all of the deliverability metrics they actively monitor. **More than 12% of respondents admitted they don't track deliverability at all.** Among those who are monitoring deliverability metrics, the **Delivery rate** topped the list at nearly 58%. **Open rates** (57%) and **Click rates** (48.4%) rounded out the top three.



We explained in the previous chapter that delivery rates only tell part of the story about email deliverability. So, while it is certainly a key metric, senders need to dig further into their analytics and measure other factors connected to deliverability.

> *One of the biggest misconceptions among senders is that email deliverability is all about the delivery rate.*

You may wonder what opens and clicks have to do with deliverability. Our deliverability experts explained that it's important to monitor these engagement metrics over time because they reflect list health and can alert you to potential problems.

"A quick and easy way to monitor how your email marketing program is performing is to look at your unique open rates trend over time. In an ideal word, it should stay stable, or better yet, increase. If you start noticing a trend of open rates dropping, it is usually a good indicator that you are facing email deliverability issues."

Alexandre Zibrick, Compliance and Deliverability Engineer, Sinch Mailgun

There are two reasons the open rate is related to deliverability:

1. A good open rate shows mailbox providers your subscribers are engaged and want to receive your emails. This improves your sending reputation and makes emails more likely to land in the inbox.
2. A sudden dip in the open rate could be a sign you've got more emails than normal that are landing in spam.

Unfortunately, opens aren't the most reliable email metric. Measures such as Apple's Mail Privacy Protection (MPP) can inflate open rates because bots automatically open emails. As a result of this inaccuracy, many senders are focusing more on clicks to better measure email performance and subscriber engagement.

Hard bounces (40.8%), **Unsubscribes** (40.3%), and **Spam complaints** (37.2%) are all important deliverability metrics to monitor as well. Here are some reasons why:

- **A high hard bounce rate is a sign you need to look at list hygiene.** You are likely sending to inactive or invalid email addresses, which should be removed.
- **Unsubscribes are a natural part of the subscriber lifecycle.** But too many unsubscribes mean you should review your sending practices, including frequency and content relevancy.
- **Spam complaints are much more serious than unsubscribes.** They are a strong signal to mailbox providers that your emails are unsolicited and unwanted.

The average unsubscribe rate is around 0.1%. That's one unsubscribe for every 1,000 emails delivered. While most senders hate to see a subscriber leave their list, you should make the unsubscribe process simple and straightforward. When it's hard to unsubscribe, your emails are more likely to be marked as spam.

Your spam complaint rate should be significantly lower than the unsubscribe rate – shoot for about 0.02%. At Sinch Mailgun, our Acceptable Use Policy (AUP) requires that senders on our platform keep their complaint rate at or below 0.08%.

Here are some quick tips to help keep your spam complaint rate low:

- Include an easy-to-find unsubscribe link in every email.
- Use a double opt-in process to ensure new subscribers want your emails.
- Find the right sending frequency by monitoring email engagement and staying consistent.
- Remove unengaged subscribers before they start complaining.
- Segment your lists and personalize emails to keep them interesting and relevant to recipients.

If you want to learn more, check out our blog post with advice on keeping spam complaints in check.

With both spam complaints and unsubscribes, you must stop sending to those contacts immediately. Failing to do so could definitely damage email deliverability. Plus, it could also get you into legal trouble as there are privacy laws requiring that senders respect removal of consent.

Perhaps the most important metric of all is buried near the bottom of the list. **Inbox placement is the ultimate email deliverability metric.** It tells senders whether delivered emails made it to the inbox or landed in spam. Yet only 16.4% of survey respondents say they are actively monitoring their inbox placement rate.

"I was very surprised to see Inbox Placement listed so low, especially because deliverability is all about getting your messages into the inbox."

Ashley Rodriguez, Deliverability Engineer, Sinch Mailgun

Exploring the inbox placement rate

Before we further explain what makes the inbox placement rate valuable and how it works, let's make sure we're clear on what defines this metric and what makes it different than the delivery rate.

Here's a comparison of how the two metrics are calculated:

```
Delivery rate % = (# of messages delivered ÷ # of messages sent) X 100

Inbox placement rate % = (# of messages in the inbox ÷ # of messages
delivered) X 100
```

Inbox placement tells you what happened to all the emails that were successfully delivered. If your inbox placement rate is 85%, that means as much as 15% of your messages were filtered into spam.

So, why don't more senders monitor inbox placement? One reason is that it's not a metric you can easily find in reporting from a typical email service provider (ESP). That's because providing a report on inbox placement requires some extra work.

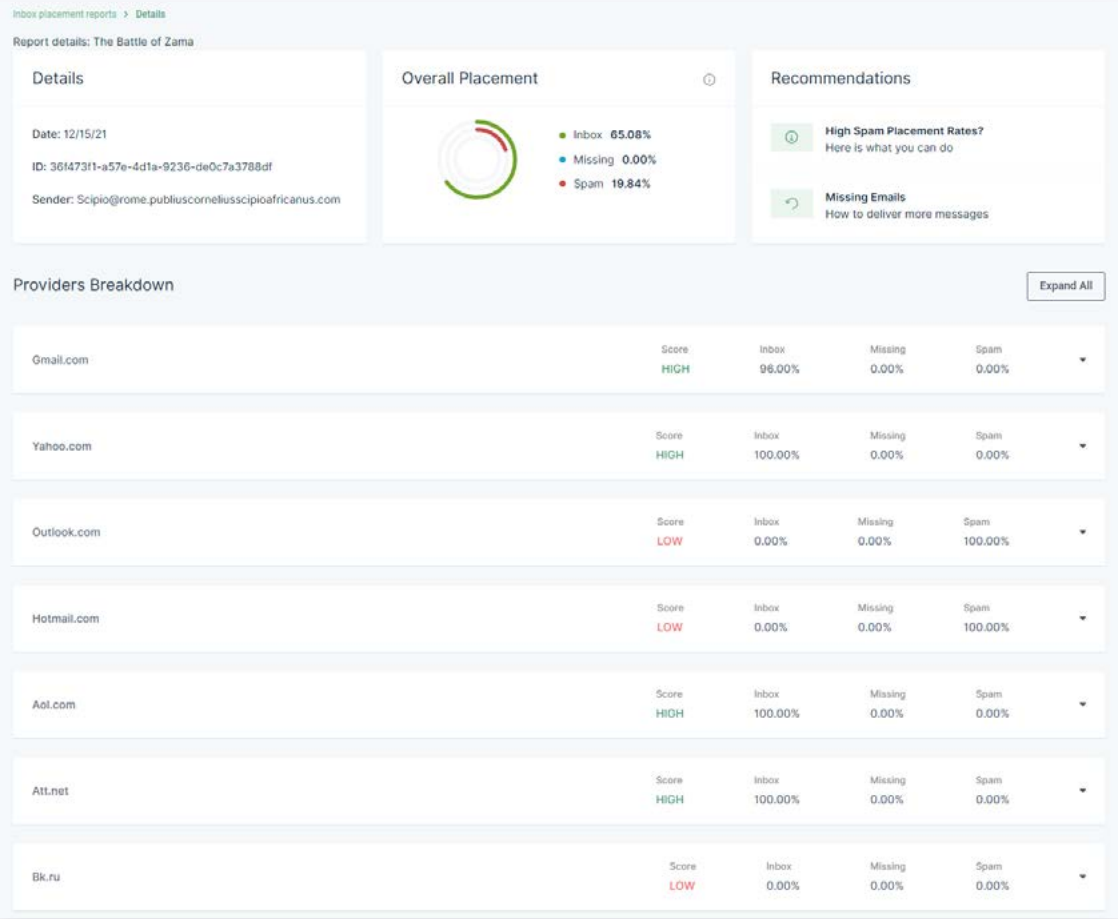
"People may not even be aware that there are ways to track the inbox placement rate. It's not a metric that can be measured in the traditional sense. Most providers can show opens, clicks, bounces, and delivery rates pretty easily. But to do an inbox placement test you need to do something else. You need to use a seed list and seed mailboxes."

Nick Schafer, Sr. Manager of Deliverability and Compliance, Sinch Mailgun

How inbox placement testing works

Inbox placement reports are based on results from sending to email addresses and mailboxes that aren't actually on any of your contact lists. You can conduct inbox placement testing to understand where your emails are likely to land before you send to your actual list.

A seed list includes addresses from a range of mailbox providers that the sender or email service provider owns and uses for testing. Some senders create their own seed lists to test inbox placement, but these tend to be much more limited than the seed lists and mailboxes that an ESP such as Mailgun provides. So, finding a service that offers inbox placement testing is the best way to ensure accuracy.

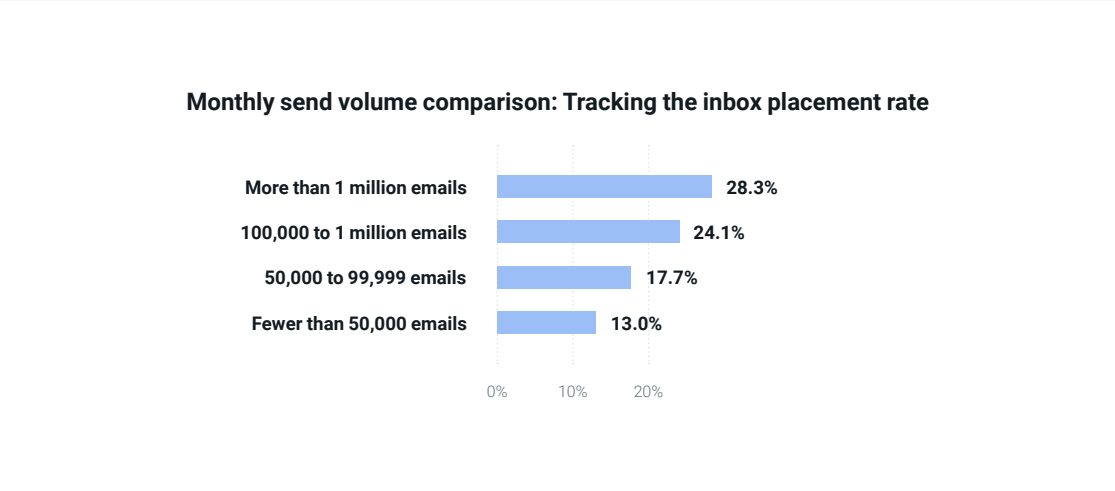


An inbox placement report from Sinch Mailgun

When senders receive an inbox placement report, such as the one above from Sinch Mailgun, they can investigate the results of a seed test for specific mailbox providers. These results provide senders with an overall score for the mailbox provider as well as a breakdown of where the emails ended up.

> *Inbox placement testing is the most accurate way to measure email deliverability. Yet only 16.4% of senders monitor their inbox placement rate.*

However, inbox placement testing is gaining momentum among senders and email marketers. It tends to be more popular among high-volume senders. **More than 28% of respondents with a sending volume of over 1 million emails a month monitor inbox placement.** That percentage drops the lower the send volume gets.



Want better inbox placement? **The best way to avoid the spam folder is to prove you deserve to land in the inbox.** Mailbox providers will ultimately decide how to filter your messages based on a variety of factors. Gmail, Outlook, Yahoo Mail, and the rest are paying attention to your sending practices. If you've got a bad reputation with them, your deliverability will suffer.

What's your reputation?

When marketers consider reputation, they're probably thinking about how customers and prospects view their brand. Those with more technical experience understand that domains and IP addresses have reputations too. **The decisions you make concerning your email program will affect what's known as your sender reputation with mailbox providers.**

Sender reputation is a score that mailbox providers assign to bulk email senders, which informs how emails from that domain or IP should be filtered. **The truth is – sender reputation and brand reputation are connected in many ways.** It's likely that a trustworthy sender with a good reputation is also a trusted brand. You don't earn a good reputation by annoying people with spam or using deceptive marketing methods.

There are two main factors connected to sender reputation:

1. **IP reputation:** This measures the behavior and quality of sending practices from a specific IP address. If it's a shared IP, the reputation applies to multiple senders.
2. **Domain reputation:** This measures the trustworthiness of your branded domain or website, including any subdomains you're using for sending mail.

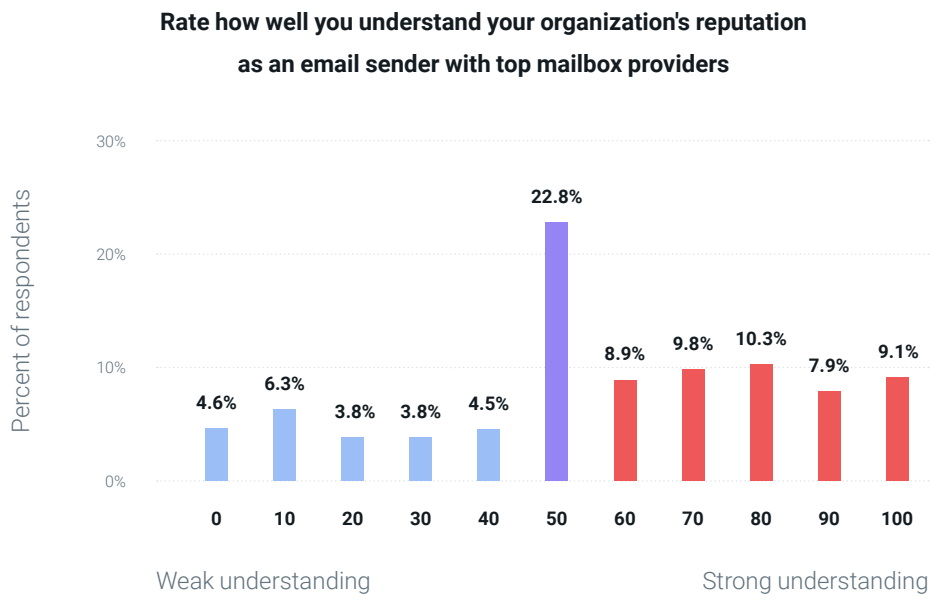
Our deliverability experts say mailbox providers like Gmail place a higher importance on domain reputation. That's because it's targeted toward specific senders. **The reputation of a domain is more closely connected to a business or brand.** IP reputation is still a factor, especially with Outlook. So, because many businesses use Outlook as their mailbox provider, IP reputation may have a bigger impact on B2B email deliverability.

"It is very easy to destroy your sender reputation, but it takes time to build it. You can damage your reputation with Gmail overnight, and it can take about four to six months to repair it."

Kate Nowrouzi, VP, Deliverability and Product Strategy, Sinch Mailgun

Just as we did with the prioritization of email deliverability, our survey asked participants to rate how well they understand their sender reputation.

Results suggest many are stuck in the middle when it comes to understanding their reputation with mailbox providers. **More than 45% of those surveyed rated their knowledge of sender reputation at 50 or below.**



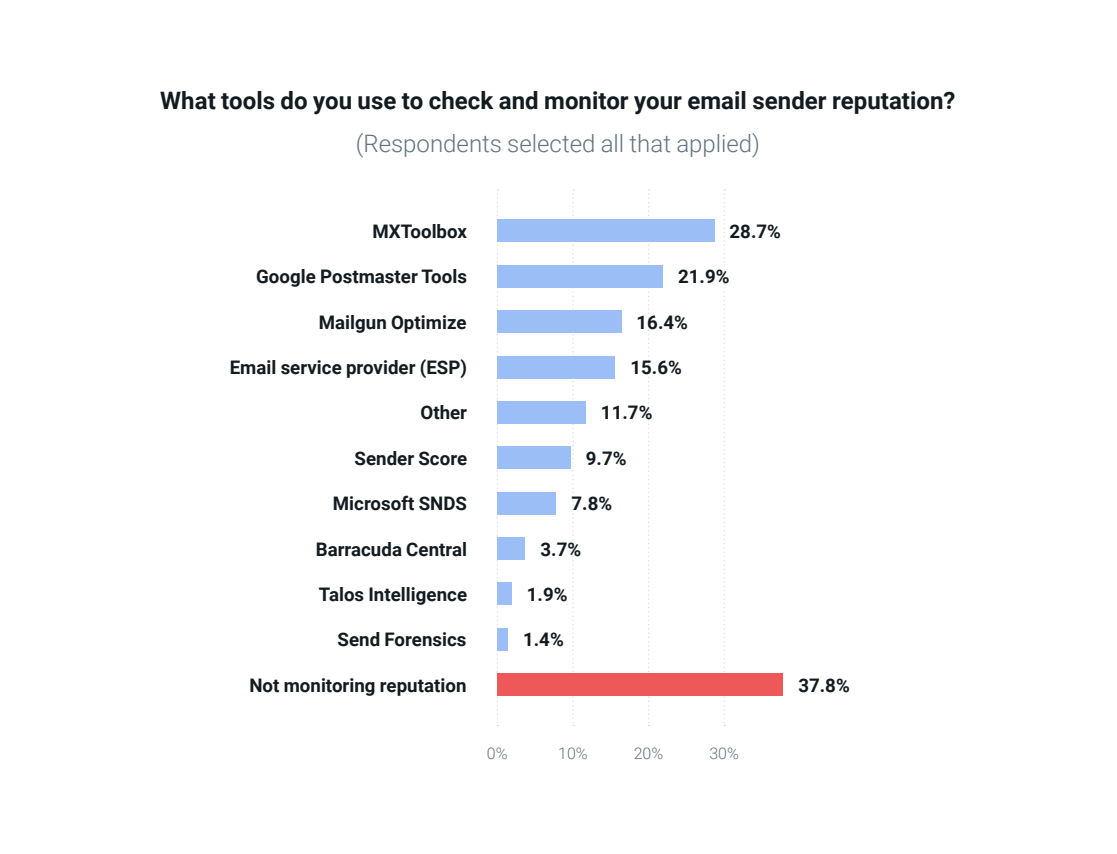
Here are some known ways to either support or damage your sender reputation:

Good for sender reputation	Bad for sender reputation
An updated email list with verified addresses	Purchased or scraped email contacts on your list
Highly engaged subscribers	Low email engagement rates
Quality content in email campaigns	Lots of spam complaints
Using a double-opt in process	Sudden jumps in list growth
Removing or segmenting inactive subscribers	Ignoring list hygiene
Strong email authentication practices	Lack of proper email authentication
A history of consistent sending practices	Failure to warm up new sending IPs/domains

While mailbox providers won't come straight out and tell you their opinions of your domain and IP reputation, there are ways to check and monitor sender reputation.

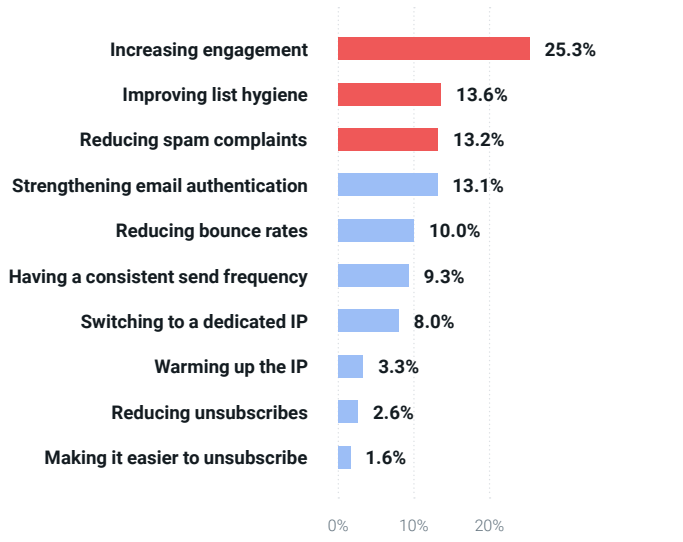
Our survey found that the most popular tools for keeping track of sender reputation are **MXToolbox** (28.7%), **Google Postmaster Tools** (21.9%), which specifically tracks sender reputation with Gmail, and **Sinch Mailgun** (16.4%).

However, **nearly 38% of respondents admit they are Not monitoring reputation**, which means they could be in the dark until something goes wrong and a deliverability issue needs to be addressed.



Let's say you discover you don't have the best sender reputation with mailbox providers, and you want to repair it. What are the most effective ways to build a stronger email sender reputation?

When we asked survey participants for their opinion on what would have the biggest positive impact on sender reputation, they selected **Increasing engagement** (25.3%) most often. **Improving list hygiene**, **Reducing spam complaints**, and **Strengthening email authentication** each received around 13% of the vote.



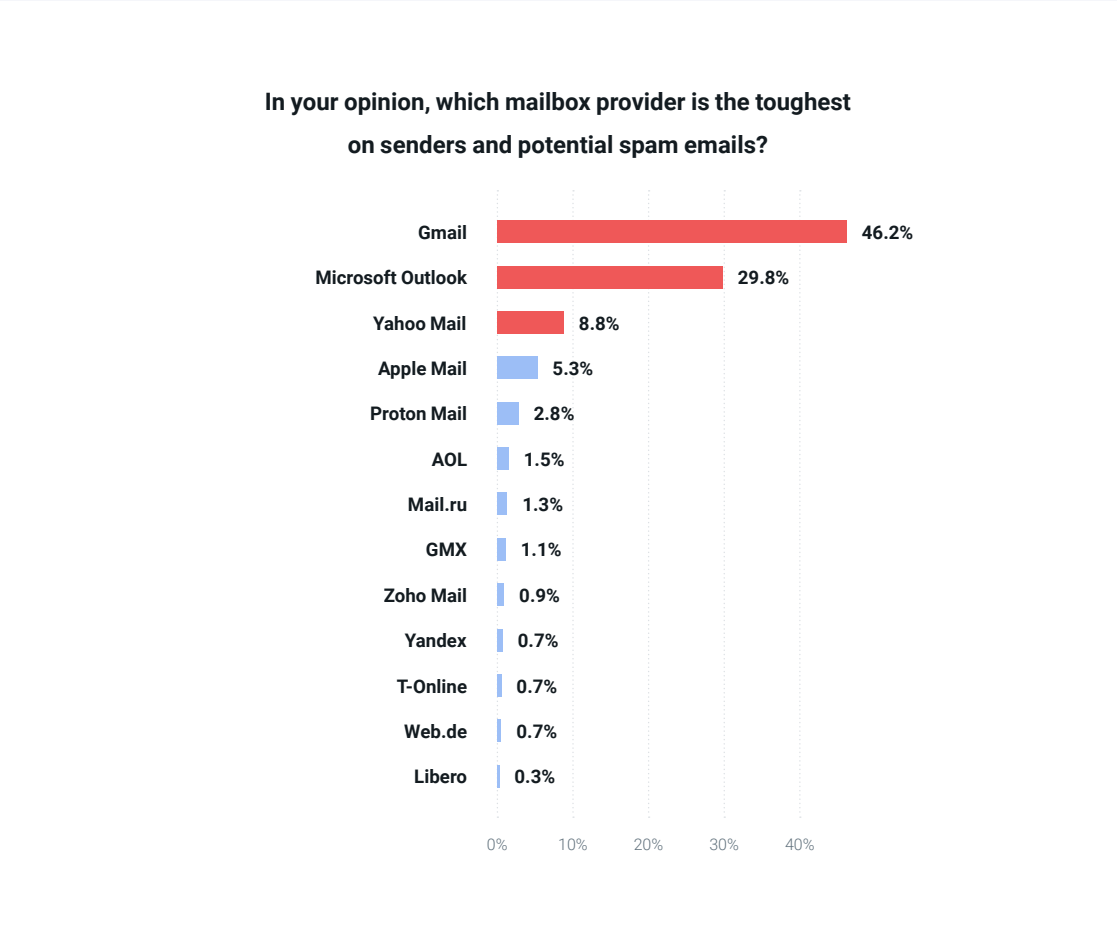
Of course, the recipe for a good sender reputation includes everything on this list. But Mailgun experts agree that the health and quality of your list is a top priority, and that includes keeping contacts engaged.

"All of these efforts can improve sender reputation. Personally, my focus would be on engagement, which ties heavily into list building practices. Make sure the recipients' addresses you've collected have agreed in a clear way to receive your emails from the start. Then, ensure they stay engaged with your emails over time. Making sure that you're aligned with their expectations about your email program will go a long way to solidify your sender reputation."

Alexandre Zibrick, Compliance and Deliverability Engineer, Sinch Mailgun

Finally, we asked senders to let us know which of the major mailbox providers tend to be the toughest on senders, including potential spammers. In other words, who is the toughest mailbox provider to keep happy?

The results weren't even close. Respondents in our survey overwhelmingly chose **Gmail** (46.2%) as the toughest mailbox provider. The next closest was **Outlook** (29.8%) followed by **Yahoo Mail** (8.8%).



Some of our deliverability experts weren't surprised at all by these results. For one thing, Gmail is one of the most popular email clients in the world and Gmail deliverability matters to every sender. Gmail is also known for being tough on spam as they have gotten very good at identifying and containing it.

At the same time, Gmail gives legitimate senders ways to keep tabs on their reputation (Postmaster Tools), and it is transparent about how Gmail spam filters work. Gmail also provides best practices for bulk senders as well as specific guidelines to prevent mail from going to spam or getting blocked.

EMAIL'S NOT DEAD

The big deliverability episode

Discover what's new in the world of email deliverability. Check out an episode of our podcast featuring deliverability guru Brad Gurley and our own Nick Schafer. Learn about sender reputation and more.

Listen Now

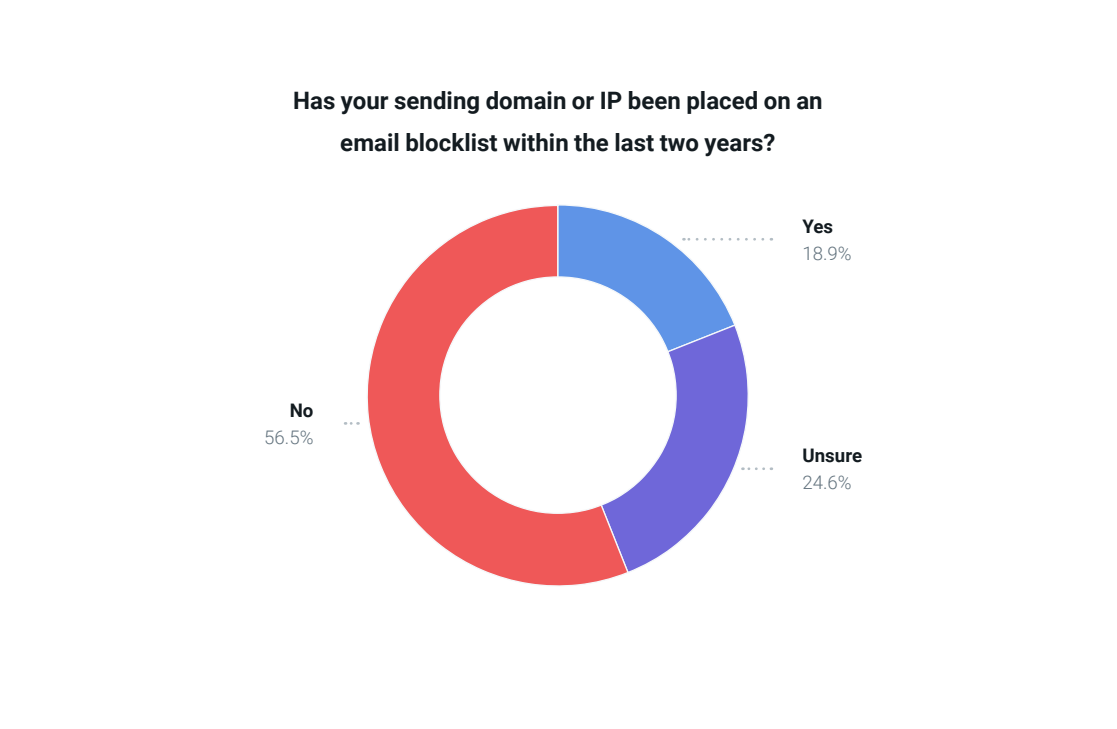
PART 3

Blocklisting and its impact

An email blocklist is a collection of domains or servers that have been identified as sending unsolicited bulk mail. In other words, it's a list of known and potential spammers who get blocked from delivering mail to providers that are using that blocklist service.

Legitimate, non-spammy email senders occasionally land on blocklists too. In some cases, it's not the sender's fault, and sometimes it's because of an honest mistake. Other times, blocklisting can be traced back to a failure to follow best practices around list building, list hygiene, authentication, and more.

Our survey found that around 19% of senders had been placed on a blocklist within the last two years. More than 24% were unsure whether they'd been blocklisted during that time.



Not all blocklists are created equal. Some will have an outsized impact on deliverability, but others may not cause much disruption to your email traffic at all. Mailgun's deliverability team says that Spamhaus is by far the most important blocklist provider to monitor.

The Spamhaus Project is an international, nonprofit organization that works to stop spam and cybersecurity threats. Spamhaus maintains several blocklists that mailbox providers use to protect their users from both spam and cyberattacks.

Other major blocklists providers include:

- Barracuda
- SpamCop
- SORBS

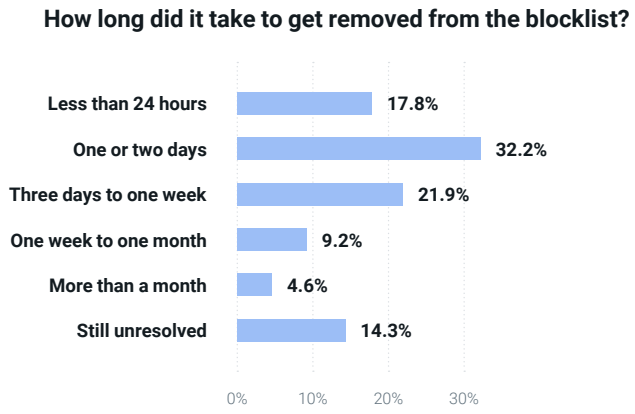
Depending on the blocklist and the specific situation, being blocklisted may not be a reason to freak out. But if you've been listed with a major blocklist provider like Spamhaus, you need to start the delisting process as soon as possible.

"Senders who haven't been educated on blocklists can get really scared when they are blocklisted, even if it is a minor one that will not affect their results in any way. But if you are talking about a major blocklist, and it's going to take you a couple of days or longer to get delisted, you will definitely see some email traffic being rejected. And you will most likely see revenue going down."

Alexandre Zibrick, Compliance and Deliverability Engineer, Sinch Mailgun

So, what are the reasons a sender can end up on a blocklist, and how long does it typically take to get delisted so emails start flowing again? We asked respondents in our survey who experienced blocklisting in the last two years to tell us more.

When it comes to removal, **about half of the blocklisted senders say they were able to get delisted in less than three days**. For nearly 18%, it took less than 24 hours. However, more than 14% of blocklisted senders say they are still dealing with an unresolved situation.

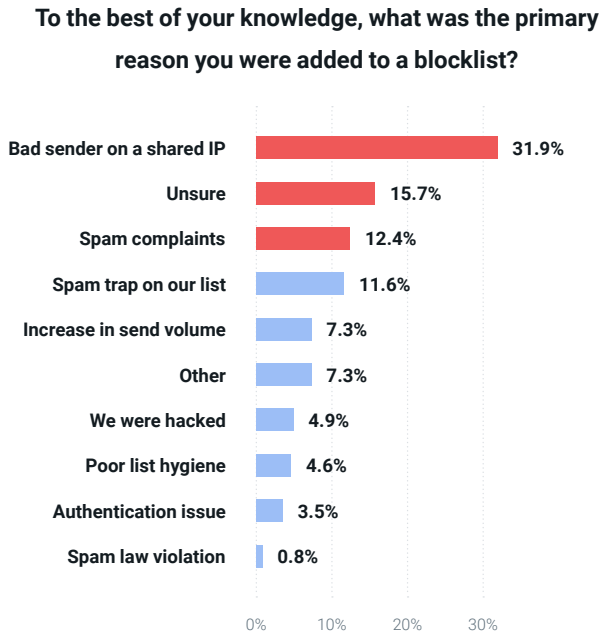


Even when blocklisting lasts just a few days, there can be serious business consequences for the blocked sender, especially if it impacts transactional messages. But even temporarily blocked marketing emails could result in serious declines in website traffic and revenue from email.

That's why a service such as blocklist monitoring protects your investment in the email channel. The right partner can also help senders get delisted faster. Thanks to Mailgun's industry connections, our team often vouches for reputable senders who land on blocklists, which can expedite the delisting process. **Our research found around 30% of senders turned to outside help for blocklist removal.**

If you've done something to deserve getting added to the blocklist, the delisting process could take longer. You may need to work with the blocklist provider and document how you've cleaned up your act.

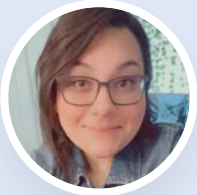
Many of the senders we surveyed believe their blocklisting can be blamed on the actions of others. By far the most common reason for getting blocklisted was a **Bad sender on a shared IP** (31.9%). Another 15.7% of respondents were **Unsure** why they'd been blocklisted, and 12.4% say **Spam complaints** caused them to land on a blocklist.



When you send from a shared IP address, you share the reputation of others sending mail from that IP. If you happen to be sharing the sending IP with spammers, it is certainly possible that it could lead to blocklisting. When you send from a dedicated IP, you don't have to worry about bad actors. You've also got no one to blame for blocklisting but yourself.

We typically recommend that higher volume senders with more than 100,000 emails per month strongly consider a dedicated IP. This helps those organizations establish a reputation with mailbox providers and protect it. But not every organization needs – or can afford – a dedicated IP. Those with lower email sending volumes may actually want to avoid dedicated IPs. A low volume of emails (and inconsistent sending) makes it harder for mailbox providers to assess your sender reputation. In that case, it may be better for deliverability to use a shared IP with lower volumes.

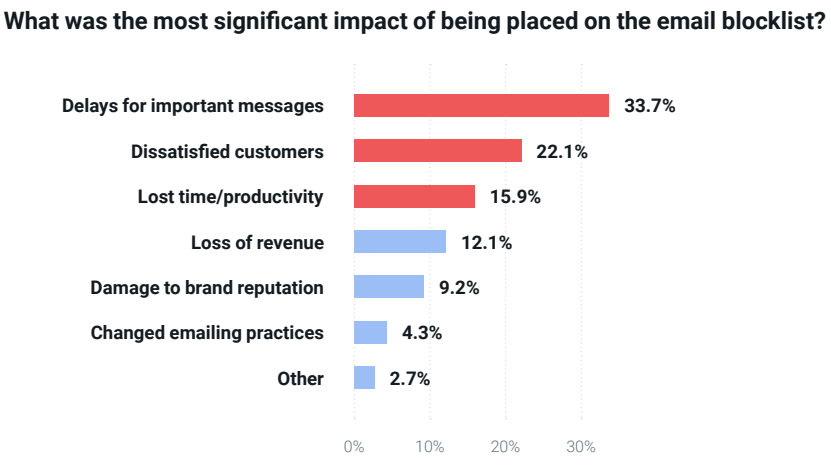
The policies your ESP adheres to can impact the risks of using a shared IP. If a service provider allows spammers and shady senders to use its platform, it puts you in greater danger of getting blocklisted. That's why Mailgun only accepts customers who meet the guidelines in our Acceptable Use Policy (AUP). It's designed to protect our reputation as an ESP as well as that of our shared IP customers.



"A shared IP will obviously have its risks. With dedicated IPs it's different because it's your responsibility, and if you're unsure why you've been blocklisted, it probably comes down to your list building, list hygiene, or sending practices."

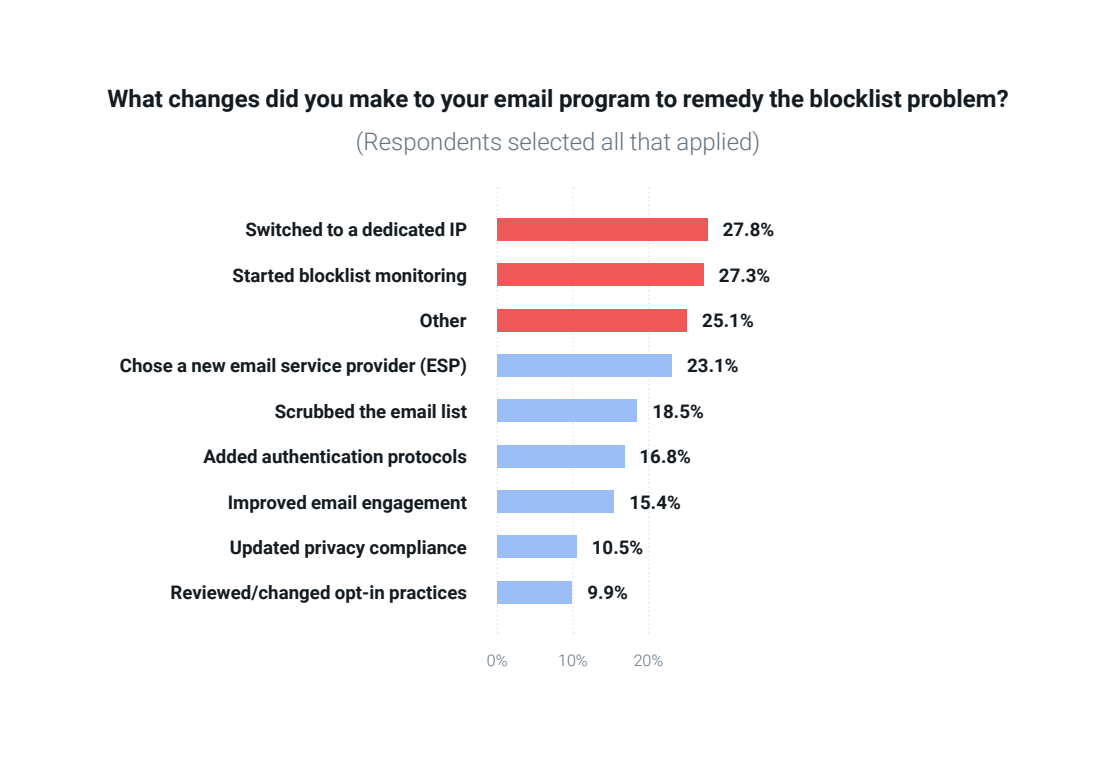
Ashley Rodriguez, Deliverability Engineer, Sinch Mailgun

There are several ways landing on a blocklist can damage a business. **More than a third of the senders we surveyed (33.7%) said Delays for important messages was the most significant impact of getting blocklisted**. That was followed by just over 22% who cited **Dissatisfied customers**, almost 16% who experienced **Lost time/productivity** to fix the problem, and 12% who say **Loss of revenue** was the biggest impact of the blocklisting.



Sometimes blocklisting requires that a sender make changes to get delisted. Other times, they may voluntarily take action to avoid getting blocklisted in the future. We asked senders to identify all the changes they made because of being blocklisted.

Our survey found that the most common change among blocklisted senders was that they Switched to a dedicated IP (27.8%). Not far behind, 27.3% of respondents **Started blocklist monitoring**. Another 23.1% **Chose a new email service provider**, and 18.5% **Scrubbed their email list** after being blocklisted.



Mailgun's deliverability experts say that switching to a dedicated IP or finding a new ESP with a better reputation and stricter policies could certainly help those who are concerned about sharing an IP with bad senders. But what if it's you and not them?

If you're ignoring best practices, and you take bad habits with you to a dedicated IP or a new ESP, your problems will likely follow you. If you don't realize it is your actions putting you at risk, or if you have no idea what prompted the blocklisting, you need to get to the bottom of it so the right changes can be made.

"Finding out what caused a blocklisting is something we can help our customers look into. With Microsoft, for example, our team can often map out events that led up to the block by investigating failures and warnings that point back to the problem. That's the benefit of having folks on your side who understand deliverability."

Ashley Rodriguez, Deliverability Engineer, Sinch Mailgun

EMAIL'S NOT DEAD

Keeping it real and authentic with Spamhaus

Curious to know more about Spamhaus and its blocklists? Check out an episode of our podcast featuring industry liaison, Matt Stith. Hear directly from someone inside the organization.

Listen Now

PART 4

Email authentication

How do mailbox providers know whether incoming mail is from a spammer or a legitimate sender? What's being done to keep bad actors from impersonating your brand and using the trust you've built to carry out phishing attacks? Email authentication is a big part of the answer.

Email authentication involves a collection of protocols and specifications designed to verify the origin and authenticity of mail that comes from legitimate senders. In other words, it's a way of showing receiving mail servers that you are who you say you are.

Mail servers use what's known as Simple Mail Transfer Protocol (SMTP) to send, relay, and receive messages between senders and recipients. The problem is that SMTP has some major flaws. It does not support encryption and lacks a way to validate the identity of the sender, which has made email a popular attack vector for bad actors.

To remedy this, several authentication protocols and related specifications were developed to thwart bad actors, help mailbox providers filter mail, and protect email recipients. These are DNS TXT records that receiving mail servers reference to verify the authenticity of messages.

Email authentication essentials

Sender Policy Framework (SPF): An SPF record includes a list of all the domains and mail servers that are authorized to send mail on behalf of your organizational domain. Receiving mail servers reference the SPF record to make sure messages that appear to come from your company are from an approved source.

DomainKeys Identified Mail (DKIM): The DKIM authentication method uses a pair of encrypted digital signatures also known as public and private keys. These keys help receiving mail servers associate an incoming message with a specific domain. DKIM also ensures messages are not altered during transit.

Domain-based Message Authentication, Reporting and Conformance (DMARC): The DMARC specification harnesses the power of both DKIM and SPF by checking for alignment. It is an effective way of preventing email brand spoofing. DMARC policies inform mailbox providers on what to do with messages that fail authentication. DMARC also provides reports that detail who's sending mail on behalf of your domain.

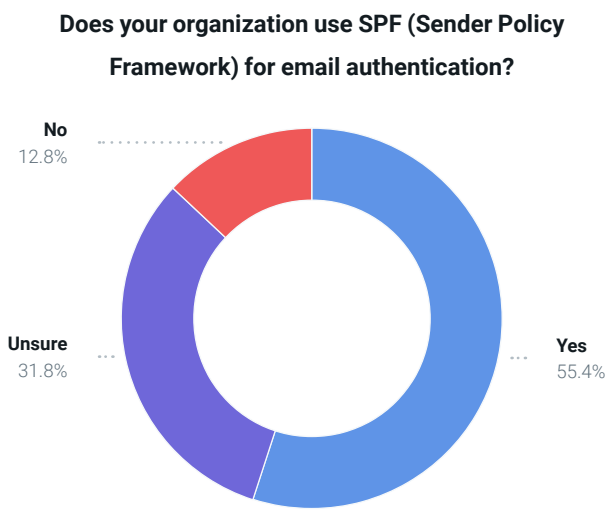
Brand Indicators for Message Identification (BIMI): Brands that enforce DMARC are eligible to have a verified logo appear in the inbox. BIMI logos are meant to be a reward for senders with strong authentication. It gives brands control over inbox logos and could boost engagement while serving as a trust mark.

Messages that lack proper email authentication are much more likely to be blocked or filtered into spam. In 2022, Gmail began requiring that new senders trying to deliver messages to its users must set up either SPF or DKIM at a minimum. However, it is highly recommended that senders use both of these protocols.

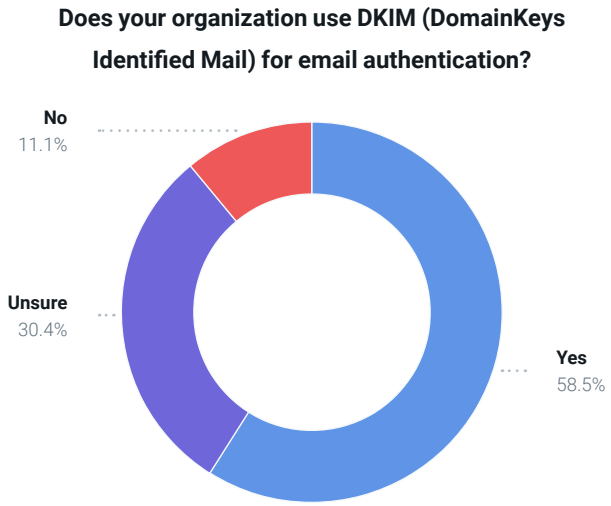
SPF and DKIM usage

According to Mailgun's deliverability experts, the use of SPF and DKIM is table stakes for most senders. It's highly likely that your ESP makes SPF and DKIM setup a requirement, or your ESP may be using its own protocols to authenticate messages for you.

To find out more about senders' familiarity with these important protocols, we simply asked whether they were using SPF and DKIM or not. Results for the Sender Policy Framework protocol show that while more than half of those surveyed say they use SPF, nearly 13% say they are not and close to one-third are **Unsure**.



When it comes to the DKIM protocol, 58.5% of senders report that they have implemented DomainKeys Identified Mail. Around 11% say they don't use DKIM and more than 30% are **Unsure** if the protocol is implemented or not.



When isolating survey results for responses from marketing job roles, uncertainty around the use of authentication protocols increases. Uncertainty also *drops* significantly when results are filtered for those who work in IT or specialize in email deliverability.

Many marketers may be unfamiliar with the technical aspects of authentication because it's all happening behind the scenes on domain name servers. Since IT professionals are the ones setting up these DNS TXT records, they have more email authentication knowledge.

"There are some senders who may not be familiar with SPF and DKIM protocols. But with most email service providers, it's a requirement to have that set up. In many cases, their messages are signed with SPF and DKIM, but it might be the ESP's and not their own. If you're using a modern sending platform, your messages are going to be authenticated."

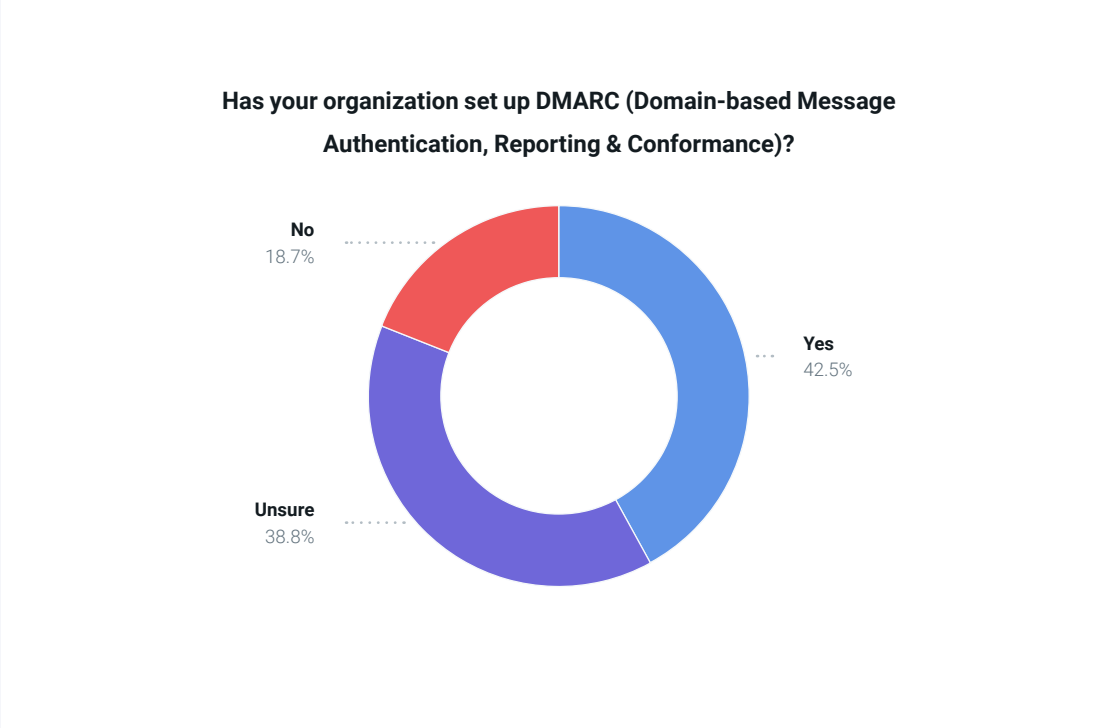
Nick Schafer, Sr. Manager of Deliverability and Compliance, Sinch Mailgun

If you don't know whether your organization is using SPF or DKIM authentication, check with your IT department or ask your ESP to make sure these measures are being taken care of for you.

DMARC implementation

DMARC is a powerful tool for email authentication, security, and protecting a sender's brand. However, it is also underused and misunderstood. One of the biggest problems with DMARC is that, even among senders who've set it up, it is not being enforced in a way that helps stop spoofing.

More than 42% of senders in our survey say they are using DMARC as part of their email authentication. A recent analysis from MXToolbox suggested that around half of Fortune 500 companies still haven't implemented DMARC. So, while the 42.5% using DMARC in Mailgun's survey is lower than SPF and DKIM usage, it's an encouraging number since it includes senders of all sizes. Around 13% of respondents say they are not using DMARC and close to 40% are **Unsure**.

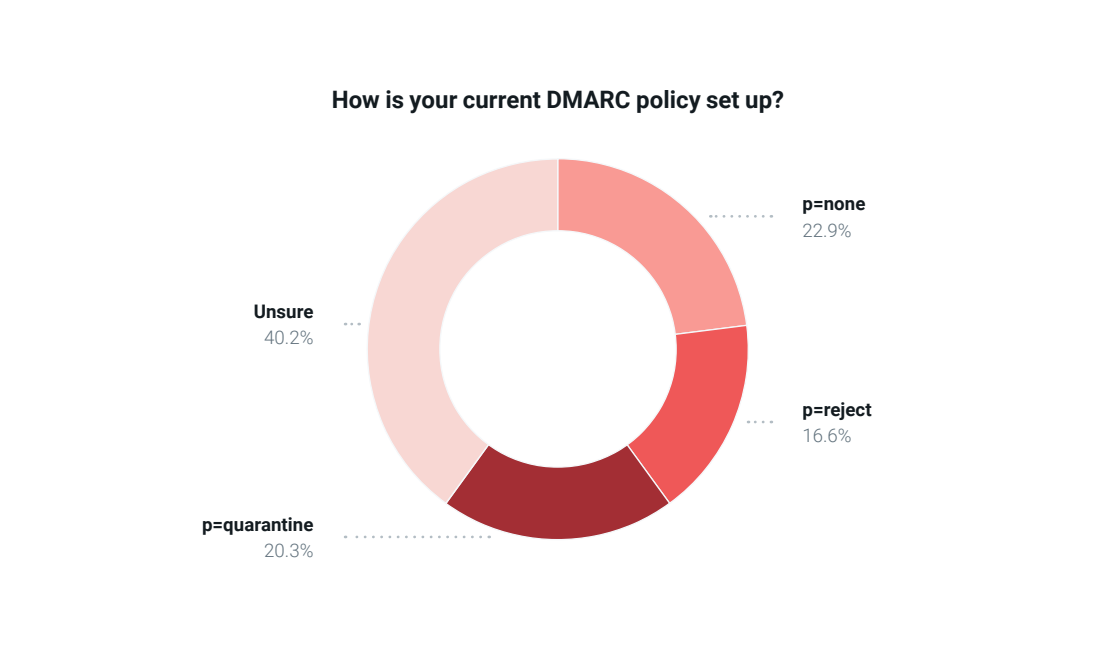


To experience the benefits of DMARC, senders need to enforce the right policy in the DNS TXT record. There are three possible DMARC policies. They suggest how receiving mail servers should handle messages that fail DKIM and SPF authentication.

DMARC policy options

1. **p=none:** This policy tells receiving mail servers to do nothing if an email fails authentication. The message will be delivered to the inbox unless the mailbox provider chooses to filter it into another folder. The p=none policy does nothing to stop email spoofing.
2. **p=quarantine:** This policy tells mailbox providers that authentication failures should be quarantined and treated with caution. That means the receiving mail server will probably accept the message, but it will likely get filtered into the spam folder.
3. **p=reject:** This is the strongest DMARC policy. It informs mail servers to treat authentication failures as malicious. The email will most likely be blocked from delivery. It won't even go to the junk folder and the recipient will never see it.

Our survey revealed that many respondents are unaware of how their organization enforces DMARC. When we asked senders who've implemented DMARC to describe their policy, more than 40% were **Unsure**. Around 23% say their policy is set to **p=none** and just over 20% are using **p=quarantine**. Only 16.6% of senders have implemented the strictest policy of **p=reject**.



The lack of awareness around DMARC policies stood out as a concern to Mailgun's deliverability experts. That's because senders need to be very careful when setting up DMARC as a mistake in the TXT record could have negative effects on your deliverability.

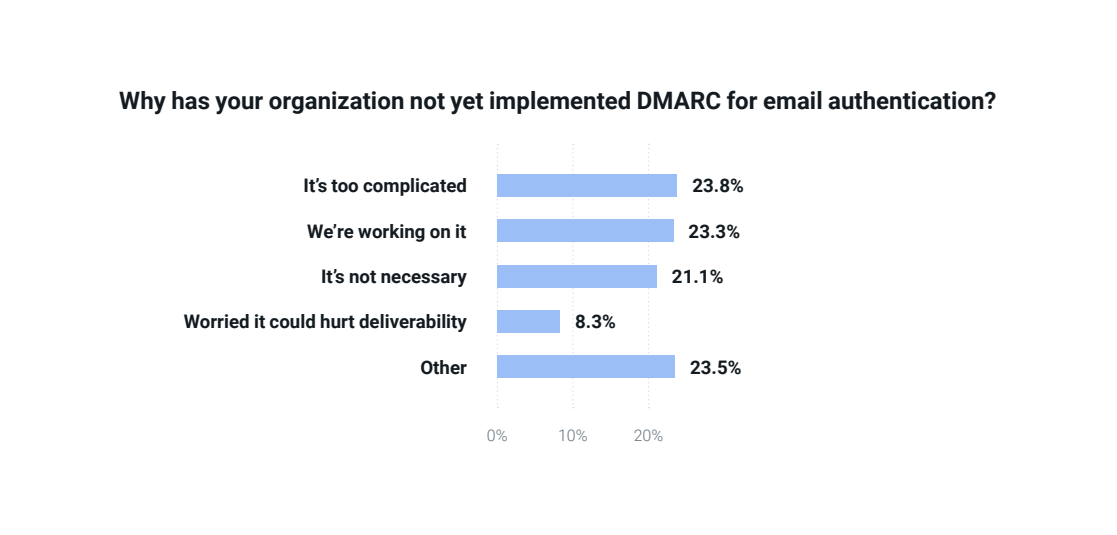
In fact, that's the entire reason the p=none policy exists. The less stringent policy was meant to let senders test their DMARC setup before enforcing it. **Unfortunately, too many organizations never move away from the p=none policy.** This means they might be receiving DMARC reports, but they won't be strengthening authentication.

"If senders want to experience the benefits of DMARC, they need to change their policies to either quarantine or reject after a testing phase. Otherwise, you're doing nothing to prevent bad actors from spoofing your brand in the inbox."

Kate Nowrouzi, VP, Deliverability and Product Strategy, Sinch Mailgun

So, if DMARC is such an effective addition to email authentication, why have senders been slow to adopt the specification? We asked respondents who say they are not using DMARC to tell us what's holding them back.

For some senders, DMARC setup is an ongoing project. Just over 23% said **We're working on it** when asked why they haven't implemented DMARC. But a similar percentage of respondents said **It's not necessary** or **It's too complicated** while around 8% are **Worried it could hurt deliverability**.



Those who feel DMARC is unnecessary or too complicated may believe SPF and DKIM are enough. They don't see the benefit of adding more authentication. While DMARC can protect brand reputation by preventing spoofing, its primary purpose is protecting recipients and helping mailbox providers stop spammers and scammers.

Still, adopting DMARC could be a very smart move if you want mailbox providers to view you as a reputable sender. Some in the industry even believe DMARC could become mandatory in the future.

"At some point, mailbox providers may decide to prioritize messages from senders that have DMARC policies set to reject or quarantine, because those are the ones they can verify and trust. We haven't seen anyone take that step yet, but the groundwork is there to require senders to have a DMARC policy set to something besides p=none. That might be what it takes for adoption."

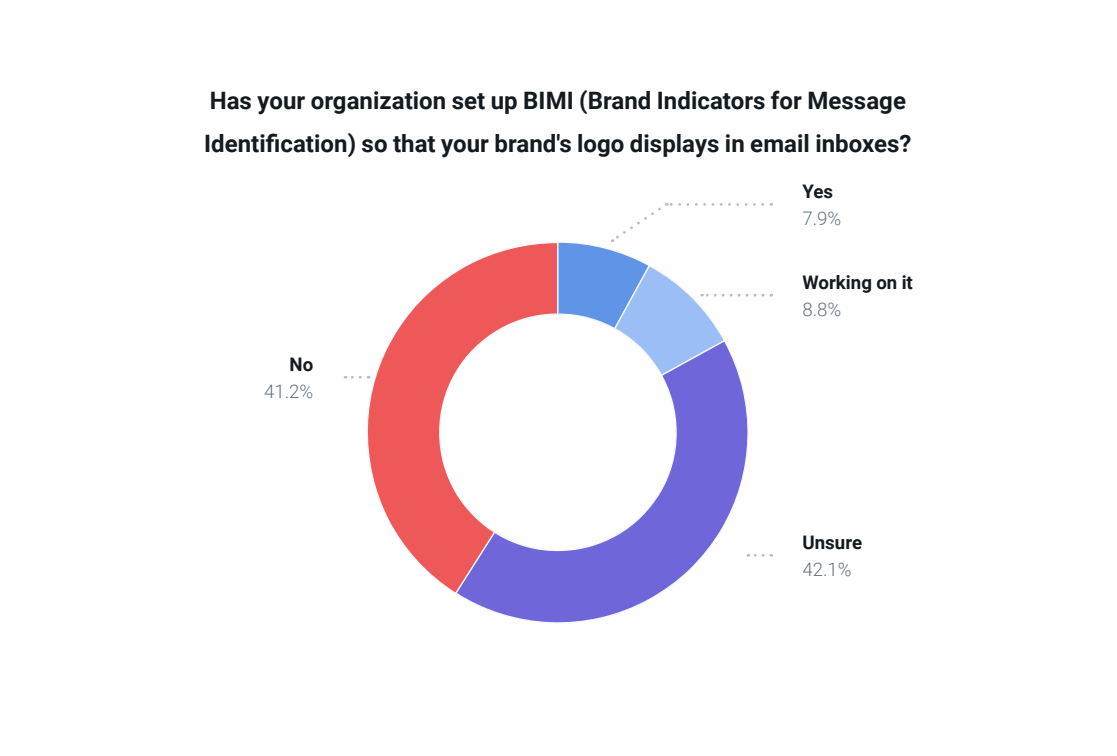
Jonathan Torres, TAM Team Manager, Sinch Mailgun

BIMI adoption

BIMI is the newest email standard connected to email authentication. Technically, it doesn't do anything to help authenticate emails, but the presence of a BIMI logo represents senders who are taking the issue seriously.

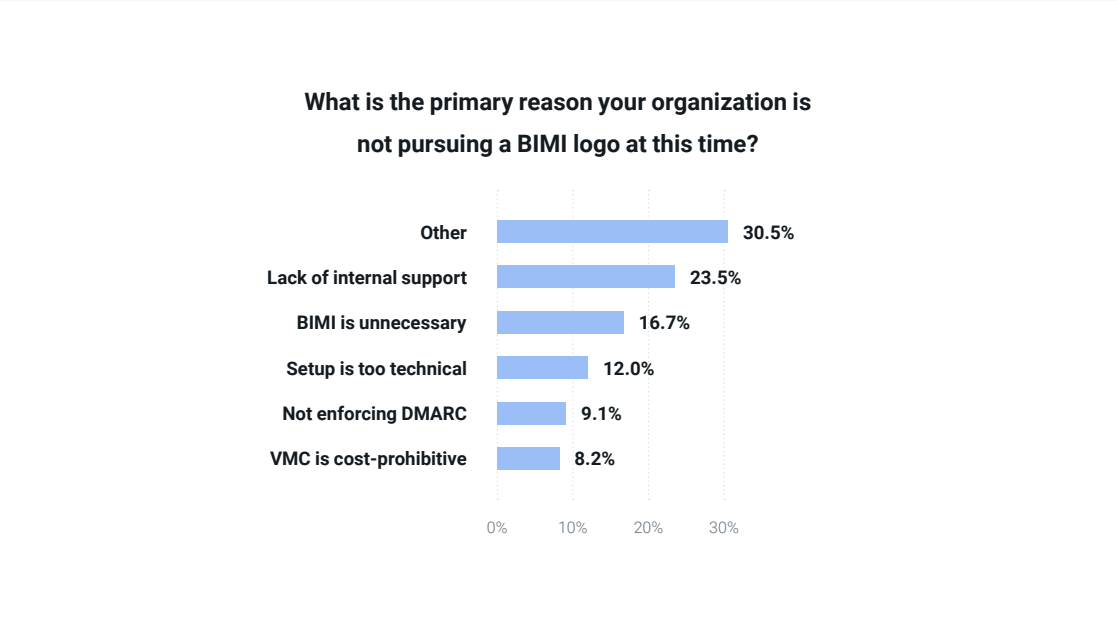
That's because **only senders with a DMARC policy of quarantine or reject are even eligible for a BIMI logo**. In fact, the BIMI standard was created to encourage DMARC adoption and stronger enforcement.

Only around 8% of senders in our survey have successfully implemented BIMI to date. Another 8.8% say they are working on setting up BIMI. There's a fairly even split between respondents who know they have not implemented BIMI and those who are **Unsure**, which indicates a lack of awareness.



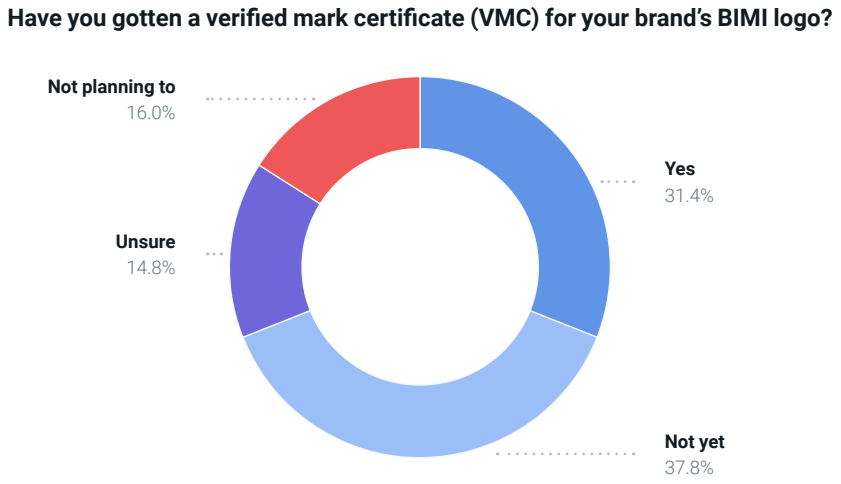
For the respondents who answered **No** to the previous question, we followed up to ask why BIMI isn't something they are at least pursuing. Apparently, the options we provided in the survey didn't cover all the potential reasons as **Other** was the top choice at more than 30%.

23.5% of those who are not pursuing BIMI implementation say it's because there is a **Lack of internal support** for the idea. 16.7% believe **BIMI is unnecessary**, and 12% think **Setup is too technical**.



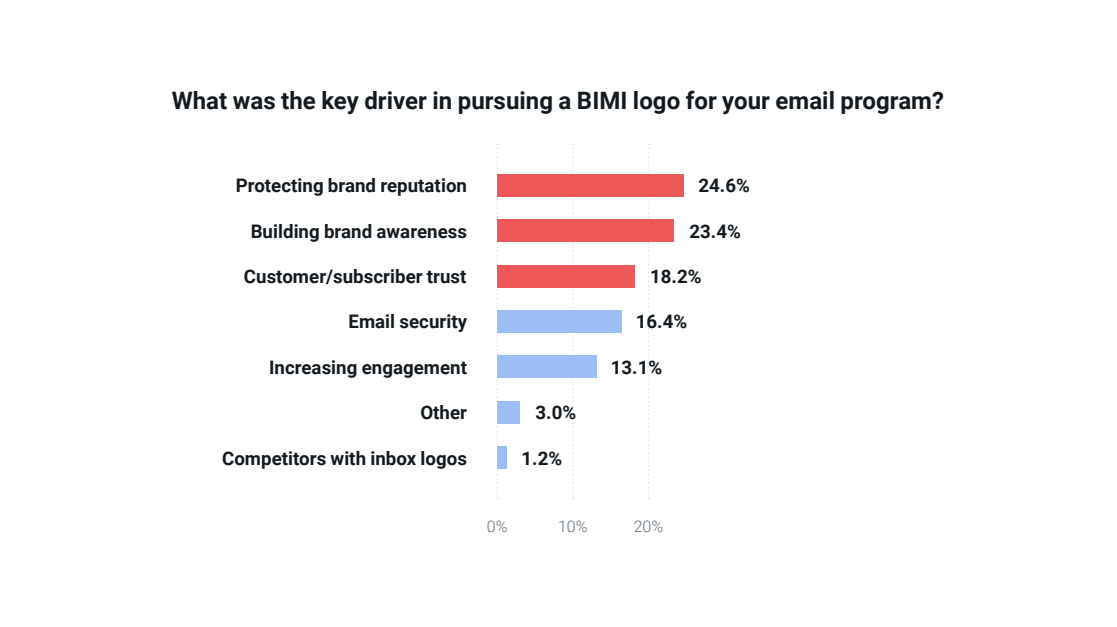
At the bottom of the list of reasons why BIMI is not being pursued is that the **VMC is cost prohibitive** (8.2%). A Verified Mark Certificate (VMC) is required to get a BIMI logo to display in both Gmail and Apple Mail, which are the two most popular email clients. To obtain a VMC, you need a copyrighted logo that is verified by one of two entities: Entrust or DigiCert. This can cost around $1,500 a year, which may be too much of an investment for some smaller senders.

Among senders using BIMI, our survey found that close to one third have purchased a VMC, while 37.8% may plan to but have not done so yet. 16% of senders who've set up BIMI are **Not planning to** get a VMC while almost 15% are **Unsure** if they have one or not.



It's true that implementing BIMI can be a technical and time-consuming process. In addition to DMARC enforcement requirements and the cost of a VMC, BIMI logos also must be created in a specific file format, and it's yet another TXT record to add to the DNS. Ultimately, it requires that marketers and IT specialists work together.

So, why do a growing number of brands see value in BIMI adoption? According to our survey results, the biggest driver for pursuing BIMI logos is **Protecting brand reputation** (24.6%). That's followed by **Building brand awareness** (23.4%). So, it's clear that BIMI implementation is a branding move.



There are also senders who see value in BIMI for other reasons. More than 18% of those using BIMI say they do so because it can increase **Customer/subscriber trust**. Another 16% say it has to do with improving **Email security**.

As BIMI adoption becomes more widespread, email recipients will likely take notice of those inbox logos. If a logo is not there, people may be more suspicious of possible spoofing and phishing attempts, because those malicious messages won't have a BIMI logo. That's how BIMI builds trust and helps promote a more secure email inbox.

As a bonus, there's evidence that inbox logos really do help with **Increasing engagement**, which more than 13% of senders called a key driver of BIMI adoption. A study from Entrust and Red Sift found that **BIMI logos could increase open rates by as much as 21%**. The study also suggested that the presence of an inbox logo increases the likelihood of purchase by as much as 34%. That kind of engagement is a strong signal to mailbox providers that your messages should land in the inbox and not spam.

"That's why I love BIMI. If senders want to enjoy the benefit of having that brand identification, then they need to implement DMARC. And DMARC is great. It's not going to improve deliverability directly. But it can protect your reputation as a sender."

Nick Schafer, Sr. Manager of Deliverability and Compliance, Sinch Mailgun

Email security and compliance guide

Want to learn more about authentication and how to make the email inbox a safer place? Get a free guide from Sinch Mailgun to find out what our experts have to say.

Download Now

PART 5

List building and hygiene

While email infrastructure and authentication protocols are part of the IT professional's world, list building and hygiene often fall squarely on the shoulders of email marketers.

It is usually marketers who are responsible for acquiring new subscribers and managing various lists of email contacts. **Your approach to growing the list, verifying new contacts, and even segmenting subscribers will impact your ability to reach the inbox and stay out of spam.**

"I always talk to our customers about list hygiene because I think it's so important. Building and maintaining a healthy list is huge for email deliverability."

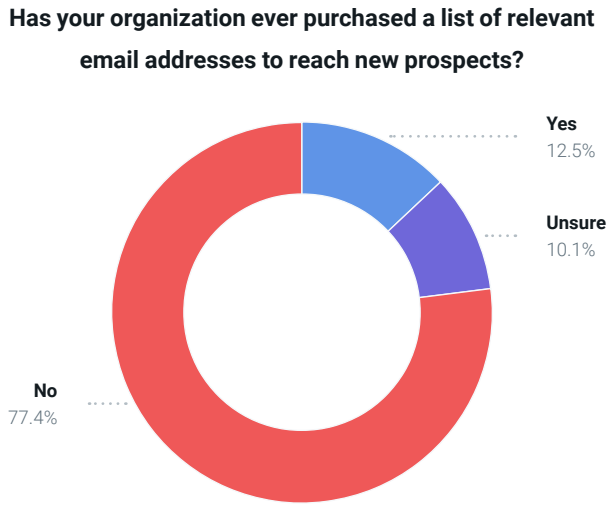
Nick Schafer, Sr. Manager of Deliverability and Compliance, Sinch Mailgun

When it comes to list building and maintenance, there are good habits and bad habits. Let's explore some survey results to find out what senders are doing right and where they're veering off course.

Bad list building habits

If we've said it once, we've said it one million times: **Purchasing a list of email contacts is a very bad idea**. Yet, our deliverability experts see people bragging on social media about building a huge email list using questionable methods.

When we asked the 1900+ senders who took our survey if their organizations ever purchased email contacts, 12.5% admitted they had. While 77.4% claim their companies had not purchased a list of addresses, more than 10% were **Unsure**.

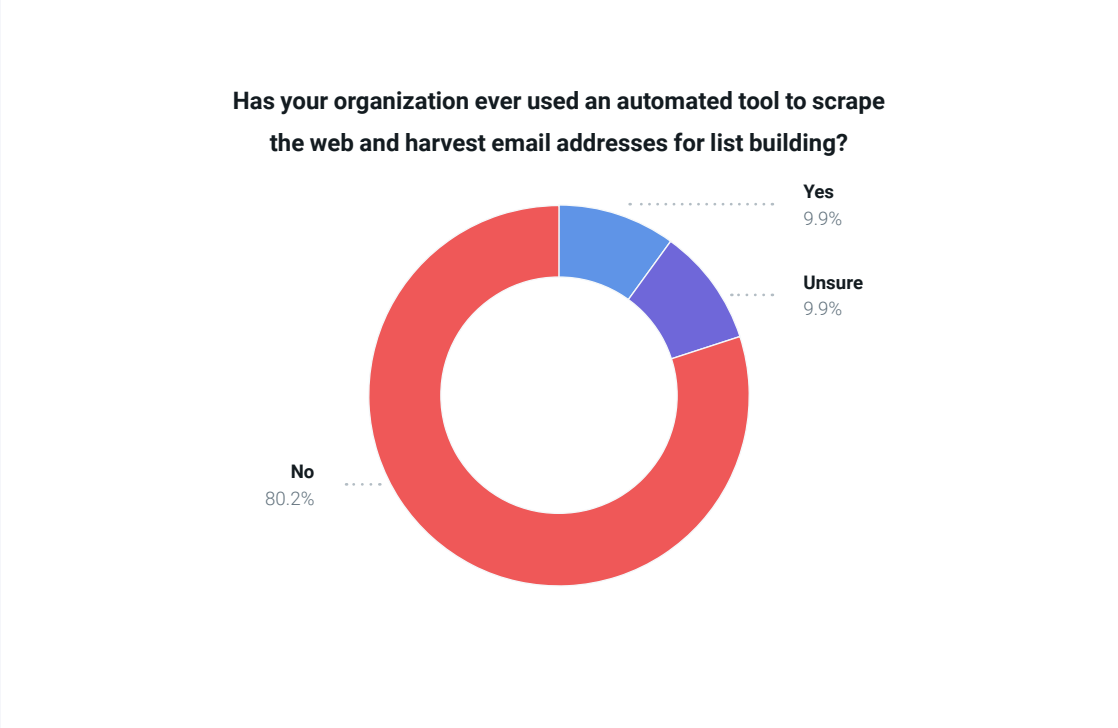


The foundation of responsible list building involves obtaining consent and monitoring interest from subscribers. **When you purchase a list of new contacts, you become a spammer the moment you send them anything.** It doesn't matter if they represent a relevant target audience. If those people never signed up to hear from your brand, you are sending unsolicited mail they're probably not interested in, and there's a good chance it will eventually hurt your deliverability.

Even valid email addresses on a purchased list can create deliverability problems because those users never opted in and aren't expecting to hear from you. Sending emails to these contacts will no doubt generate plenty of spam complaints. And the higher your spam complaint rate climbs, the lower your inbox placement rate is likely to fall.

On top of that, purchased email lists often contain pristine spam traps (aka honeypots). These are essentially fake email addresses that mailbox providers create to catch spammers. **Sending mail to spam traps is a good way to end up on blocklists.**

Another questionable acquisition practice involves scraping the web to find email addresses you can use to build your list. Our survey found nearly 10% of senders have tried this technique and another 10% were **Unsure** if it's something their organization has done.



This is another good way to get spam traps on your list. It's likely that some of these senders were simply unaware that this practice is frowned upon and can have negative consequences for email deliverability. But even though an email address may be publicly available on the web, it doesn't mean that you have *permission* to email that account.

Not only will purchased and scraped contacts be more likely to hit the "report spam" button and less likely to engage with your email, but you could also be violating privacy laws. The European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) prohibit sending commercial messages without consent. Those are just two of the more well-known privacy laws. Many other regions have their own rules for senders regarding the consent to email.

Good list building habits

There are also some email list building strategies that ensure you only collect contacts who are likely to be engaged with what you send. Plus, senders can also implement policies that help them manage their lists by identifying contacts who've stopped engaging.

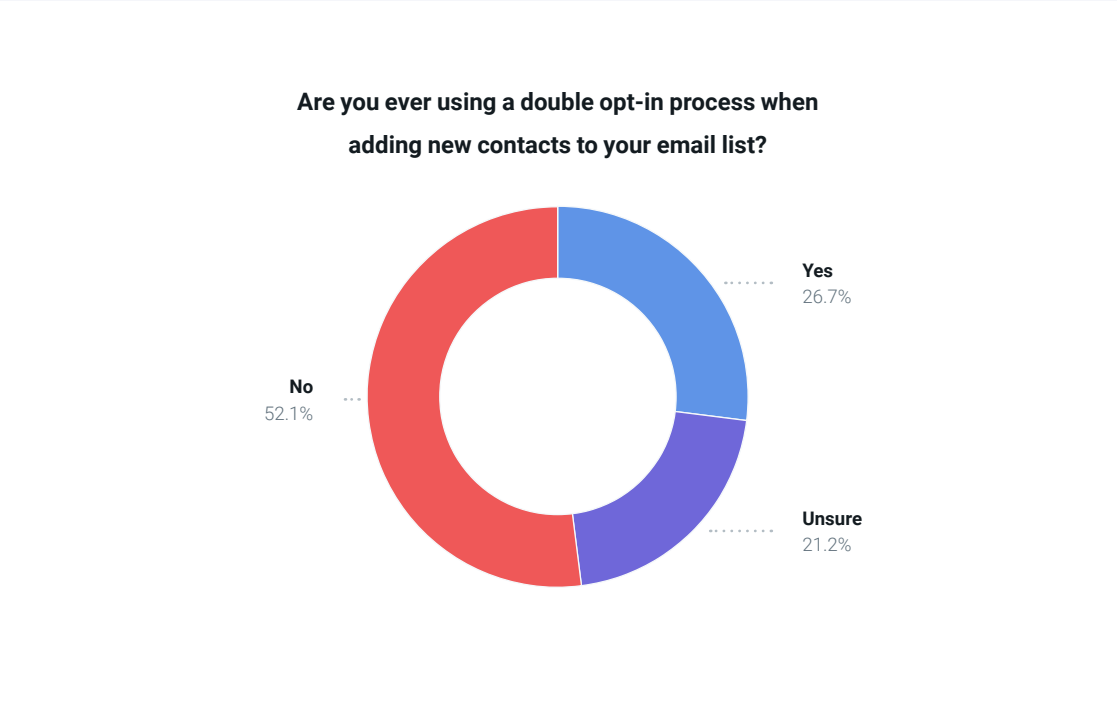
One of the best ways to be sure new contacts consent to receive your emails is to implement what's known as a double opt-in process. Here's how double opt-in works:

1. Someone fills out a form to receive emails from your brand.
2. You then deliver an initial email asking them to confirm they want to subscribe.
3. After the individual clicks a link in the confirmation email, they are officially added to your list.

Some marketers aren't fans of the double opt-in method because it does add an extra step that's a bit of a barrier to list growth. However, a double opt-in promotes list health and helps verify that new contacts are using valid email addresses at signup.

As an alternative, senders may implement what's known as confirmed opt-in lite (COIL). In this process, new subscribers are segmented onto a separate list until it's clear whether they'll be engaged with emails or not. Those new contacts won't be added to your main list unless they start opening and clicking.

When we asked survey respondents if they ever use a double opt-in process for subscriber acquisition, just over a quarter of them said they do. **But more than half of senders admitted they *do not* use a double opt-in for list building.**



According to Mailgun's deliverability experts, ignoring the benefits of the double opt-in for new subscribers is a major missed opportunity. More senders should consider it.

"Being in the position I'm in, I would recommend that every sender use a double opt-in all the time. Not only does it ensure you only acquire subscribers who are more likely to engage, but it also helps prevents bots from abusing signup forms, which is a significant email security risk."

Nick Schafer, Sr. Manager of Deliverability and Compliance, Sinch Mailgun

But a double opt-in isn't enough either. Over time, good contacts can go bad. People abandon email addresses, change jobs, or sometimes subscribers just lose interest and become unengaged. To maintain the health of your list, it's important to manage these contacts.

Left alone, those inactive and outdated contacts can erode your deliverability efforts. If too many recipients are unengaged, it could negatively affect your sender reputation. Plus, old email addresses can become recycled spam traps. These are addresses that mailbox providers repurpose to catch spammers and senders who fail to keep their data clean.

> ***Sunset policies help you define when to remove or segment unengaged contacts to avoid these problems.*** *A sunset policy is an email segmentation strategy that represents a proactive approach to list hygiene.*

Essentially, you set benchmarks to define disengaged contacts based on the last time they opened an email or clicked a link. When a contact reaches a certain threshold, they are either removed or segmented to a list of low-engagement subscribers to which you send less frequently.

"A sunset policy is one of my favorite practices. I've used this many times to help customers recover from a damaged sender reputation. I know from experience working with different senders that it can work."

Nick Schafer, Sr. Manager of Deliverability and Compliance, Sinch Mailgun

While it's a helpful best practice, **only 22.5% of senders in our survey say they are using a sunset policy to identify disengaged subscribers**. Nearly 60% admit they don't have a policy in place while almost 18% are **Unsure** if sunsetting subscribers is part of their strategy.

Marketers tend to place a lot of value on the number of contacts they have on their lists. But the truth is – that's a vanity metric. **It's not the size of your list that matters most, it's how subscribers respond to your campaigns that matters.** You won't see a higher return on investment from email by simply adding lots of contacts. Your ROI goes up only when that list growth is coupled with high engagement.

It may be tough to fight the urge to send every email marketing message to every subscriber. It may also be painful to voluntarily remove contacts. But it's much better to control the situation yourself before an old address becomes a spam trap or a disengaged subscriber makes a spam complaint.

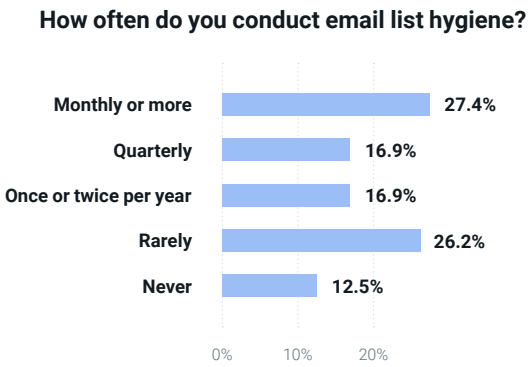
"People always fear reducing their list size and targeting subscribers differently. But once they start to see the benefits, the story tells itself. Sunsetting allows you to focus on engaged recipients. A subscriber who never opens or clicks isn't bringing you any value."

Ashley Rodriguez, Deliverability Engineer, Sinch Mailgun

List hygiene processes

Every household has its cleaning schedule, and email senders have different timeframes for housekeeping when it comes to list hygiene, too. **The general best practice is to conduct thorough list hygiene at least twice a year.**

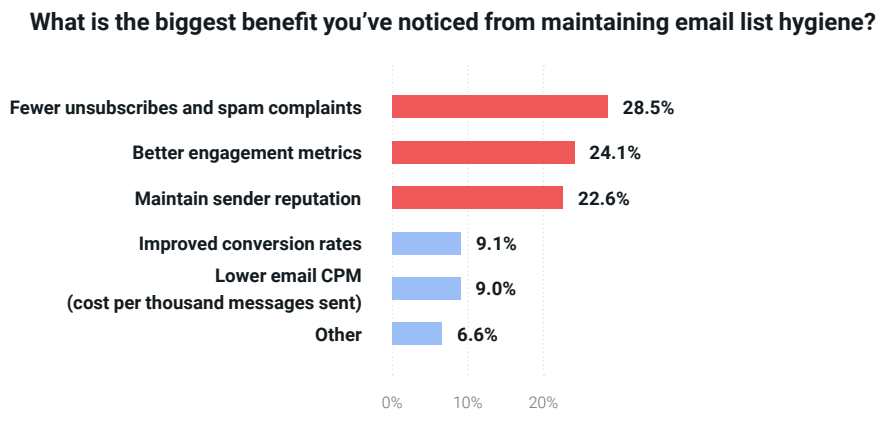
When our survey asked respondents to tell us about their list hygiene practices, results show 27.4% clean their lists **Monthly or more**, and nearly 17% do it **Quarterly**. Unfortunately, we also found 26.2% of senders **Rarely** conduct list hygiene and another 12.5% **Never** do it. **That's a combined 38.7% of senders who are not prioritizing list hygiene.**



The survey also found more than 40% of respondents with send volumes above one million emails a month conduct list hygiene Monthly or more. As you'd imagine, these senders likely have massive databases that are constantly changing.

Paying attention to list hygiene is important for email deliverability, but it also helps email teams get a more accurate picture of how their campaigns perform. If you're sending emails to invalid addresses, outdated contacts, and inactive subscribers, your metrics will suffer.

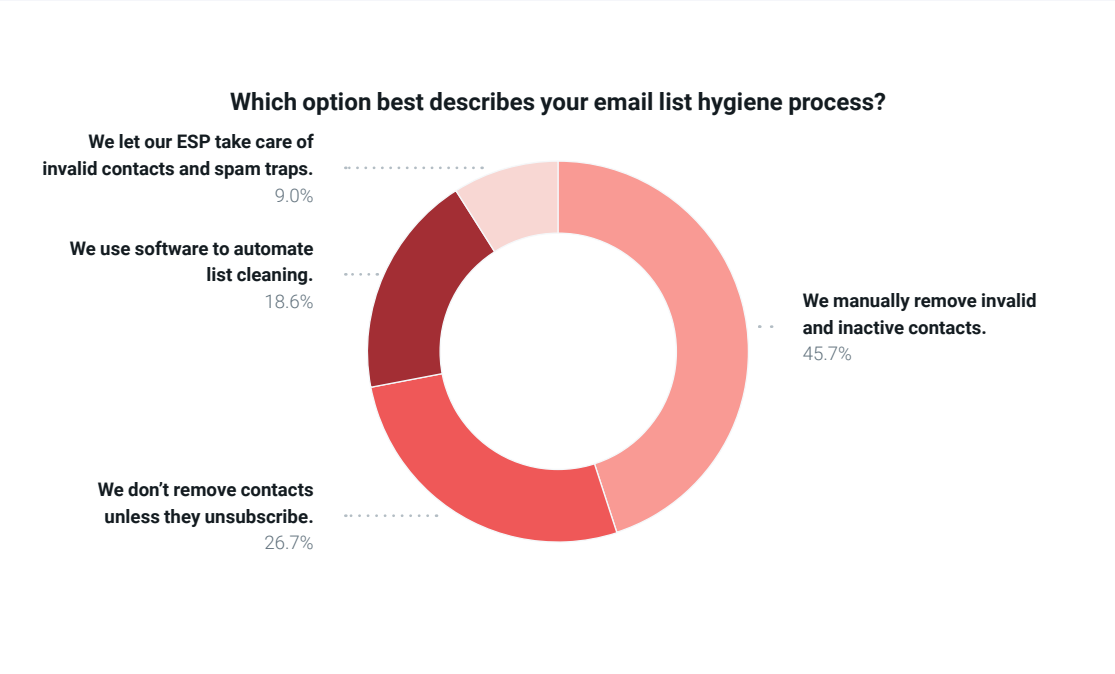
Among those who conduct list hygiene quarterly or more often, 28.5% say the biggest benefit is **Fewer unsubscribes and spam complaints** while another 24% cite **Better engagement metrics**. There are many other benefits to maintaining a healthy email list, including the ability to **Maintain sender reputation** (22.6%) and **Improved conversion rates** (9.1%). **You will definitely see conversion and engagement rates from email increase once you remove dead weight from your list**.



When you clean the house, you can use a broom or a vacuum. You can also get a robotic vacuum that automatically cleans your floors while you sit back and relax. Likewise, email teams can conduct list hygiene processes themselves or rely on tools and partners to help them out.

Our survey found that 45.7% of senders are manually removing invalid and inactive contacts from their lists. Another 26.7% say they're only removing contacts who explicitly unsubscribe, which is not a proactive approach to list hygiene.

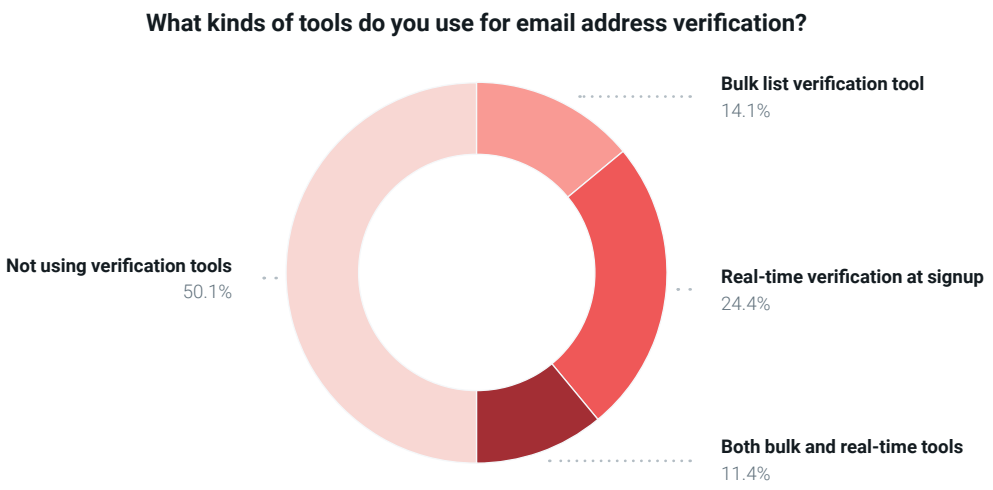
A total of 9% of senders rely on their ESP to remove invalid addresses, spam traps, and hard bounces. **Only 18.6% of senders say they are using software to automate list hygiene processes.**



A good way to keep a clean house is to make sure it never gets too messy in the first place. Email teams can do the same with their lists when they focus on email address verification. There are tools that help you catch things like fake contact information or typos in email addresses so they never make it on your list (or get fixed before they're added).

Some tools validate emails at signup while others examine the entire list and look for problematic contacts. Our survey found that 24.4% of respondents take advantage of **Real-time verification at signup** and another 14% use **Bulk verification tools**. Only 11.4% of senders are using **Both bulk and real-time tools**.

But perhaps most surprisingly, **more than 50% of the senders we surveyed say they are Not using verification tools at all**. That's going to make it a lot harder to keep your list clean, and your sender reputation could suffer along with your email engagement metrics.

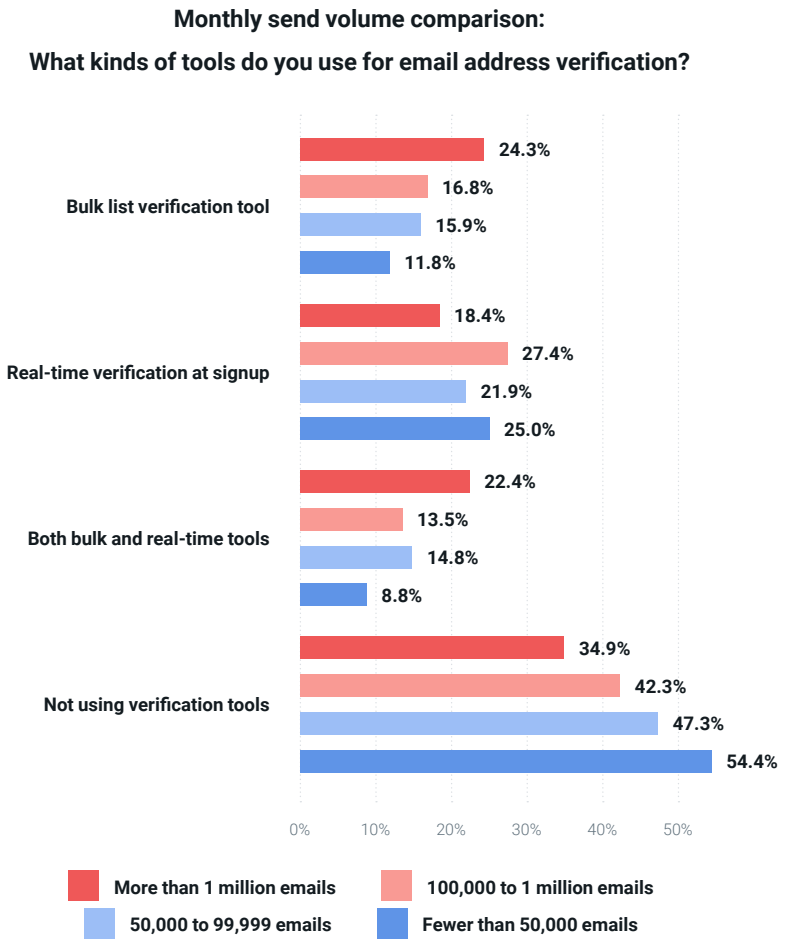


When you're consistently validating emails at signup, you can have more confidence in the quality of your list as it grows. Plus, real-time verification decreases the need for manual list hygiene and bulk verification. Still, there's value in being able to validate both individual signups and your entire list.

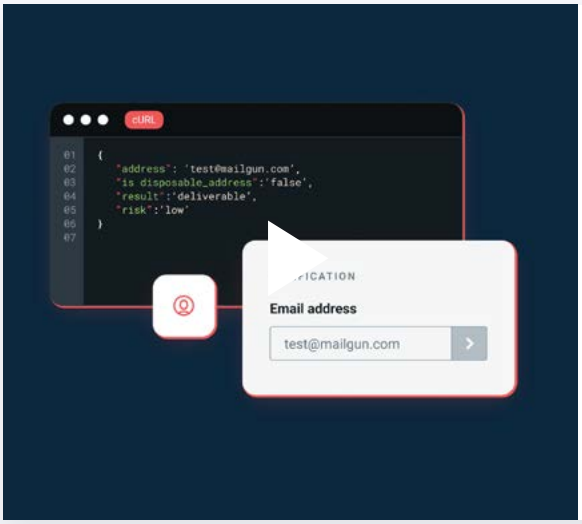
"Real-time verification lets you plug in an API wherever you have forms collecting contacts. What this does is it checks emails as they come in and validates them, including for things like spelling mistakes and high-risk addresses. Bulk verification can be very useful if you're aware of questionable list building practices or a lack of list hygiene in the past. It's also a good tool to use when you start a new job or inherit a list and need to be sure it's clean."

Natalie Hays, Product Marketing Manager, Sinch Mailgun

When filtering these survey results by sending volume, **it's clear that high-volume senders are more likely to use automated tools for list hygiene**. Those with the highest send volumes are more likely to use both types of tools, and those with the lowest send volumes are most likely to say they are **Not using verification tools**.



The bottom line is that list hygiene and proper acquisition practices lead to better email deliverability. That's because it ensures you're only sending to valid contacts and people who've actively opted-in to hear from you. When you automate list hygiene with helpful tools, it not only supports your sender reputation, but it also makes the job a lot less time consuming.



Future-proofing customer data with email validations

Find out how automating the process of email verification protects the integrity of your data while improving deliverability, engagement, and sales. Check out this discussion with Gavin Sherry and Nick Schafer.

Watch Now

PART 6

Best practices for better deliverability

We've covered a lot of ground in this report, including expert advice and guidelines for achieving high deliverability. Let's review 12 of the most important best practices for reaching the inbox and avoiding the dreaded spam folder.

1. Choose the right email infrastructure

Deliverability starts at square one. That includes the servers, domains, and IP addresses used for your email sending infrastructure.

Perhaps the biggest decision you'll make is whether to use a shared or dedicated sending IP. Dedicated IPs may be a necessity for high-volume senders. Remember that the behavior of other senders on a shared IP may affect your deliverability. With a dedicated IP, you only have yourself to blame for deliverability issues.

More about email infrastructure →

2. Warm up new IPs and domains before you start sending

Without a sending history, mailbox providers may be suspicious of emails coming from a brand-new sending domain or IP. You need to take things slow at the start and ramp up to high-volume sending.

Be sure to warm up IPs and domains, which allows you to establish credibility with receiving mail servers. Without a proper warm-up period, you may experience deliverability issues such as throttling, greylisting, or outright blocking of your messages.

Find out how domain/IP warm-up works →

3. Separate transactional and marketing messages

If automated transactional emails are a crucial part of your program, consider separating these messages on their own IP addresses or subdomains. This protects them from being associated with marketing emails that have a reputation for being more likely to get filtered into spam.

People expect transactional emails to arrive in a timely manner and land in their inboxes where they're easy to find. These communications are an important part of the customer experience, and their deliverability should be a priority.

More on transactional email deliverability →

4. Achieve delivery rates above 95%

While the delivery rate metric is only one of many ways to measure deliverability, it's a good starting point. Average delivery rates could be as low as 80% to 85%, but you should aim for better than average.

Transactional email delivery rates should be near 99% while marketing emails should try to achieve delivery rates as close to 95% as possible. A sudden drop in the delivery rate could indicate your emails are being blocked.

More on deliverability metrics →

5. Test and monitor inbox placement

The inbox placement rate is a measurement that can tell you the most about deliverability. It measures the percentage of delivered emails that actually land in the inbox (not spam). But many email sending platforms lack this sort of data.

Find a service that helps you with seed testing and provides inbox placement reports. This will give you detailed insights into how major mailbox providers filter your messages.

More on improving inbox placement →

6. Track email engagement over time

Trends in metrics such as opens and clicks are important to monitor, and they can help you identify deliverability issues.

A dip in engagement may mean more emails are landing in spam and you need to make changes. Higher levels of engagement prove you're delivering quality content to the right people and that your growing list of contacts is valid and healthy.

Get key learnings from a global email engagement study →

7. Understand your sender reputation

Engagement rates are one of many things mailbox providers evaluate when scoring your sender reputation. They'll also pay attention to unsubscribes, spam complaints, and whether you're sending mail to inactive and non-engaged contacts – just to name a few factors.

Senders with a good reputation always put subscribers first. Use services like Google Postmaster tools and find platforms that integrate with sender reputation tracking tools to better understand your sender reputation.

Get tips to improve sender reputation →

8. Monitor blocklists

Landing on a blocklist could be a huge problem, or it may barely impact email deliverability. The most important blocklists to avoid are run by Spamhaus.

Blocklist monitoring alerts you when your messages are being blocked so you can start the delisting process as soon as possible. You can also adjust your sending strategy to reduce any negative impact on the business. That could include temporarily moving a mail stream to a different sending IP to keep messages flowing during remediation.

More on what to do if you're blocklisted →

9. Use strong email authentication

Mailbox providers have the tough job of identifying legitimate mail and separating it from unsolicited spam and malicious messages. You can help by using email authentication protocols that verify you are the authorized sender and not a bad actor.

While SPF and DKIM cover the basics, you can strengthen your authentication using DMARC. But make sure you eventually enforce DMARC with a policy of either reject or quarantine.

Get an overview of email authentication →

10. Implement safe list building strategies

Purchasing email addresses or harvesting them from around the web is how spammers conduct list building. If you don't want to land in spam, don't do these things.

Legitimate senders who prioritize deliverability are careful about who gets added to their list. Consider using a double opt-in process for new subscribers and use a sunset policy to identify inactive or disengaged contacts over time.

Get advice on growing your email list →

11. Segment subscribers by engagement

Pay attention to the cues subscribers are giving you. If there are contacts who are less likely to engage, maybe they only need to receive your most important marketing messages.

Manage your list by creating different segments for active and inactive subscribers based on their levels of engagement. This turns segmentation into a strategy for both marketing and deliverability purposes. You can even segment new subscribers from the start until you find out if they're going to be engaged or not.

Find out more about strategic engagement segmentation →

12. Take advantage of email verification tools

Your deliverability strategy starts with the signup form. If you can verify the validity of new contacts before you start sending to them, email list hygiene becomes much easier.

For real-time verification, look for a service that uses cached send data. That's much faster and more reliable than the broken SMTP handshake method used by many email validation services. Bulk email verification is also useful if you ever need to evaluate the quality of your entire list.

More on what to look for in a verification tool →

"If you're not following best practices for email deliverability, it's going to catch up with you eventually. Once you've invested in the right infrastructure, authentication, and marketing technology, focus on maintaining good list hygiene while delivering high-quality, relevant content to engaged subscribers."

Kate Nowrouzi, VP, Deliverability and Product Strategy, Sinch Mailgun

CONCLUSION

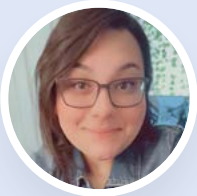
Deliverability: Why IT and marketing need to team up

The IT crowd and the marketing team have different points of view, goals, and responsibilities. While IT professionals are working to keep technology running smoothly, marketers are working to reach people.

Email deliverability is one area in which the worlds of IT and marketing intersect. The efforts and failures of one department will inevitably affect the other. So, these teams and individuals are going to need to work together.

- IT professionals make email infrastructure decisions for different types of mail, which could impact deliverability if technical mistakes are made or if they hire the wrong technology partner.
- Marketing teams oversee list building practices that could lead to high engagement or destroy a brand's sender reputation with mailbox providers.
- Technical teams are responsible for setting up and testing email authentication protocols that make the inbox a safer place by making it easier for mailbox providers to identify spam.
- Email marketers lead strategies surrounding important sending practices. That includes segmenting disengaged contacts and delivering relevant content to the right people at the right time.

There are two sides to the email deliverability coin. If you want to consistently reach the inbox, you need a solid understanding of both the marketing and technical aspects. Deliverability has a direct impact on your email ROI. To get the most out of this communication, you need to develop a strategy for your organization. To do that, you need the right knowledge, tools, and technology partners.



"Meeting in the middle and bringing technical teams and email marketers together is what helps you be successful because you're able to have your marketing team meet their goals while making sure it's done in a proper manner that supports deliverability."

Ashley Rodriguez, Deliverability Engineer, Sinch Mailgun

How we can help

Sinch Mailgun is an email platform with solutions for both technical users and marketing teams. Developers love our flexible email sending API, and marketers can easily create campaigns with our drag-and-drop email template builder.

Mailgun Optimize also offers industry-leading ways to **monitor and improve email deliverability** with a suite of tools and expert support:

- Inbox Placement Testing from Mailgun Optimize gives you unprecedented insights into where your messages land. Use it to catch deliverability problems before they impact your business. This feature also includes checks on the status of email authentication protocols.
- Mailgun Validate gives you effective ways to verify and optimize new and existing contact data. Make sure new subscribers enter valid addresses with real-time validation at signup and use full list validations for overall hygiene. This product is available as a standalone solution or as part of the Mailgun Optimize suite.
- Reputation Monitoring includes a variety of valuable features. Monitor for spam traps and blocklists. Get notified when your IP is listed so you can take immediate action. Review Bounce Classifications to understand why messages aren't delivered. Plus, integrate Mailgun with Google Postmaster Tools and Microsoft SNDS to keep tabs on your reputation with Gmail and Outlook.
- Email Previews show you how 100+ different email clients and devices render your marketing emails. Notice a problem? Adjust the code before you hit send to be sure campaigns display as expected and subscribers can easily engage.
- Deliverability Services from Sinch Mailgun puts an expert on your team. Get a custom deliverability strategy for your organization, including monthly reports on email program health and performance.

Not using Sinch Mailgun to send and receive emails? Not a problem. **You can take advantage of deliverability solutions from Mailgun Optimize with any email service provider.**

Start Optimizing Your Deliverability

About this survey

During May of 2023, Sinch Mailgun surveyed its customers as well as email senders from its sister brands, Mailjet by Sinch and Email on Acid by Sinch. The survey collected data and insights concerning the email deliverability knowledge and practices of senders around the world.

More than 1,980 individuals completed the survey. Respondents were invited to participate via email messages as well as in-app communications. They were also incentivized to participate by the chance to win a $100 Amazon gift card, which was awarded to one random customer. See below for further information on respondent demographics. Due to rounding, the sum of percentages in certain survey results may exceed or fall short of 100% by a difference of 0.1%.

Regional

- United States: 22.5%
- France: 18.4%
- India 4.8%
- United Kingdom 4.1%
- All other regions: 50.2%

Business size

- 10 or fewer employees: 50.6%
- 11 to 50 employees: 24.8%
- 51 to 500 employees: 16.2%
- 501 to 1,000 employees: 3.3%
- 1,001 to 5,000 employees: 2.8%
- More than 5,000 employees: 2.4%

Business type

- B2C: 28.4%
- B2B: 34.4%
- Both B2B and B2C: 37.2%

Monthly email send volumes

- Fewer than 50,000 emails: 64.3%
- 50,000 to 99,999 emails: 14.2%
- 100,000 to 1 million emails: 13.8%
- More than 1 million emails: 7.7%

Job title

- Software developer: 18.6%
- IT professional: 15.4%
- Small business owner: 14%
- Marketing leadership: 10%
- Email/digital marketer: 8.7%
- C-suite executive: 8.0%
- Director/VP of product: 7.0%
- Freelancer: 6.9%
- Product management: 6.6%
- Email deliverability specialist: 4.2%
- Reliability engineer: 0.6%

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**.