twilio

2024 Email Deliverability Guide

Improve the way your email is delivered



Over the past year, significant updates from major inbox providers like Google and Yahoo have reshaped the email deliverability landscape. New sender requirements and stricter filtering mechanisms mean that maintaining a strong sender reputation and reaching the inbox requires more art and science than ever.

Fortunately, you've got SendGrid's team of email experts at your back. We eat, sleep, and breathe email–and we have all the updates you need to stay on top of your email deliverability in 2024 and beyond.

When the first email was sent in 1971, no one knew the lasting impact this channel would have over 50 years later. Today, email is still alive and thriving. It boasts the highest ROI of any marketing communications channel, to the tune of $36 returned for every dollar spent. And recipients of all ages use and love it. From Baby Boomers to Gen Zers, folks continue to choose email to communicate with their favorite brands.

That said, email is not a set-it-and-forget-it solution.

While powerful, it requires ongoing effort and routine maintenance to ensure your messages land in customer inboxes. Maintaining strong email deliverability requires regular work as it's constantly shifting and adapting. That's why we update and release a new version of this guide every year.

Fortunately, getting to the inbox is the sender's responsibility, so there's a lot you can do to ensure your messages arrive in the right inboxes at the right time. In this guide, we'll take a closer look at what deliverability is and why it matters, the steps you can take today to guarantee your messages land in customer inboxes, and more.

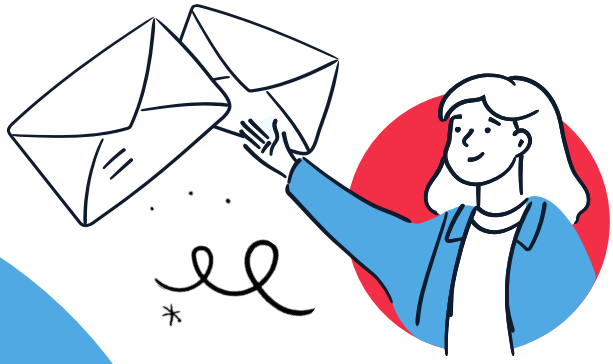
New additions in our 2024 guide:

- New Google and Yahoo! Sender Requirements
- Generative AI and Email Sending
- Secured Signup Forms
- DMARC Policies and Implementation

Contents

1. **New Google And Yahoo! Sender Requirements**
2. **Generative AI And Email Sending**
3. **What Is Email Deliverability?**
4. **What Is Sender Reputation?**
5. **Maintaining Your Reputation And Keeping Recipients Happy**
6. **The Continued Focus On User Experience**
7. **Infrastructure And Authentication**
8. **Privacy & Compliance In A World Of Engagement**
9. **SMS: A Complementary Channel Of Communication**
10. **Helpful Email Deliverability Tools**
11. **Summary**

New Google and Yahoo! Sender Requirements



Inbox providers like Gmail and Yahoo! are constantly battling to protect their users' inboxes from unwanted messages. This year, both providers introduced new sets of requirements for senders. These were made effective in February 2024.

These requirements aim to filter out spam and ensure that only legitimate, desired emails reach users. Senders who fail to comply will start rejected emails or emails filtered to the spam folder. This increase will continue throughout the year.

As of June 2024, senders also need to provide a one-click unsubscribe to their emails.

Ask The Expert:



Denis O'Sullivan, Sr. Deliverability Consultant

Denis has been working in the email marketing space for 12 years, with most of that time spent managing email programs for various brands. A native of Ireland, Denis now lives in Colorado, where he enjoys exploring nature with his family.

> **"Legitimate senders should be thrilled with the new Google and Yahoo sender requirements. The majority of spammers won't be able to meet the requirements and your customers' inboxes will be less cluttered as a result."**

Most of these new requirements have been considered best practices for years. Gmail and Yahoo! are now making these practices enforceable standards to ensure a higher quality of email communication.



Here's a detailed look at each requirement and how you can comply:

1 Set up SPF and DKIM Email Authentication for Your Domain

- What It Means: SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) are foundational email authentication methods that verify the sender's identity and protect against email spoofing.
- Action: Ensure your SPF and DKIM records are properly set up through your domain authentication process.

2 Ensure Sending Domains or IPs Have Valid Forward and Reverse DNS Records

- What It Means: Reverse DNS (PTR records) allows mailbox providers to verify the sender when they perform a reverse DNS lookup upon receipt of emails.
- Action: Set up reverse DNS on your sending IP address. For shared IP users, this is already handled.

3 Keep Spam Rates Reported in Postmaster Tools Below 0.3%

- What It Means: Maintain a spam complaint rate below 0.3% as reported by Google Postmaster.
- Action: Sign up for Google Postmaster Tools to monitor and manage your spam complaint rates. It's important to note that the spam rate you see in Google Postmaster will likely be higher than you see with other providers in your SendGrid reporting, due to different methods of calculation.

4 Format Messages According to the Internet Message Format Standard (RFC 5322)

- What It Means: Adhere to the correct format for email messages, including headers, body, and attachments.
- Action: Ensure your email components meet RFC 5322 standards. SendGrid blocks non-compliant emails.

5 Don't Impersonate Gmail From: Headers

- What It Means: Avoid using Gmail addresses in your From: header to prevent delivery issues.
- Action: Use your own domain's email addresses in the From: header.

6 Add ARC Headers to Forwarded Emails

- What It Means: ARC (Authenticated Received Chain) headers verify previous authentication checks for forwarded messages.
- Action: Implement ARC headers if you regularly forward emails via mailing lists or inbound gateways.



7 Set up DMARC Email Authentication for Your Sending Domain

- What It Means: DMARC (Domain-based Message Authentication, Reporting & Conformance) builds on SPF and DKIM to protect against email spoofing.
- Action: Add a DMARC record to your DNS and configure it to align with your SPF and DKIM settings.

8 Align the Domain in the Sender's From: Header with Either the SPF or DKIM Domain

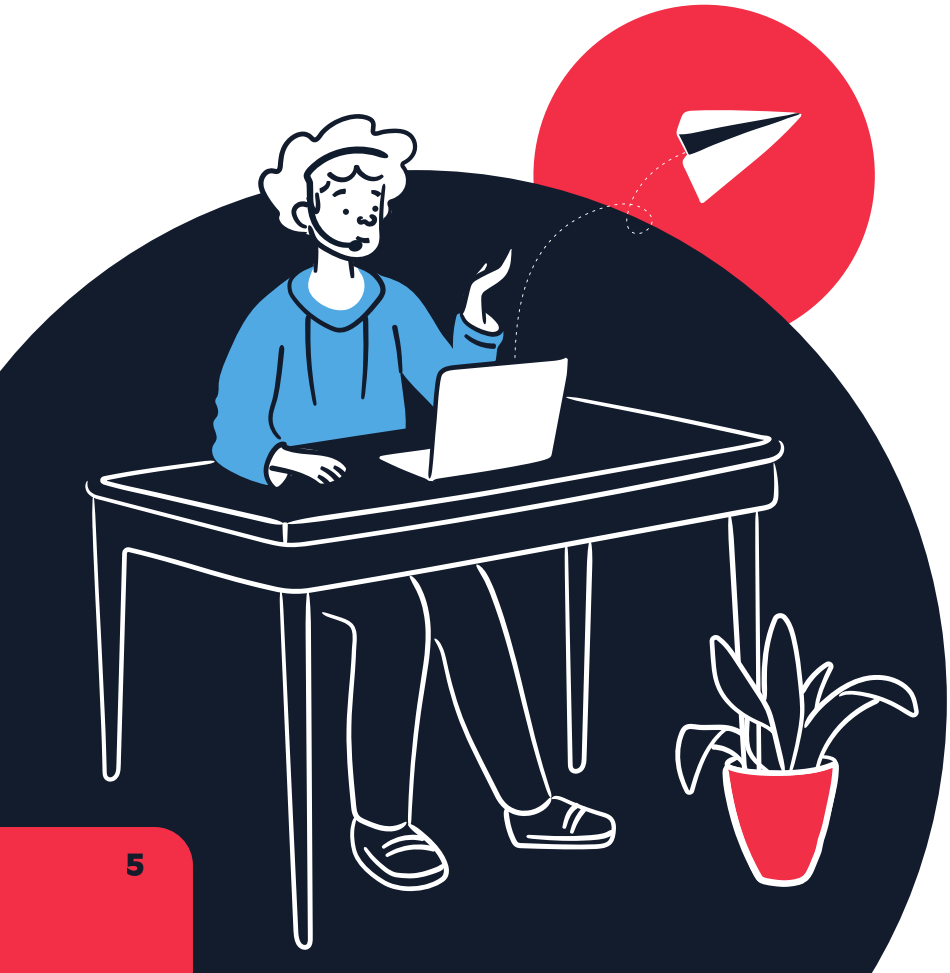
- What It Means: Ensure the domain in the From: header matches the domain used in your SPF or DKIM authentication.
- Action: Verify domain alignment in your email headers to comply with DMARC requirements.

9 Enable One-Click Unsubscribe and Include an Unsubscribe Link

- What It Means: Provide a clear and easy method for recipients to unsubscribe from your emails.
- Action: Implement one-click unsubscribe features in your emails.

10 Use a TLS Connection for Transmitting Email

- What It Means: Ensure all email transmissions are secured with Transport Layer Security (TLS).
- Action: SendGrid handles TLS connections, so this requirement is automatically met.



For senders overwhelmed by these new requirements (especially those sending over 5,000 messages per day), our Professional Services team is available to help navigate domain authentication, DMARC setup, and other compliance issues.

Contact us today for expert guidance and support.

Generative AI and Email Sending

Generative AI is transforming the landscape of email marketing by enabling more personalized, efficient, and effective communication. AI-driven tools can assist in writing, optimizing, and sending emails to guarantee your campaigns resonate with recipients and achieve higher engagement rates.

Generative AI can craft highly personalized email content tailored to individual recipient preferences and behaviors. It can analyze past interactions, purchase history, and demographic information to generate emails that more likely to engage and convert:

Dynamic Content Generation:
AI can create unique email content for different segments of your audience so that each recipient receives a message that speaks directly to their interests and needs.

Subject Line Optimization:
AI tools can test and optimize subject lines to improve open rates by predicting which variations are most likely to catch the recipient's attention.

Behavioral Triggers:
AI can automate emails based on recipient actions, such as cart abandonment, browsing history, or previous purchases.

AI can also optimize the sending process to send emails at the right time and frequency to maximize engagement:

Send Time Optimization:
AI analyzes recipient behavior to determine the best time to send emails and increase the likelihood that the email will be opened and read.

Frequency Management:
AI helps balance the frequency of emails to avoid overwhelming recipients while maintaining regular engagement.

A/B Testing and Continuous Improvement:
AI can automate A/B testing for various elements of your emails to continuously learn and improve the performance of your campaigns based on real-time data.





Privacy Considerations with AI

While AI offers huge advantages in email marketing, it also raises important privacy considerations. Double-check that your use of AI complies with privacy regulations and respects recipient data to maintain trust and avoid legal pitfalls:

Data Protection Laws:
Maintain compliance with data protection regulations such as GDPR, CCPA, and others. This includes obtaining explicit consent for data collection and providing clear information on how data will be used.

Transparency and Consent:
Be transparent about your use of AI in email marketing. Inform recipients if AI-generated content or decisions are being used and obtain their consent where necessary.

Data Security:
Implement security measures to protect recipient data from breaches and unauthorized access. Use encryption and secure storage solutions to safeguard sensitive information.

Ethical Use of AI

Generative AI is fresh and exciting, but it's far from perfect. You'll need to keep an eye on a few factors to maintain ethical use:

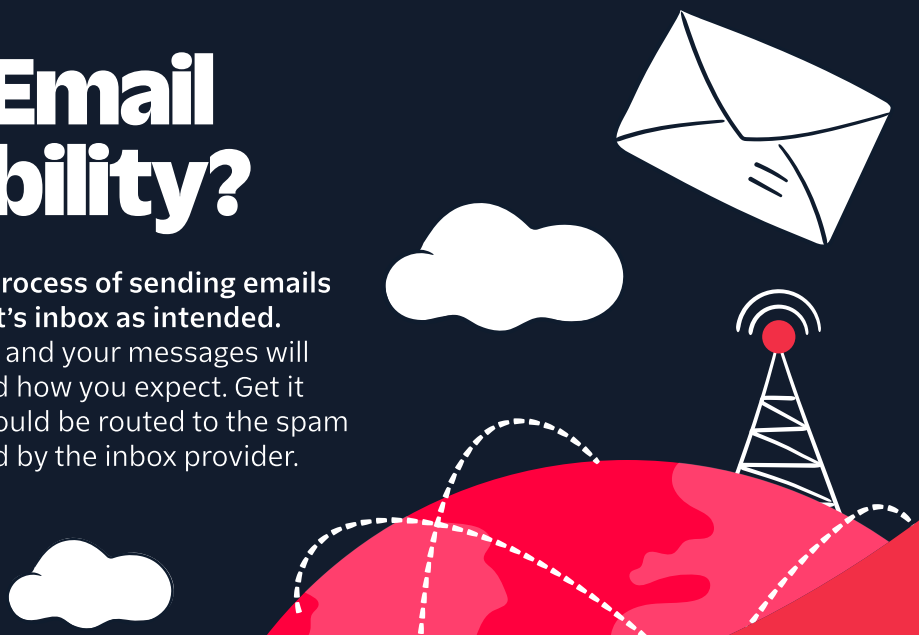
Avoiding Bias:
Check that your AI models are free from biases that could affect the fairness and inclusivity of your email campaigns. Regularly audit and update AI algorithms to maintain ethical standards.

Maintaining Human Oversight:
While AI can automate many aspects of email marketing, you'll still need to provide human oversight. Double-check that AI-generated content aligns with your brand values and messaging guidelines.

Respecting User Preferences:
Allow recipients to easily opt-out of AI-driven personalization if they prefer. Provide options for recipients to manage their preferences and control how their data is used.

What Is Email Deliverability?

Email deliverability is the process of sending emails that arrive in your recipient's inbox as intended. Get your deliverability right, and your messages will arrive in the inbox when and how you expect. Get it wrong, and your message could be routed to the spam folder or completely blocked by the inbox provider.



To maintain consistent delivery rates, businesses need to constantly prioritize their email program's health. This means properly establishing your infrastructure and authentication, maintaining a positive sending reputation, creating a great user experience, and adapting your program to meet new and changing regulations.

Unfortunately, most businesses only get serious about deliverability after they experience a major issue – once the damage is already done. With the right expert solutions, your deliverability issues can be fixed, but it's much better for you and your recipients to focus on prevention rather than a cure.

Best Practice Tip:

What's an Inbox Provider?
Common inbox providers include Gmail, Yahoo, Outlook, and Hotmail. These providers offer users a secure place to engage with email by scanning the content of the messages to filter spam, as well as prevent phishing and other unwanted email.

Deliverability isn't just a nice-to-have–it's a need-to-have. Email has the highest ROI of any digital marketing channel, but that's not even the most valuable part. Think about the critical emails your customers need to receive:

- Password resets
- Confirmations
- Shipping notifications
- Opt-ins
- Order receipts

If these emails don't arrive, you're not only losing sales. You're losing trust. You're losing loyalty. And you're eventually losing customers and subscribers.

Best Practice Tip:

Small Deliverability Improvements Can Make a Big Difference
Deliverability and ROI aren't some distantly connected concepts – they have an undeniable relationship. Even tiny improvements in deliverability can make a big impact on the success of your email program.

Improving your inbox rate by just 1% means more customers see your emails and can take engage with them, leading to increased opens, clicks, and conversions.



Wondering how much deliverability could be costing your business?

Use our free roi calculator to how a 1% increase in deliverability could help your business.



If you're already experiencing deliverability issues, don't panic. If this guide, the Knowledge Center, and our other free resources don't fix the problem, we have experts who can help.

Clients who use our Expert Services see an average:

97%
delivery rate
(12% over the industry average)

6% increase
in open rates

9.3 out of 10
satisfaction score

Having issues getting into the inbox or can't pinpoint why your current strategies aren't working?

It's time to work with a Twilio SendGrid delivery consultant.



Email is complicated, but our experts offer hands on support for even the most complex email programs. They can help you get set up for success or solve underlying issues – whatever your needs and budget require.



What Is Sender Reputation?

Your email deliverability is largely determined by your sender reputation. The better your reputation, the more likely your email will be delivered to your recipient's inbox.

So, how can you improve your reputation? Your sender reputation is determined by a variety of factors, including:

- Recipient engagement
- Email content
- Spam complaints
- Spam traps
- Invalid email addresses
- Block lists
- Domain reputation

Your sender reputation (like any great brand or personal reputation) is hard to earn, easy to lose, and takes time to build, but essentially it boils down to one simple idea: send emails users want.

Having recipients who regularly open, read, and click on your messages signals to inbox providers that your messages are both wanted and valuable. That's why it's important to always prioritize recipient engagement and send engaging messages your subscribers want to receive.



5 Ways to Check Your Sending Reputation

Wondering how your business's sending reputation is holding up? Check it now and find out.



Recipient Engagement

Every time a recipient interacts with your emails, they share important feedback with your brand around what they like and dislike. Opens, clicks, and forwards are positive indicators that your recipients like what you send, while unsubscribes and spam reports indicate your recipients don't want your messages. Of course, there are other types of positive and negative engagement that are harder to track.

Depending on the inbox provider, you might want to know how many times a message is:

- Opened
- Clicked
- Forwarded
- Ignored
- Deleted without being opened
- Moved to another folder

Inbox providers use all these signals to evaluate every email campaign you send. You won't know for certain which elements carry the most weight and which new engagement cues they're taking into consideration (which is why we publish this deliverability guide every year).

For example, if your email campaigns are getting very low open rates, inbox providers may start filtering your future emails to spam because your recipients indicate that the email is unwanted. Or, if you're getting high unsubscribe rates, inbox providers might read this as another signal that you're sending unwanted mail.

Check out these additional design resources:

- 9 Strategies to Increase Email Engagement
- 13 Types of Email Content Ideas to Amp Up Your Engagement
- Customer Engagement Inspiration Guide

Best Practice Tip:

The Upside to Unsubscribes
Don't take unsubscribes personally. Sending to an unengaged audience hurts your sending reputation, so your recipient is doing you a favor by unsubscribing instead of ignoring your messages or marking them as spam.

Email Content

Email content refers to everything from the words, images, GIFs, templates, links, preheader text, subject lines, and from addresses you use in your emails. All of this content can either help or hurt your reputation. You can build a good reputation over time if you regularly send engaging emails with a professional look and legitimate links.

If you're looking for some design help, check out our free email marketing template gallery– it's chock-full of plug-and-play templates you can use for just about any email use case. Each template is highly customizable so you can incorporate your brand's logo, branding, and voice to create simple, stunning emails.

Check out these additional design resources:

- Our Picks for Free Design Tools for Marketers
- 10 Tips for Designing and Developing Emails
- How To Maintain Brand Standards in Your Email Designs



Ask The Expert:
Ashley Ortiz, Sr. Delivery Consultant

Ashley is a Sr. Delivery Consultant on the Twilio SendGrid team. She's worked at Twilio SendGrid for over 5 years and has helped countless businesses improve their email programs.

"Because there are so many nuances to deliverability, there is no one mailing practice that, when implemented, is a guarantee of success. However, sending relevant and timely content that meets consumer expectations is the best way to maximize the likelihood your mail reaches its intended destination: the inbox.

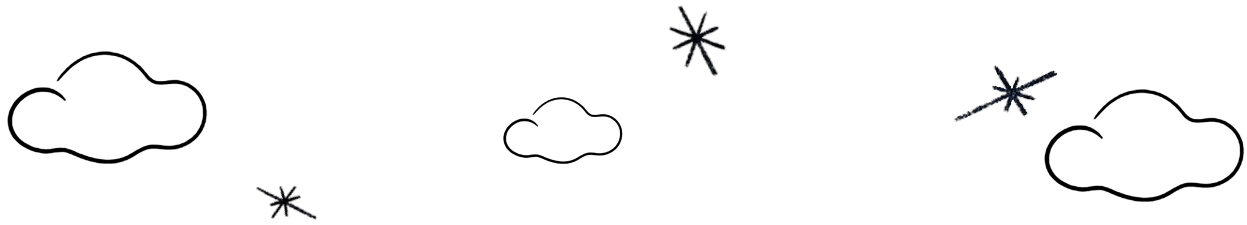
TL;DR: Send mail people love."

Spam Complaints

A recipient marking your email as spam is the strongest negative signal to inbox providers. Spam complaint rates even lower than 0.08% are considered high, and these levels can lead to poor deliverability. Some inbox providers consider spam rates even lower than .08% as high, so you should always keep a close eye on your spam complaints after each campaign. Learning to listen to rather than fight against spam complaints is a key skill of advanced email programs.

Additional resources:

- 10 Tips to Stop Your Emails From Going to Spam
- Why Are My Emails Going To Spam?
- What Your Recipients Think of Spam



Spam Traps

Spam traps are old or unused email addresses that should never receive your emails. They hurt your engagement and are a signal that your list is not well-maintained.

In fact, ISPs and anti-spam organizations intentionally plant email addresses to catch spammers and list buyers. These could be email addresses that never signed up to receive communications (AKA pristine spam traps or honeypots) or emails that haven't been used recently (AKA recycled spam traps), but each pose a threat to your sending reputation.

For this reason, it's important to avoid renting, scraping, or purchasing email addresses, as those recipients did not sign up to receive your content and will likely provide little to no engagement. Instead, focus on building a healthy, engaged contact list over time. As your list grows, avoid these spam traps by periodically removing recipients that no longer engage with your emails or have gone long periods without engagement.



Check out these additional resources:

- Spam Traps: What They Are and How to Avoid Them
- Email List Hygiene: 5 Tips to Help You Keep Your Lists Clean
- 50 Shades of Graymail: Why Your Email Ends Up in the Spam Folder

Best Practice Tip:

What Is List Scraping?
List scraping or list harvesting is the process of using software or a bot to crawl through different websites and find email addresses that can be added to your contact list. The problem with this strategy is that they (and their respective recipients) have no relationship with you or your company, which means that you shouldn't be sending them any email.

Only send your emails to people who have indicated an interest in your product or service or asked for your emails outright. Otherwise, you're at risk for spam complaints and a damaged sender reputation.

Invalid Email Addresses

Continuing to send email to large groups of invalid or nonexistent email addresses is a big red flag for inbox providers and can damage your sending reputation. Here are a few tips on how to remove invalid email addresses:

1. **Regularly clean your active mailing list** to remove bounced and non-engaged email addresses can ensure your lists remain clean and engaged.
2. **Send confirmation emails to new recipients.** This process validates their email and confirms that they want your messages. This ensures everyone on your list willingly and knowingly signed up to receive your messages.
3. **Send welcome emails** to gauge the use and validity of an email address. You can set up an automated workflow to remove these invalid recipients from your mailing list if your welcome emails bounce.

"One of the things I have to work on most often with my clients is updating their list acquisition methods," says Ashley Ortiz, a Senior Email Delivery Consultant at Twilio SendGrid. "Rather than bringing over an old list, buying a list from someone, or scraping email addresses off social networks, senders need to create opportunities for people to provide their email addresses legitimately."

So how can you responsibly grow your email marketing list? Try leveraging other digital channels to build your email list rather than sending unsolicited emails that could damage your reputation. You can use channels like display ads to reach new potential subscribers that may be interested in signing up for your communications. Just drive interested parties to a landing page explaining the benefits of receiving your emails and collect their permission to send to them.

Best Practice Tip:

Avoid "Typo" Traps

Recently, we've seen "typo" traps become very common among senders. Avoid this trap by making sure your address collection methodology removes typos in email addresses (e.g. local@gmall.com vs. local@gmail.com) and double-checking that recipients interact with an opt-in or subsequent welcome message before including their address in email campaigns. If you want to take this one step further, we recommend using Kickbox to clean your list of typos prior to sending.

Additional resources:

- 3 Reasons Why You Shouldn't Buy an Email List
- How to Use SMS to Grow Your Email List
- The Best (and Worst) Ways to Verify Email Addresses



Catch misspelled, fake, or invalid email addresses at sign-up

Use Twilio SendGrid's email validation api to deliver more messages to real contacts.



Ask The Expert:

Denis O'Sullivan, Sr. Deliverability Consultant

"While it's crucial to any email program to see database growth, it's even more important to make sure the correct recipients are opting in. Test out several methods for generating new subscribers, but make sure to closely monitor the engagement and complaint levels from each of these sources so you know where to focus your efforts and your budget in order to attract high quality recipients."

Blocklists/Denylists

Many inbox providers monitor blocklists to help determine which senders need to be blocked or filtered. Most blocklists will list your IP address or sending domain if they notice a high number of:

- Spam trap hits
- Spam or junk complaints
- Or a combination of both

You can avoid blocklists by sending relevant content to recipients who have recently engaged with your emails.

Just because you're on a blocklist doesn't necessarily mean that your deliverability will suffer. Some blocklists have a much greater impact on deliverability than others. If you're interested in seeing whether or not you've been blocklisted, we think MXToolBox is the best free lookup option.

Additional resources:

What Are Email Denylists and How to Avoid Them

Best Practice Tip:

Be Wary of Pay-to-Play Blocklists
Not all blocklists are created equal. Some are more prominent than others and may have a larger impact on your sending reputation if you get listed. Keep in mind that some blocklists have moved to a pay-to-play model, wanting senders to pay to get delisted rather than prove their reliability as a sender. If you believe you have been blocklisted or may be targeted in pay-to-play blocklist, it's likely time to talk to a Twilio SendGrid Delivery Consultant and get their expert advice.



Best Practice Tip:

Pay Attention to Cousin Domains
Cousin domains are triggers for inbox providers. For example, let's say that company.com also uses company-mail.com, companymail.com, and companydeals.com to segment different email streams. Those extra domains could impact your deliverability, so it's important to practice responsible sending from every one of these domains.

Domain Reputation

Your sending domain has a reputation associated with it – and it's equally as important as your IP address's reputation. If messages sent from your domain generate a negative response from recipients, it won't matter what IP addresses the messages come from–they may still be filtered by inbox providers.

Watch your links to third parties–they could do more harm than good. Even if you're doing everything else right, a single link to a disreputable website in the body of your email could prevent your message from getting to the inbox. Be sure you're only linking to trusted websites and sources and, ideally, only those you control.

Additional domain reputation resources:

Email Sending Reputation 101: IP Reputation vs. Domain Reputation

What is Domain Reputation and Why is It Important?

Maintaining Your Reputation and Keeping Recipients Happy

Best Practice Tip:

Be a Polite Inbox Guest
Be a polite guest in the inbox by asking for permission to send email to a recipient and then honoring the terms of that permission. If a recipient agrees to receive your weekly newsletter, you're asking for trouble if you start to send them daily offers.

Now that we've covered all of the different factors inbox providers take into account when evaluating your emails, it's time to look at the messages you're sending.

The actual messages you send have a big impact on your deliverability and the ways that recipients engage with them. Below are some of our best tips for creating and sending email campaigns that engage and interest recipients.

Ask Permission and Respect It

Unlike other forms of marketing and advertising, email recipients have the choice of whether or not they open or even receive email communications from your brand. Think of your brand as being a guest in a recipient's inbox. If you aren't polite and respectful (or if you wear out your welcome), you'll get kicked out.

Secure Your Signup Form

Emily Thrasher, one of our Senior Email Deliverability Consultants, recommends you secure your signup form. If your website collects email addresses via web forms and doesn't have appropriate defenses in place, your site may become a funnel for abuse. By ignoring the risk nefarious actors pose for unsecured signup forms, you increase the risk of damaging your brand reputation.



Here are some best practices to implement with your signup forms:

Add CAPTCHA to your sign up form to prevent bot signups. Google's free reCAPTCHA is a good option to integrate. If you use Marketing Campaigns, consider using our Signup Form solution which includes reCAPTCHA.

Validating email addresses helps to identify mistyped, inactive, non-existent, disposable, or shared (team@, help@) addresses that pose a risk for your list hygiene. With a clean list, you reduce your bounce rate and perform better with mailbox providers to improve delivery. Twilio SendGrid has an email validation API that allows for real time verification via website forms.

Be wary of allowing social media signups– oftentimes, users sign up with social media accounts linked to very old, if not disabled, email addresses. These types of signups are also vulnerable to abuse. Make sure you are still collecting consent and confirming opt in for users who sign up via this method.

Use double opt-in, even if the above best practices are implemented. This is the most accurate way to confirm a real human has signed up, is actively using their mailbox, and is genuinely interested in your brand. This also ensures your email program is aligned with Twilio SendGrid's Email Policy and complies with applicable laws, regulations, and industry standards/ guidance.



Create an Email Preference Center

This goes hand-in-hand with being a welcome guest in your recipient's inbox. An email preference center allows users to tell you exactly what types of email they're interested in receiving. The key to a healthy email program is sending messages that people are interested in receiving.

As Jessica Hunt, a Senior Email Deliverability Consultant at Twilio SendGrid, puts it, "The first question senders should ask themselves before sending is 'are my recipients expecting to receive this email?' If the answer is anything other than a resounding 'yes' then you should rethink sending that email to your recipients.'

Creating and maintaining an email preference center takes out the guesswork of knowing what your recipients care about. By simply asking your recipients exactly what they want and how often they want it, your business can create an email program tailored to their individual preferences.

Additional resources:

- 3 Types Of Email Preference Centers
- Email Preference Center Perfection

Send a Welcome Message

A well-written welcome message helps set the tone for a new email relationship. Welcome messages should remind users why they signed up for your email program. This message should arrive after sign-up as close to real-time as possible and detail what kinds of email the recipient can expect to receive from you and how often they'll receive it. Welcome messages should also include unsubscribe and preference center links.

Additional resources:

- 11 Effective Welcome Email Campaign Examples
- The Welcome Email Series: Strategy and Benefits of a Layered Brand Introduction

Test Before You Send

Before you send any emails, it's important to test your messaging and content to know how it'll perform when it gets to the inbox. Twilio SendGrid's Email Testing tool helps our customers see how their emails will look across any inbox client, browser, or device, while also checking how the message will perform against the most powerful spam filters. Even little mistakes like broken links can lead to a decline in your deliverability in the long run, so testing your content before you send is crucial.

Additional resources and testing tips:

- Test for Success: Email Testing for Your Programmatic Sending
- Email Testing: Spam, Links, and Rendering Tips
- Email Testing Walkthrough and Examples: Send Flawless Emails Every Time



Bundled Messages in Gmail Promotions

While many people worry the promotions tab is a commercial/promotional purgatory where messages are sent to float infinitely through the digital abyss, Gmail users still regularly check and engage with the tab.

Plus, Google has been working to improve the promotions tab for both marketers and subscribers alike since its inception. Senders have the ability to add "annotations" to promotional messages to call out discounts, add company logos, and highlight helpful information including deal amounts and expiration times. This can help your recipients easily spot your brand's email and understand the value it can offer them. Gmail, in conjunction with their machine learning, uses these annotations to provide recipients with "bundles" of messages most relevant to their interests at the top of the promotions tab.

Segment Your Emails

Effectively segmenting your emails could improve your engagement, which can help lead to higher deliverability rates. New to audience segmentation? Try sending emails based on recipient:

- Timezones
- Engagement levels (those who open and/or click on your emails)
- Sign-up dates
- Purchase histories
- Gender
- Age

Grouping subscribers into these segments can allow your brand to send relevant and valuable messages that your recipients will be more likely to read and engage with.

Learn more about audience segmentation:

- The Essential Guide to Email Segmentation
- Email List Segmentation Strategy: Ask!

Send Personalized Emails

Personalization takes many forms. It might look like using a recipient's name in an email subject line, suggesting new products based off of their past purchase history, or sending them content based on their demographic information, like age or gender. However you choose to do it, personalizing your messages can boost your open rates and drive deeper customer engagement.

Looking to get started with personalization? Twilio Segment unifies your customer's touch points across all platforms and channels, giving you a full picture of the customer journey so you can send the right message to the right customer at the right time.

However you choose to personalize your messages, we have just a quick word of caution. You don't want your content to come off as invasive, so stick with information your customer either voluntarily shared with you or that you've collected from their past website browsing sessions.

Additional resources and testing tips:

- Personalized Email Marketing: Tips and Examples
- Send personalized emails and notifications in real time
- Twilio Segment's The State of Personalization Report



Ask The Expert:

Jessica Hunt, Sr. Deliverability Consultant

With over 11+ years of experience working in email deliverability and customer service, Jessica has a proven track record of helping businesses with email compliance, marketing, content creation, and operational excellence.

"Personalizing your email is key! With as much competition as there is in the inbox, the more you're able to personalize your email, the better chance of it being opened. With 57% of global respondents saying personalization would influence whether they find an email memorable, the more you can tailor your emails to your recipients–be it by adding their name or including topics related to their interests and/or past purchases– the closer you'll be to increasing your recipients' engagement with your emails and your brand."

Personalize Emails with Twilio Segment

Use the power of a cdp to collect, consolidate, and utilize engagement data to create better customer experiences with segment.



Remove Unengaged Recipients

Sending emails to recipients who no longer engage with your messages can damage your sender reputation for several reasons:

- Addresses that don't open or click on your messages are more likely to mark your messages as spam
- Unengaged addresses can become spam traps
- Unengaged recipients can lower your open rates, which make your messages and traffic look unwanted

That's why it's important to periodically "scrub" your subscriber lists, or remove inactive, bounced, and other non-engaging email addresses. You might always want to consider implementing an email sunset policy, which reduces the frequency that an email address receives campaigns or suppresses it entirely based on engagement, or lack thereof.

Instead of just outright removing an unengaged email address from your list, some sunset policies can include a reengagement campaign, which gives subscribers one last chance to keep receiving your emails. This way you can keep valuable subscribers that still want to hear from your brand on your list, while deleting users who haven't engaged in some time.

> **"Your sunsetting policy can be as basic or as granular as you need it to be; the most important thing is that you have one and that you are using it."**
>
> **Jessica Hunt**
> **Senior Deliverability Consultant, Twilio SendGrid**



Email sunset policies can be particularly important for B2B businesses, since employees often leave companies (and work email addresses). Sunsetting can help ensure you're not sending messages to corporate email addresses that no longer exist or are no longer in use, allowing you to clean up your lists and maintain a strong sender reputation.

Additional resources:

Proactively Remove Unengaged Email Addresses



Ask The Expert:

Emily Thrasher,
Sr. Deliverability Consultant

Emily is a Sr. Email Delivery Consultant for Twilio SendGrid. For the last 6 years, she's helped guide clients through their email program journeys.

> **"I probably sound like a broken record on a lot of client calls, but a common theme among clients with deliverability issues is their sunsetting policy... or lack thereof. I've seen companies sending their email campaigns to people who haven't engaged in an email in YEARS!**
>
> **Not only is this bad practice, but it's also costing them money to store those old, unengaged email addresses. Get rid of them. If you have recipients who haven't opened an email of yours in the last 30 days, it's time to start saying goodbye. Slow down how often you send to them and remove them if they still haven't opened anything in 3 months."**

Make It Easy to Unsubscribe

Although it may sound counterintuitive, making your unsubscribe process as simple and clear as possible improves the recipient experience and can benefit your sender reputation. If a recipient no longer wants or needs to receive your emails and there isn't an easy way to unsubscribe, they're very likely to report your content as spam or junk. Remember, someone who opts out can always opt back in later, but a spam complaint can be detrimental to your entire campaign as well as your email deliverability moving forward.

In addition to putting a clear "unsubscribe" link in your email footer, your business can also use list-unsubscribe. List-unsubscribe is an optional email header that allows recipients to remove themselves from a mailing list without clicking through an unsubscribe link or reporting a sender as spam or junk. If you implement list-unsubscribe, the major inbox providers will add unsubscribe links into the headers of your emails, which makes it easier for recipients to unsubscribe.

Additional resources:

- Unsubscribe Email Best Practices and Email List Management
- The Art of the Email Unsubscribe

Best Practice Tip:

Allow Your Recipients to "Down Subscribe"
Use your email preference center to your advantage by allowing recipients to "down subscribe," AKA allowing recipients to remove themselves from certain mailing lists or campaigns rather than removing themselves completely by unsubscribing.

The Continued *Focus* on User Experience

Recipient engagement is one of the most critical signals impacting your sender reputation. Yes, infrastructure and authentication are important–however, top-notch wanted emails get engaged with, and engaging emails get delivered.

Email that customers love make it to the inbox–simple as that.

The inbox environment is evolving, and brands that evolve with it to prioritize the user experience will see more engagement, improved reputation, and greater deliverability. Here are a few things you'll need to focus on to enhance your users' inbox experiences.

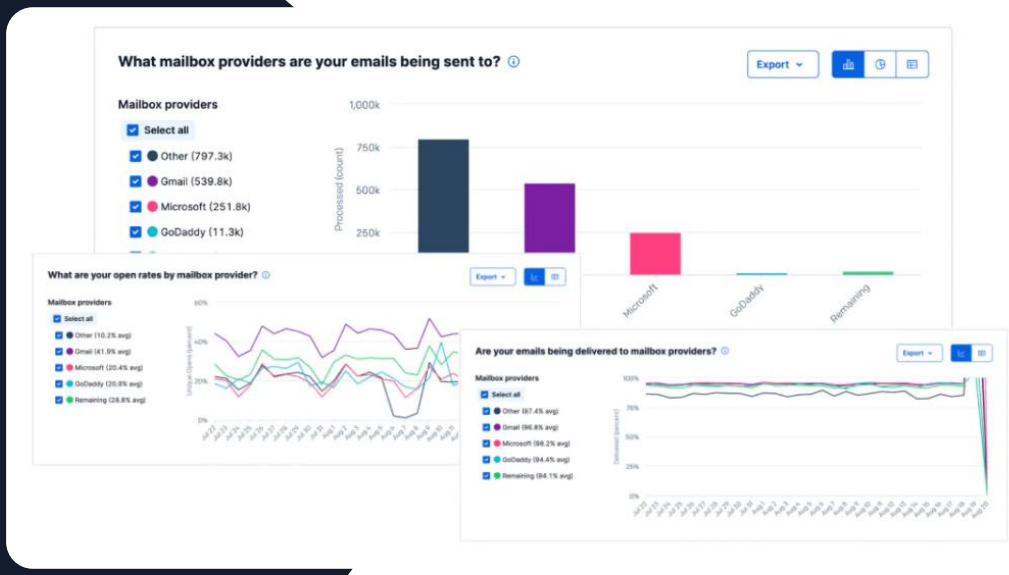


Track Your Deliverability

Twilio SendGrid's Deliverability Insights helps senders monitor key metrics from a simple, easy to use dashboard. Using Deliverability Insights, you can:

- Track overall trends in volume, open rates, spam complaint rates, and other key metrics
- Segment these metrics by mailbox provider
- See dynamic tool tips designed to help you improve your email program
- Determine why your emails are not landing in the inbox with 7 bounce and block classifications

Deliverability Insights gives you all the tools you need to understand the key issues facing your email program and take quick action to improve them. If your business requires more hands-on email and messaging guidance, the Twilio SendGrid Expert Services team is always available to help.



Twilio SendGrid's Deliverability Insights dashboards help senders keep tabs on what's working and what isn't with their email programs.

Monitor and improve email program health from a single dashboard.

See first-hand how Twilio SendGrid's deliverability insights can help you land in customer inboxes.



Apple and Google prefetching

In 2021, Apple's launch of Mail Privacy Protection (MPP) and a renewed interest in Google prefetching opens ramped up the anonymization of email open data.

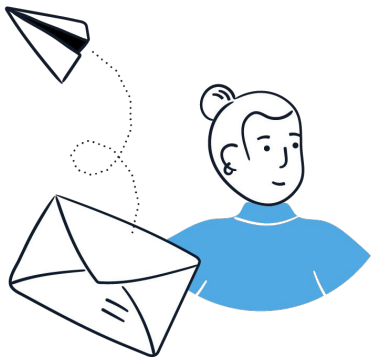
What do these "anonymized" opens mean for senders? Your company may experience inflated open rates.

If you use open rate as a key performance indicator (KPI), you could be getting an inaccurate view of how your recipients are engaging with your messages. To help, Twilio SendGrid's Apple Open Indicator empowers our customers to identify MPP-related opens. SendGrid customers can also use our Event Webhook to search for a user agent string and identify Gmail prefetch opens (read this article to learn how).

Even with these identifiers, we still encourage all senders to rely less on open data and instead lean more heavily on alternative engagement metrics–like clicks, conversions, and app activity–to better understand which messages are actually engaging recipients.

Additional resources:

- Apple Mail Privacy Protection in 2022: Guide for Email Senders
- Apple's Mail Privacy Protection: How Email Senders Can Adapt
- What Is the Impact of Google Prefetching Opens?



Find Out What Your Users Want with A/B Testing

Thoughtful A/B testing ensures you're listening to your recipients and continuously improving your email campaigns. A/B testing helps you dial-in your user preferences by changing one element at a time to find what your customers like best.

Do more of your users engage with a text-only email? Drop the images from your campaigns and deliver on the copy.

Do your customers open more of your messages on Tuesday or Friday? Strategize your campaigns to send when your users are most likely to engage.

A/B testing isn't used just to boost open rates or click-through rates–it's used to identify exactly what your users want so you can craft better email campaigns.

Keep It Simple

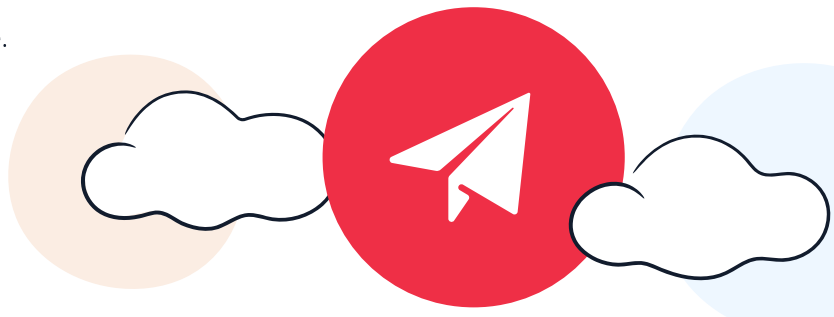
Get the small things right. The logo in your email should be hyperlinked to your website and every message should have a clear, direct purpose.

One way to simplify your messages is to identify your email's call-to-action (CTA). This is the purpose of your email. Why are you sending it? What do you want your recipients to do after reading it?

Do you want them to answer a survey, make a purchase, or read an article? Make that clear with a singular, obvious CTA that tells your recipients exactly what to do:

- Buy
- Learn
- Contact Us
- Review
- Verify

Your recipients should know the purpose of every email–make it clear and obvious.



Understanding Your Sending Metrics

Every email you send generates a wealth of information that your business needs to collect and analyze in order to build a healthy and successful email program. From email processing data to customer engagement metrics, these powerful indicators give you insight into what parts of your email program are working and what need some extra attention.

Ask The Expert:



Jose Sucre, Deliverability Consultant

A native of Venezuela, Jose has been working in the email deliverability space for 4+ years in the US. Prior to working as a consultant, Jose spent half of this time working as a Compliance and Deliverability Specialist helping senders reach the inbox by following best practices. Outside of work, Jose is passionate about cooking, music, and traveling.

> **"I like to look at bounces and blocks like receipts of your declined transactions. It is always important to check how much of your mail is being rejected by the ISPs. However, understanding why your messages are being rejected can help you identify any potential deliverability issues in your email program."**

For Twilio SendGrid customers, our Event Webhook registers two types of events: delivery and engagement events. Delivery events indicate the status of email delivery to the recipient, while engagement events indicate how the recipient is interacting with the email. From bounced to deferred, here are the 9 different types of sending events that Twilio SendGrid tracks:

9 Primary Events of Email

1 Processed

Twilio SendGrid has received your message and it's ready to be delivered.

2 Dropped

Some emails will be dropped (meaning not delivered) due to spam content, unsubscribe email addresses, bounced addresses, and more.

3 Deferred

Email can't always be delivered immediately. When it can't, the email is deferred (often called a soft bounce)–we'll continue trying to send your message for up to 72 hours. After that, the deferral turns into a block.

4 Bounce

If a server doesn't deliver your message, you'll see a bounce. A bounce will help you know if you have invalid or outdated email addresses.

5 Delivered

Your message has been successfully delivered to the receiving server. That doesn't mean it's landed in the inbox, though–it could have ended up in the spam folder.

6 Open

Your recipient has opened your email message.

7 Click

Your recipient has clicked on a link within the message.

8 Spam Report

Your recipient has marked the email as spam.

9 Unsubscribe:

Your recipient has clicked the link to unsubscribe from your mailings.

While some of these events are more informational and can help you refine your email program, some may require you to react and take action immediately. To that end, it's important to have a sense of what rates are normal for your business, that way if you see a positive or negative spike in one or more of these events, you can take swift action to correct it and ensure your deliverability and sender reputation aren't impacted.

The Complete Email Metrics Guide (with Formulas)

Find the right metrics for your campaign goals and get the full picture of your email performance today.



Ask The Expert:



Dale Langley, Delivery and Operations Engineer

Dale has over 15 years of experience in the digital marketing industry, building teams that focus obsessively on improving their customer's email marketing strategy and deliverability.

> **"To a great extent, email deliverability is self-fulfilling. If you send content that your audience wants to receive and that they find interesting, the algorithms will learn that your email should be delivered to the inbox.**
>
> **If you send email that wasn't asked for and doesn't deliver value, your recipients will act in a passive, or negative way and the algorithms that control filtering will learn to deliver your email to the junk folder. Of course, there are other influencing factors that contribute to email success, but ultimately, if you send an email that people love, it will be successful."**

Mobile and Desktop Responsive

Now more than ever, your emails must be accessible on any device–especially when many consumers read emails almost exclusively on their phones. This means that all of your content must be responsive and adapt to different device displays. That being said, recipients do still switch between computers and devices when checking their emails, with some users reporting a preference to click through links on a computer.

So, how do you handle these needs for adaptation?

We recommend responsive templates (our Free Email Template Gallery has some great options). Responsive templates allow you to create emails that adapt to the unique needs of devices while maintaining great visual quality and consistency, no matter where an email is viewed.



Dark Mode

Dark Mode is a color scheme that uses light-colored text and icons on top of a dark background. The darker design decreases the light emitted by screens while maintaining the contrasting colors necessary for readability. This saves the device's energy, relieves eye strain, and can reduce screen glare.

Dark Mode has made its way into just about every app, browser, and device–and the inbox is no exception. Some surveys estimate iOS adoption rates to be between 55-70%, so with so many users opting to use Dark Mode, it's critical your emails still look great in this environment.

Best Practice Tip:

Optimize for Dark Mode
Each inbox provider renders your HTML emails differently, but there are a couple of general best practices you can follow to make sure your email looks great regardless of the color scheme. First, enable Dark Mode in your email's HTML and CSS. Second, optimize your transparent logos and images to look good with both light and dark color schemes–this is especially important if your PNG contains black text.



Accessibility

One billion people, or 15% of the world's population, have some form of disability, ranging from hearing and vision impairment to loss of motor control. Certain disabilities may make it harder for your recipients to engage with your digital content. As a sender, ensuring your emails are accessible to everyone can make all the different to your recipients.

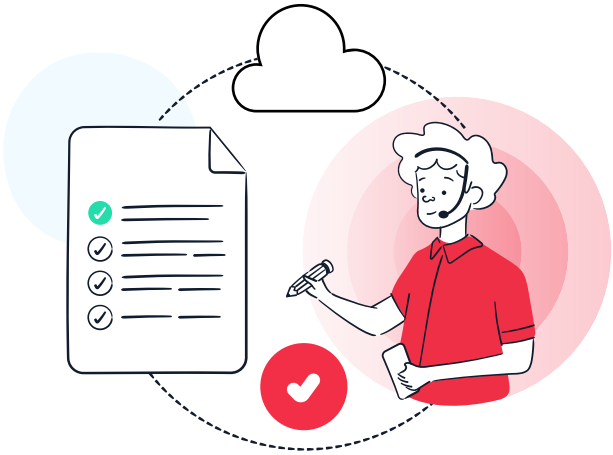
Mozilla's MDN defines accessibility as "the practice of making your websites usable by as many people as possible." That doesn't just limit catering to disabilities, either–that includes those with slower internet speeds, lower-quality devices, and other barriers. Better accessibility means better engagement, and better engagement leads to fewer unsubscribes and spam complaints.

What're some ways to ensure your email designs are accessible to all of your recipients? Leverage color thoughtfully, use sufficient contrast, and add alt-text on all images so every one of your recipients can easily read and interact with your email content.

While there's no single paramount law to make your digital content accessible, the World Wide Web Consortium (W3C) sets forth modern-day best practices in their Web Content Accessibility Guidelines, or WCAG guide. It's important to note, however, that some industries must follow certain guidelines to make content accessible by all (finance, government, etc.), so make sure you review The Americans with Disabilities Act (ADA) to ensure your digital content is compliant.

Deliver on Promises

Another way to improve engagement and reduce spam complaints is to deliver on your email promises. While technically legal, certain gray-hat marketing practices (like gimmicky subject lines) can spoil your recipient's inbox experience. Here are a few best practices to help you deliver on your inbox promises:



- **Ensure your subject line and email content match:** While clever, cutesy subject lines might get more clicks, try to avoid clickbait. Your subject line should be relevant to the content in your email. If not, recipients can quickly send you to the spam folder.
- **Send what you said you'd send:** When a subscriber enters their email address to signup for your blog's weekly digest, that doesn't automatically give you permission to start blasting them with product announcements and sales. Only send the email you promised to send–nothing more, nothing less.
- **Honor your unsubscribes:** When a recipient unsubscribes from your emails, remove them from your mailing list as quickly as possible. Failing to do so is a surefire way to earn yourself a spam complaint.

Communications Fatigue

Recipients know exactly what they want from senders and will unsubscribe or report emails as spam if they are feeling communications fatigue.

We define communications fatigue (or more specifically, email fatigue) as the feeling recipients get when they receive more emails than they want from a sender. This could happen for a variety of reasons: the recipient could have a change in interest, there could be a lack of access to an email preference center or even a change in your sending frequency.

Based on our research, recipients are much more likely to forgive their favorite senders for sending multiple or repetitive emails, simply because they like their content. So long as they are interested in your product, service, or content, they may be interested in higher rates of communication.

As a sender, you'll need to identify these high-volume recipients and determine how frequently they want to receive emails (once a day, once a week, etc.).

Often, however, these high-volume recipients are not the norm. For many recipients, receiving plenty of emails over a short period of time can be a turnoff and lead to deletion or unsubscribes.

You'll also need to keep in mind your business's collective communications with each recipient. While you may only send a recipient a few marketing emails a week, keep in mind they may also be receiving SMS, display ads, LinkedIn InMails, and more from your brand. Too much contact on too many channels begins to feel like an invasion of privacy and a bit spammy–so make sure you approach your email with a holistic view.



Infrastructure and *Authentication*



Infrastructure often refers to the IP addresses and servers you're using to send email, while authentication refers to the validation techniques you use to show that email coming from you is in fact yours. Your email infrastructure is what goes on behind the scenes to ensure your messages get to your recipient's inbox.

Properly configuring your infrastructure can make or break your email deliverability. We'll walk you through the basics below to get you up and running.

Setting Up Your Email Infrastructure With Twilio SendGrid

Check out our step-by-step guide to learn the process of setting up your infrastructure and authenticating your email.

Dedicated IP Address

All email is delivered over an IP address. Inbox providers use your IP address to judge your sending reputation when determining whether or not to deliver your email to the recipient's inbox.

If you're a high-volume sender who wants to make sure you're in complete control of your sending reputation, you're going to need a dedicated IP address (or even a few addresses if you're segmenting your email streams by type of email). Here's why:

- If you're sharing an IP address with other senders, their poor sending practices could impact your deliverability.
- With your own dedicated IP address, you're in full control of your sending reputation and the impact it makes on your deliverability.
- If you send over 100k emails per month, a consistent sending pattern could help you build a solid reputation on a dedicated IP address. You'll also be able to take advantage of other services for improved email deliverability.



Sharing an IP address can be a great solution, especially if you're a low volume sender sending less than 100k emails per month. In fact, if you're fortunate to end up with a cohort of senders following email best practices, you could reap the rewards of a reputable IP address. However, many of Twilio SendGrid's lower volume senders choose to upgrade their accounts to Pro so that they can claim the benefits of a dedicated IP.

IP Warmup

If you're sending email over a new IP address, you'll need to properly warm up your IP to ensure inbox providers deliver your emails.

Warm up an IP address by sending a low volume of email on your new dedicated IP and then slowly increasing the number of messages over time. This provides internet service providers (ISPs) time to recognize, identify, and evaluate your sending practices to make sure you're a legitimate sender.

Once you've hit your predicted usual sending volumes and your IP is warmed up, you can send like normal. At this point, ISPs should have a clear understanding of how much email you'll be sending so they can better identify unusual or dangerous behaviors.



Email Stream IP Segmentation

Sharing a root domain across email streams (transactional vs. marketing) will combine reputations into each other. This can lead to deliverability issues if one of your streams is receiving more spam complaints or less engagement than the other. To avoid potentially damaging your transactional email delivery, segment your different email streams onto multiple IP addresses and subdomains.

For example, you may want to send all your transactional emails (password resets, confirmations, notifications, etc.) on one IP address and all your marketing emails (newsletters, promotions, product announcements) on another IP address. This way, if your marketing emails are flagged as spam, you won't encounter deliverability issues on your essential transactional mail.

The most basic separation is at the level of marketing and transactional messages. These mail streams often have very different reputations and must comply with CAN-SPAM differently. For companies with multiple brands, it may be wise to separate the traffic by IP for each brand, and then further separate the marketing and transactional mail streams under each brand to provide granular reporting and reputation management.

Best Practice Tip:

Use a Different IP Address for Win-Back Campaigns
According to postmasters we've spoken with, win-back (or reactivation) campaigns often have the poorest deliverability and highest spam complaints of any mailstream. Consider an ongoing drip campaign of reactivation emails (just a few hundred at a time) instead of a large one-time reactivation campaign to keep the volume of complaints low. You might also consider using a different IP so that you don't potentially damage your primary IP/domain.

SPF Record Creation

SPF stands for sender policy framework and is an email authentication method that identifies the mail servers that are approved to send email from a specific domain. ISPs use this validation protocol to determine when spammers and phishers are trying to impersonate your brand to send malicious emails from your domain.

DKIM Email Signature

DKIM stands for DomainKeys Identified Mail and allows you to publish a key that ISPs use to verify that the email message didn't change in transit and the sender can take ownership of the content. DKIM defends against malicious modification of messages in transit, and it carries a lot of reputation weight with inbox providers.

DMARC Record Publishing

Domain-based Message Authentication, Reporting & Conformance (DMARC) record is a protocol that builds on SPF and DKIM to protect against email spoofing. It allows you to specify how ISPs should handle emails that fail SPF or DKIM checks. Implementing DMARC enhances domain protection, helps prevent phishing attacks, and can qualify you for BIMI (Brand Indicators for Message Identification).

With almost 10 years in the email industry, Beth is an email deliverability problem-solver and best practices advocate.

Ask The Expert:



Beth Kittle, Senior Deliverability Consultant

"I am always surprised at how many good senders are still not taking advantage of DMARC. DMARC offers domain protection, keeps your customers safe from phishing attacks, and can eventually qualify you for BIMI. But there is also tremendous value in the DMARC reports alone, even if you don't believe your domain is under threat. Many organizations don't have a good understanding of their email infrastructure or even where their emails are being sent from. Digesting and monitoring DMARC reports is vital to building solid infrastructure and maintaining trust in your brand."

DMARC policies can be set to different levels of enforcement:

- **p=none:** This is a monitoring-only mode where no actions are taken on emails that fail SPF or DKIM checks. Use this setting to gather data and understand how your emails are being processed.
- **p=quarantine:** Emails that fail SPF or DKIM checks are sent to the recipient's spam folder.
- **p=reject:** Emails that fail SPF or DKIM checks are rejected and not delivered to the recipient's inbox at all.

Recommendation: Start with **p=none** to monitor your email traffic and gather data. Once you have a clear understanding and have made any necessary adjustments to your authentication practices, gradually move to **p=quarantine** and eventually to **p=reject**. This phased approach helps ensure that your legitimate emails are not inadvertently affected while strengthening your domain's protection against malicious activity.

Steps to Implement DMARC:

1. Go to SendGrid's Sender Authentication and copy the host and value txt record with DMARC.
2. Go to your DNS hosting provider and create a record.
3. Select TXT DNS record type.
4. Add the host value you've copied from sender authentication (_DMARC followed by your domain).
5. Paste the DMARC record (value column) copied from the sender authentication page. This should look like v=DMARC1; p=none; You can also include an rua tag such as rua=mailto:dmarc_agg@vali.email to define where DMARC reports should be sent.
6. Hit the save/submit button and verify your DMARC record has been added correctly to your DNS.



Each DMARC record needs to define a policy, which can be one of three options: none, quarantine, or reject. Although Gmail's requirement for DMARC is to set it at p=none, this is the minimum. When p=none the receiving mailbox provider is instructed to take no action on an email that fails an SPF/DKIM check. If you are new to DMARC you can start with this policy before moving to quarantine or reject.

The most secure setting is what's called DMARC at enforcement, p=reject or p=quarantine. This requires analyzing DMARC reports to ensure that an enforcement record incorporates all third parties sending on behalf of your domain. Publishing the record incorrectly could cause your mail from these providers not to be delivered. Work with your technical personnel to ensure that your DMARC is properly formatted, affords you the greatest level of protection, and reports are actively monitored.

Brand Indicators for Message Identification (BIMI)

BIMI stands for Brand Indicators for Message Identification and is a standard that attaches your brand's logo to your authenticated email messages. With this simple, visual verification, recipients can recognize and trust the messages you send.

BIMI displays your brand's logo next to your emails in the inbox, increasing consumer trust in a message and helping build brand awareness. And although BIMI has been a hot topic over the last couple of years, now Gmail has announced it'll roll out general support for the new industry standard.

Here's what you need to do now to take advantage of this. Additionally, as of IOS 16, Apple MPP now supports BIMI as well. With Apple, Gmail, Yahoo, and AOL all supporting BIMI, there has never been a better time to implement it!

A Records and rDNS

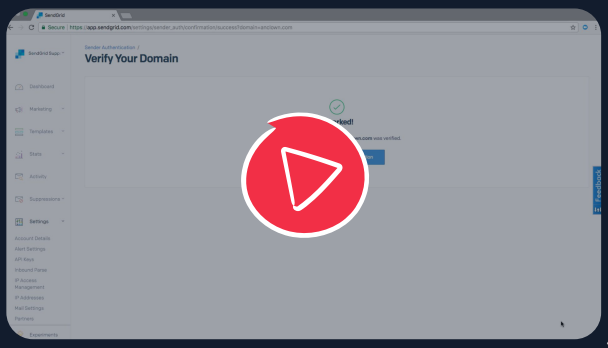
A records point your domain to an IP address, while reverse domain name system (or rDNS) links an IP to your domain. Having these pieces in place is an important step in building trust between you and inbox providers.



Domain Authentication

Your sending domain needs to be able to receive email, and it must have a valid mail exchanger (MX) record. If not, some inbox providers will block your email.

Watch the video below to learn how to authenticate your domain with Twilio SendGrid:



Getting Started with Domain Authentication

Transport Layer Security

Transport Layer Security, or TLS, encrypts email while it's being delivered. This prevents someone from reading the mail traffic as it moves between the sending and receiving servers. TLS has become a widely adopted security protocol to protect sensitive information and communications over email channels.

Feedback Loops

Spam feedback loops (FBLs) are offered by most mailbox providers to let you know when recipients mark messages as spam. Immediately remove the addresses of spam reporters from your active email lists to maintain your sending reputation and the respect of your audience.

"postmaster" and "abuse" Mailboxes

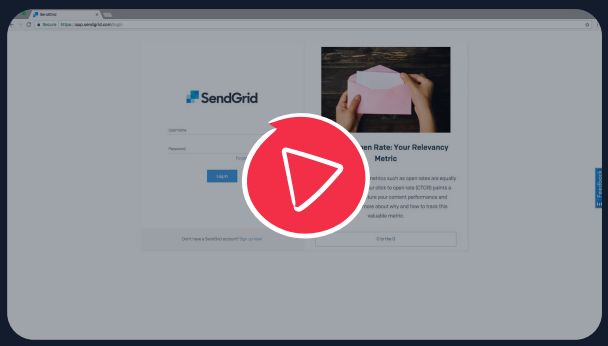
To access FBLs, many inbox providers require that you have abuse@ and postmaster@ email addresses. Monitor these mailboxes for complaints from inbox providers that don't have FBLs so you can address any reports of unsolicited email.



Two-Factor Authentication

Two-factor authentication, or 2FA, is another layer of security protection you can add to your email account. If malicious users get access to your account, their fraudulent activity will very likely damage your sending reputation, even if you are able to recover from the hack.

Watch the video below to learn how to configure 2FA on your Twilio SendGrid account:



Resetting your Password and Setting up Two-Factor Authentication

Email authentication doesn't have to be rocket science. Our Delivery Consultants are authentication connoisseurs and can guide you through the process.

Get help with your infrastructure and authentication

Privacy & Compliance in a World of *Engagement*

From Canadian Anti-Spam Legislation to the General Data Protection Regulation (GDPR), global privacy trends are consistently moving to provide recipients with more and more control over how their data is used and the types of communication they prefer to receive.

In a global marketplace, most senders should be compliant with the strictest legislation that impacts their sending. For example, if you're sending any email to recipients in the European Union, you need to make sure that all of your practices are compliant with the GDPR.

Compliance, however, isn't only about doing what's required. In fact, compliance with these new privacy laws will almost always help senders receive better results for their marketing efforts. When you set clear expectations about how a recipient's data will be used, and the types of communications they should expect from a sender at the point of address collection, those recipients tend to be much more engaged with the email they receive. Engaged recipients (who aren't reporting messages as spam) are who inbox providers look to for guidance when deciding which messages to deliver to the inbox and which ones to block at the gateway.

Think of user permissions and legal compliance requirements as an opportunity. Frame your approach to compliance with the recipient's experience, and you may have more success getting your emails into the inbox.



CAN-SPAM

In 2003, the United States Congress passed the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, or CAN-SPAM Act. CAN-SPAM slowed the influx of unsolicited emails the world saw in the early 2000s by creating restrictions on the way commercial emails are sent and giving recipients privacy and protection. CAN-SPAM remains in effect today.

The FTC defines commercial email as any "electronic mail message the… purpose of which is the commercial advertisement or promotion of a… product or service." If your business sends commercial emails of any kind, CAN-SPAM and its legal requirements of commercial entities should be on your radar.

Under the CAN-SPAM Act of 2003, all businesses using email for commercial purposes must comply with these 7 elements:

1. Do not use misleading or false information in email headers
2. Do not use deceptive language in email subjects
3. Clearly and conspicuously identify advertising messaging as such
4. Inform recipients of your business's location
5. Tell recipients how to opt-out of future communications
6. Respect opt-out requests and handle them quickly
7. Be cognizant of what third parties or others do on your business's behalf

The biggest things to remember with CAN-SPAM are avoiding deception, clearly communicating the purpose of your email(s), and ensuring that recipients' preferences are respected. More likely than not, you are already compliant with these elements. Remember, you must be compliant with the CAN-SPAM Act at all times if you send commercial emails.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation is one of the most hot-button topics related to email in the last decade. If your business works within the European Union or with its citizens, the GDPR should be top of mind when developing your international email strategy.

The GDPR updated and replaced the EU Data Protection Directive (1995) and applies to the entirety of the European Union as the de facto standard defining how companies can use customer data.

GDPR outlines 7 principles relating to the processing of personal data:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability



Under this law, EU citizens have more say over the ways organizations use their data. For those doing business in the United Kingdom, the GDPR is still in effect despite the UK's exit from the EU.

The GDPR applies to all EU businesses, regardless of size or industry, that handle personal data, as well as any organization doing business in the EU where EU citizens' data is involved.

GDPR compliance dominated conversations in the email world when it was put into effect. The importance of user privacy and compliance with international legislation are part of a larger, ongoing conversation that continues to evolve and adapt.

California Consumer Privacy Act



The California Consumer Privacy Act (CCPA) became enforceable by the California Attorney General on July 1, 2020. The CCPA grants consumers considerably more control over their data and how it is used, but only applies to businesses within specific categories.

Under the CCPA, consumers have the right to:

1. **Know** "what personal information is collected, used, shared or sold" by organizations they interact with

2. **Delete** "personal information held by businesses" which includes any of the business's service providers

3. **Opt-out** of the sale of their information
    a. Consumers have the right to "direct a business that sells personal information to stop selling that information"
    b. There are specific protections for minors as well:
        i. Those under age 16 "must provide opt-in consent"
        ii. Those under age 13 must have a "parent or guardian consent" on their behalf

4. **Non-discrimination** when exercising CCPA privacy rights, including access to "price or service"

Knowing this, here are the characteristics of businesses affected by the CCPA. Only one of the following needs to apply for your business to be affected.

Under the CCPA, businesses must comply if:

1. The business's gross annual revenue exceeds $25 million
2. The business "buys, receives, or sells the personal information of 50,000 or more consumers, households, or devices"
3. 50 percent or more of the business's annual revenue comes from the sale of personal consumer information

Under new CCPA regulations, affected businesses must notify affected parties about data collection before or at the time of collection. Businesses must continue to comply with CAN-SPAM opt-out expectations in a timely and respectful manner, and also need to include a "Do Not Sell My Info" option to comply with the CCPA. Additionally, businesses must provide a response to opt-out requests or privacy setting changes, which can be fulfilled with a confirmation email. For more information about specific regulations and obligations, check out the California Attorney General's Fact Sheet about CCPA.

Please note that compliance with CAN-SPAM and the GDPR do not ensure compliance with the CCPA. There are subtleties unique to each law that do not always overlap, so be sure to know how each law affects your strategy.

Apple Mail Privacy Protection (MPP)

Apple Mail Privacy Protection (MPP), launched in September 2021, is part of Apple's broader initiative to give users more control over their data. This feature has significant implications for email senders, particularly in how they track and understand recipient engagement.

MPP anonymizes open tracking by prefetching email content before the recipient actually opens the email. This means that open rates reported for MPP-enabled recipients may be inflated or misleading. As a result, email marketers can no longer rely solely on open rates to gauge engagement accurately. Instead, they need to focus on alternative metrics such as click tracking, conversion rates, and other forms of engagement.

This highlights an important distinction: while MPP does change how open rates are reported, it does not mean that opens from MPP-enabled recipients are invalid or should be ignored. Suppressing recipients based on MPP opens can lead to the unnecessary loss of engaged subscribers.

Twilio SendGrid developed an entire guide on Apple MPP to help senders understand the impact and complications around Apple's new privacy measure.

Country-Specific Email Regulations

Compliance with one regulation does not ensure compliance with another. While some new privacy regulations share similar protections for recipients, their individual legal obligations do not necessarily overlap. Please be sure to do your research about laws in each country you plan to send to and know what your obligations are to remain compliant.



SMS: A *Complementary* Channel of Communication



What Is SMS?

SMS stands for "short messaging service," also known as a text message. SMS is a simple, but powerful, communication tool businesses and organizations can use to send promotional or informational messages via text.

Why SMS?

SMS messages have unmatched open rates, giving businesses the opportunity to communicate with their customers in a quick, reliable way. In fact, an estimated 95 percent of text messages are read by recipients.

Like email, SMS messages are delivered in seconds. Text messages can initiate two-way conversations and are easy to track. By using SMS in addition to email, you can provide your customers with an integrated and seamless communication experience. Plus, you're giving them the option to connect and communicate on the channels they prefer.

Using Email and SMS to Engage Your Customers

Learn how sms can complement your existing email program and help you delight customers on their preferred channel.

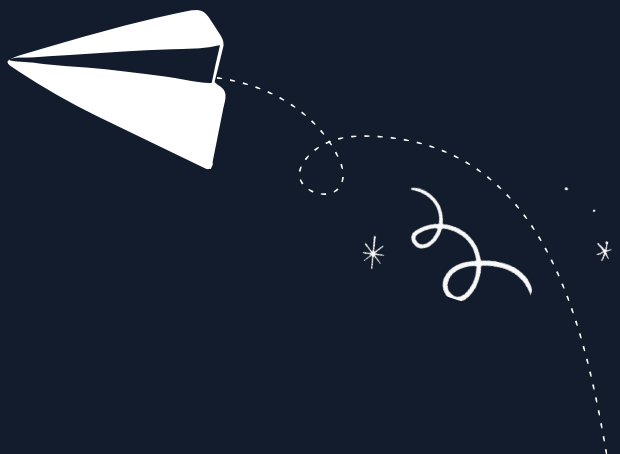
SMS Deliverability

Over 5.2 billion people have access to SMS, including many people who lack a smartphone or broadband internet. While SMS is the most widely used application in the world, businesses today face challenges with implementing and scaling their SMS delivery programs. SMS deliverability measures the percentage of outgoing SMS messages that are received at their intended destination. SMS deliverability is critical for businesses that want to reach their audience through relevant, personalized, and timely messaging.

Whether you send a text message from a mobile device or an SMS API, there is a percentage of SMS messages that will never be delivered. As opposed to thumbing out a text on a phone, SMS messages sent programmatically through an SMS Gateway have an advantage–application logic can verify delivery.

There are many places where SMS delivery might fail, especially as messages move through the interfaces between pieces of infrastructure. Common causes of message delivery failure include:

- Invalid phone numbers
- End-device level errors (like a handset being turned off)
- Problems with network connectivity



Other deliverability issues are deliberate, and messages reported by users may be blocked by carrier partners.

It's important to comply with state or local regulations and wireless carriers' messaging policies to ensure SMS deliverability for both transactional and marketing messages. Wireless carriers have filtering systems to protect mobile subscribers from unwanted spam, fraud, or abuse. Filtering can range from a simple list of prohibited terms to advanced machine learning systems that adapt based on the messages passing through them.

To reduce the risk of your messages being filtered or facing deliverability issues, businesses should follow these best practices for SMS messaging:

Get permission: Only send text messages to customers who have given you permission to do so. Request that your users opt-in to your SMS messaging via an online form or by asking them to text a particular keyword to a mobile number or shortcode, 5 or 6 digit phone numbers specifically made for mass mobile communications.

Don't be spammy: Include clear opt-out instructions, precise language, and proper capitalization and punctuation in your messaging. Message your customers with relevant, time-sensitive promotions or information.

Choose carefully: Choose an SMS provider that will provide helpful error code reporting and status callbacks so your business can diagnose any deliverability issues.

Check your list: Ensure the phone numbers on your list are correct and can receive text messages. Invalid numbers (like landlines) are the most common reason for message delivery problems, and changed (or fake) phone numbers won't reach their intended destination, decreasing your message delivery.

Use the right phone number: You can use either toll-free numbers or short codes–both support higher sending volumes and reduced filtering. Shortcodes are individually approved by wireless carriers so they won't get blocked and can send at a faster rate than regular mobile numbers. Consider using a unique, brand-friendly shortcode for mass SMS messages. However, toll-free numbers and short codes aren't available in every country.

Adhere to guidelines: Outside of simply following best practices, businesses sending SMS messages to customers should adhere to the guidelines set forth from the T-Mobile Code of Conduct and the Cellular Telecommunications and Internet Association

SMS is a universal communication channel that is meant to enhance, not replace, an existing email program. Just like email, SMS messaging should aim to keep recipients happy with valuable, relevant, and personalized information on the channels they prefer. To learn more about how you can add an SMS communication channel for your business, talk to an expert at Twilio.



Send and Receive SMS Messages Confidently with Twilio

Learn how twilio's programmable messaging api can help you reach customers on their mobile devices.

Email or SMS: Which Channel Should I Use?

SMS and email are complementary channels that can be used to create a seamless customer communication experience. You can use text messaging for short, time-sensitive communications; this means everything from appointment reminders to last-minute sale alerts. Use email to send more content and information to the place your customers are already going every day: the inbox.

Best Practice Tip:

Get Recipient Consent to Send SMS Messages
Though not yet regulated to the same extent as email, SMS sending practices have their own legal obligations. Generally, you'll need consent to send marketing or commercial communications via SMS. SMS privacy regulations beyond this vary by country, so please be sure to do your research on maintaining compliance everywhere you plan to send.

How Yelp Uses SMS to Engage Users

Using Twilio SMS, Yelp meets its user base where they're most active–on their mobile devices. Yelp customers can text their favorite restaurants to make, modify, or cancel their reservations. Businesses can easily update their customers on wait times, reservation availability, and reply to their texts straight from Yelp Reservations. Yelp empowers restaurants to build better experiences for their customers, and customers to build business for their restaurants.

Check out our other customer stories to see how other high-volume email senders are embracing Twilio SMS.





Helpful Email Deliverability Tools

We've mentioned a lot of helpful tools throughout this guide, but we won't make you read through it all again to find them all.

Below, we've listed and linked to the top email deliverability tools your brand can use:

Twilio SendGrid Email Validation API:
Improve deliverability by validating email addresses before you send.

Twilio SendGrid Deliverability Insights:
Monitor and improve your email program's health from a single dashboard.

Twilio SendGrid Email Testing:
Avoid common mistakes in your email content.

Google Postmaster Tools:
Track data on large volumes of emails sent and find data about your sending domain.

Valimail:
Improve your deliverability and protect your brand, customers, partners, and employees with automated DMARC / DKIM / SPF.

Talos IP & Domain Reputation Center:
Get real-time alerts on network and software vulnerabilities worldwide.

MXToolbox Blacklist Check:
Check to see if your mail server has been blacklisted.

Microsoft's Smart Network Data Services (SNDS):
Track your sender reputation and activity across the Microsoft network.

SenderScore.org:
Gauge your sender score just like you'd check your creditworthiness.

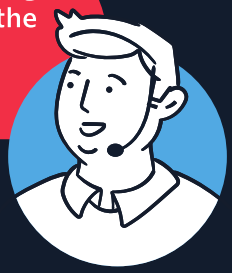
Inbox Monster:
Email reputation tool that monitors your spam trap hits, blocklistings, perform seed testing, and more.

Kickbox:
Email validation tool that helps assess the health of your opt-in email lists to reduce bounces, protect your sender reputation, and reach more high-quality subscribers.

Summary

Email delivery is an ever-evolving part of your program. As inbox providers' preferences change, new rules and regulations get implemented, and new features become available, you have to continually adapt to keep your deliverability in tip-top shape. While there's no magic bullet that's going to get all of your email to the inbox, we believe that nearly every piece of advice in this guide can be boiled down to a single principle:

Send the right message, to the right person, at the right time, with the right frequency, on the right channel.



As a sender, you should be attempting to accomplish this with the following process:

- **The right message:** Send the types of messages your recipients are expecting to receive with the content they want.
- **The right person:** Send email to people who have explicitly asked to receive it.
- **The right time:** Send messages when your recipients expect to hear from you.
- **The right frequency:** Don't send too much email to your recipients or email them too frequently.
- **The right channel:** Send on the channels appropriate to the message and audience

If you follow these guidelines and other deliverability best practices, your business should have no trouble landing in recipients' inboxes time and time again.

That said, there's no shame in asking for a little help. Twilio SendGrid's Deliverability Experts are standing by to help you reach your email goals. Create a free account now to start sending with Twilio SendGrid, or learn more about our Expert Services and how they can help you build a healthy and engaging email program.



Get Started with SendGrid

SendGrid helps you focus on your business without the cost and complexity of owning and maintaining an email infrastructure. And with a full-featured marketing email service that offers a flexible workflow, powerful list segmentation, and actionable analytics, all of your email needs are met in one simple platform.



See Plans and Pricing