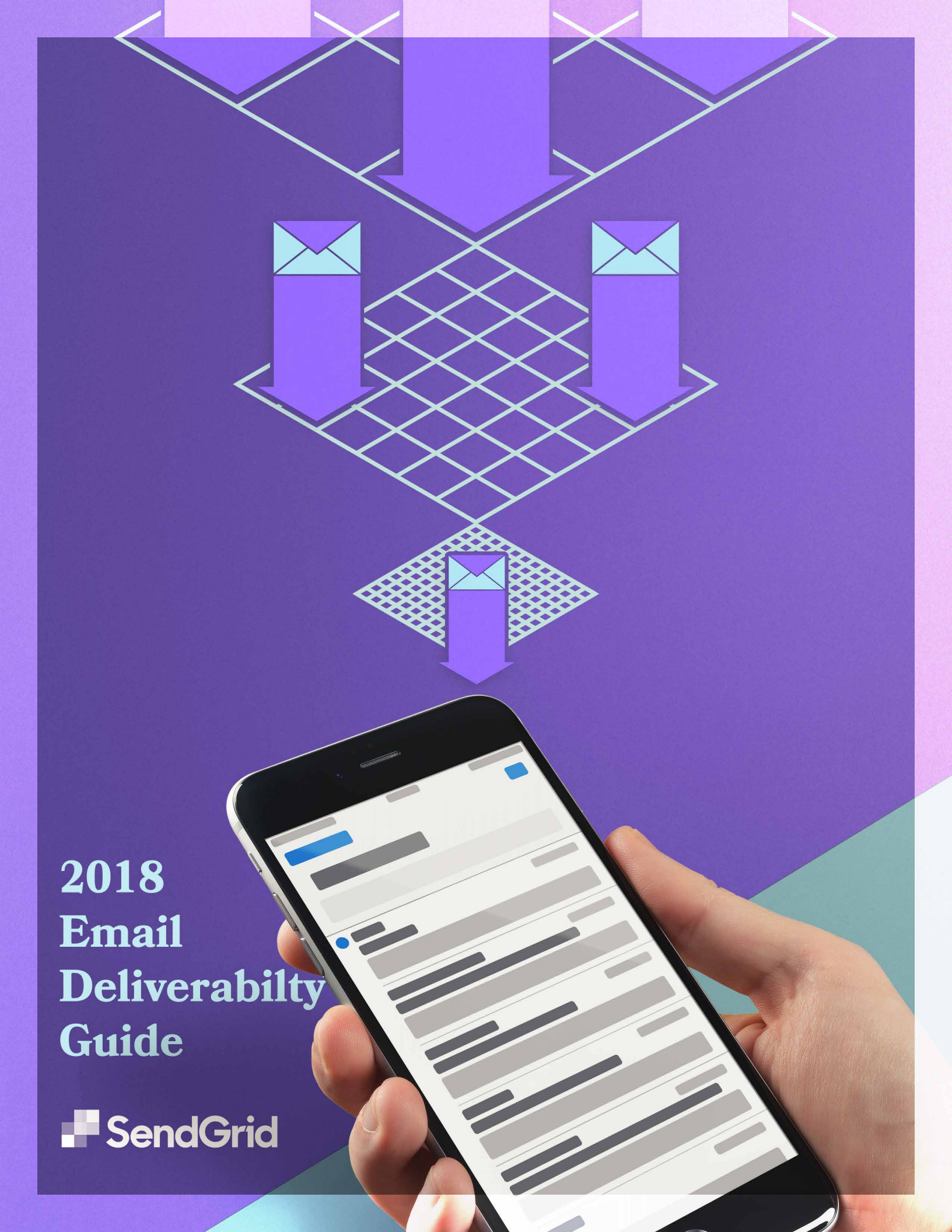
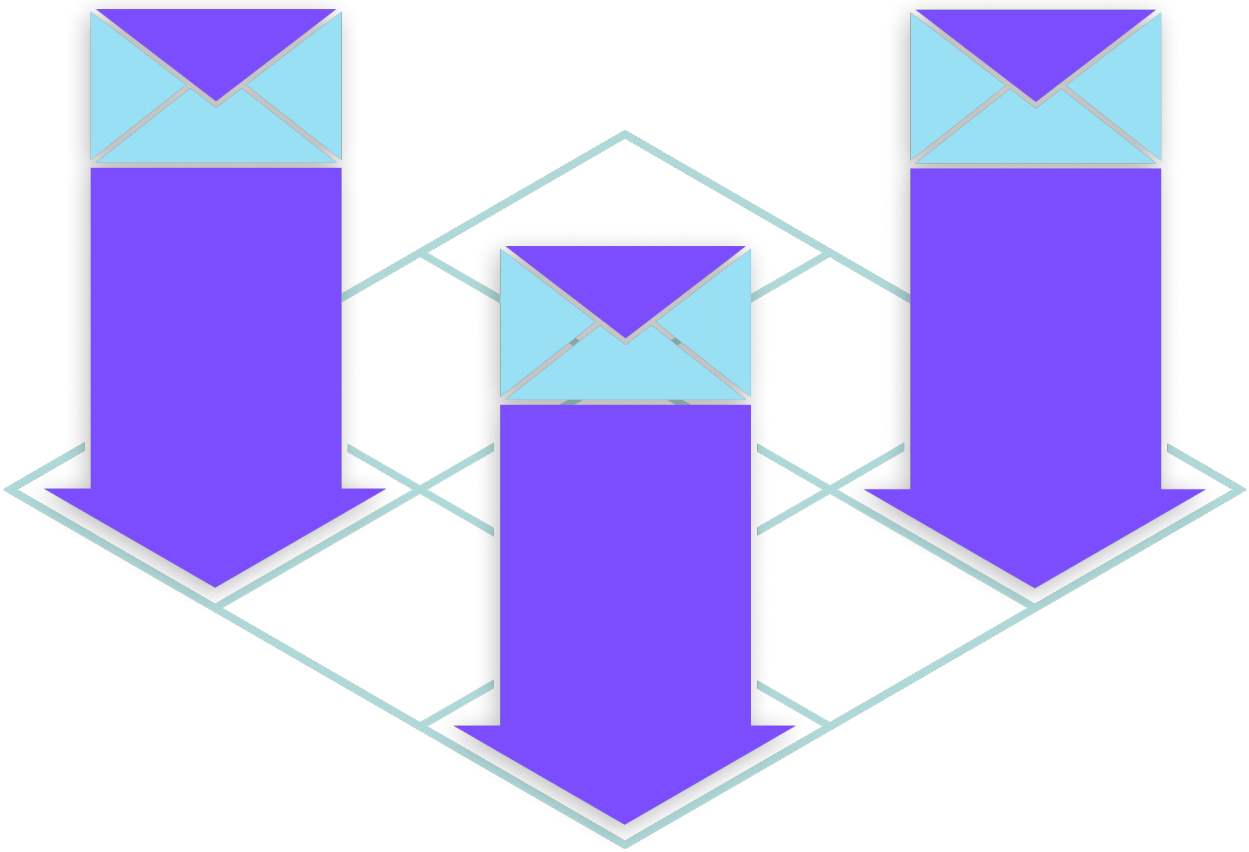


# 2018 Email Deliverabilty Guide

SendGrid

# Table of Contents





# With Updates and Contributions From

## Jacob Hansen

Jacob comes from a background in technical account management and delivery analysis for the last six years, and has been with SendGrid's Deliverability Consultant team for the last two years. He enjoys spreading knowledge to help the email community send more "wanted email" and to help senders realize their full potential. Originally from Nebraska, but living in Colorado long enough for it to feel like home, Jacob enjoys a lot of what the Denver restaurant, bar, brewery and music scenes have to offer.

## Len Shneyder

Len Shneyder is a 15-year email and digital messaging veteran and the VP of Industry Relations at SendGrid. Len serves as an evangelist and proponent of best practices and he drives thought leadership and data-driven insights on industry trends based on the massive volume of email SendGrid delivers on behalf of their customers. Len is a longtime member of M3AAWG (the Messaging, Malware, Mobile Anti-Abuse Working Group) and serves on its board in addition to Co-Chairing the Program Committee. He's also part of the MAC (Member Advisory Committee) of the EEC (Email Experience Council) where he serves as the organization's Vice Chair. The EEC is a professional trade organization focused on promoting email marketing best practices. The EEC is owned by the DMA (The Direct Marketing Association of America), a nearly 100-year-old organization where he also sits on the Ethics Committee. In addition, Len has worked closely with the ESPC (Email Sender & Provider Coalition) on issues surrounding data privacy and email deliverability.

## Seth Charles

An email nerd at heart, Seth has been working in the deliverability and marketing space for six years. He loves solving problems, helping educate SendGrid's customers, and being a part of the email community. As a sixth-generation Coloradan, he always enjoys being outside (especially if it means getting a round of golf in), and thinks John Elway should be the Emperor of Colorado.

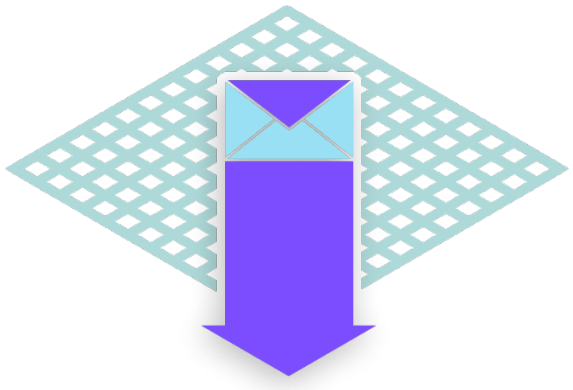
# Introduction

SendGrid's *Email Deliverability Guide* is one of our most popular resources. Not only does it provide the building blocks for improving (or implementing) deliverability best practices, but we work closely with internal email deliverability experts and industry stakeholders to ensure the information we're providing every year is accurate and up-to-date.

This year's guide is no different. Within the guide, you'll find updated suggestions, new guidance on handling authentication and subdomains, advice on IP addresses, information about GDPR, and links to new, relevant resources.

We think that in 2018, email will continue to be the most necessary, widely used identifier and communication tool on the web. Over the past year we learned that "email is essential, important, and entrenched in the lives of people today across Generation Z, Millennials and Generation X."

As companies grow and continue to be ingrained in the lives of their customers, email is the backbone of their customer communications. Can you imagine Spotify, ebay, Uber, AirBnB, or any other web application functioning without email?



**"Email is essential, important, and entrenched in the lives of people today across Generation Z, Millennials and Generation X."**

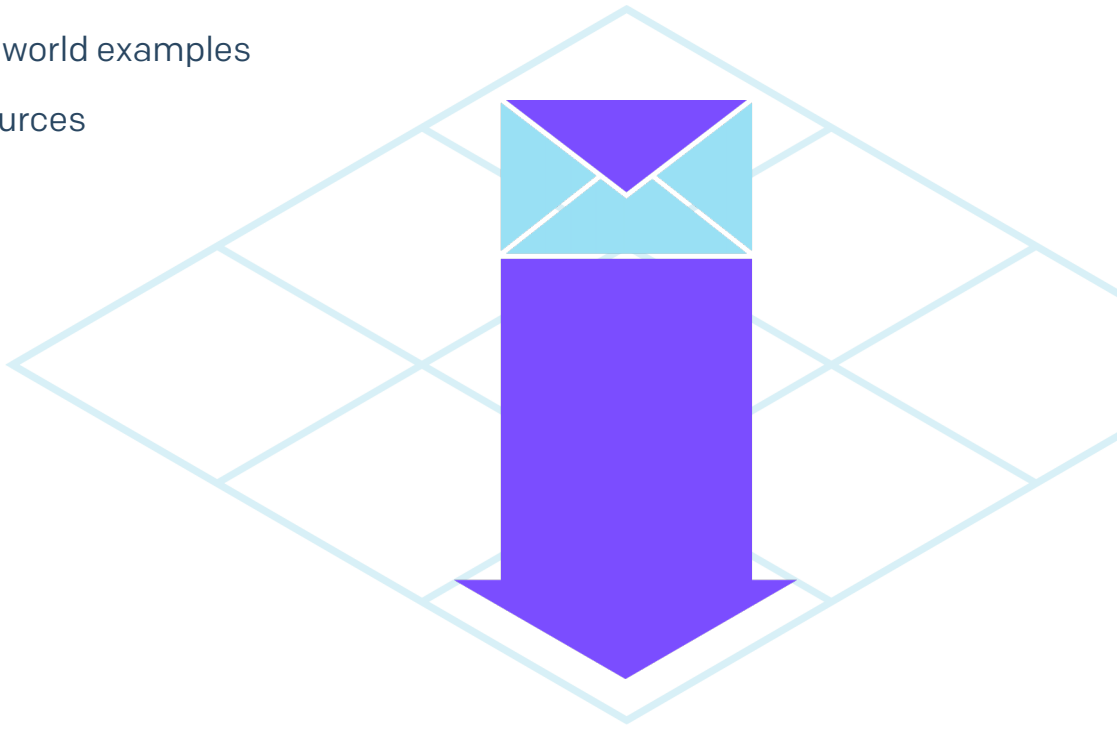
Read the rest of the study

Nearly every essential (and oftentimes non-essential) customer communication is sent via email:

- Product announcements
- Monthly newsletters
- Privacy and account updates
- Legal notifications
- Billing notifications
- Password resets
- New follower notifications

Whether you send transactional emails or marketing emails, the one thing every business can agree on is that getting to the inbox is critical—which is where email deliverability comes in. This year's *Email Deliverability Guide* includes updates on:

- GDPR
- Gmail Tabs
- Sending domain best practices
- Real-world examples
- Resources



# What Exactly *is* Email Deliverability?

Simply put: *successful email deliverability is your email arriving in the inbox of your recipient as intended*. Failed email deliverability is when your message is either routed to the junk/bulk/spam folder, or completely blocked by an Internet Service Provider (ISP).

Maintaining consistent, successful email delivery is a constant challenge facing any business that relies on email communications. Unfortunately, most companies don't think about email deliverability until they're having a major issue—like when thousands, or even millions, of emails fail to arrive.

**What's an ISP?**

While the name Internet Service Provider points to companies providing access to the Internet, like Time Warner or Comcast, in the email community, ISP more commonly refers to the email provider. The most common ISPs include Gmail, Yahoo, Outlook, and Hotmail. ISPs may also be referred to as "inbox, or mailbox, providers."

Businesses falsely assume that an email is delivered if they don't receive a bounce notification; the reality is very different. According to *Return Path's 2017 Deliverability Benchmark Report*, 80% of recipient mail is delivered to the inbox, while only 77% of mail from the United States makes it to the inbox. This means 20% of global email, and 23% of United States email doesn't make it to the inbox. Even though recipients are looking for it!

*This means 20% of global email, and 23% of United States email doesn't make it to the inbox. Even though recipients are looking for it!*

**Consider this quick calculation:**
If you have one million email subscribers, and 23% of your emails to those recipients are undelivered due to being blocked or sent to the spam or junk folder, that could be up to 230,000 people left out of your email campaign. While the impact of this loss is unique to every brand, take a minute to ask yourself: *What does losing over 80% of my list mean to me?*

To learn exactly how much money deliverability issues could be costing your business, head over to our ROI Calculator and fill out some basic email program information!

What kind of emails are we talking about? Membership confirmations, password resets, shipping notifications, and revenue-generating marketing emails and newsletters. When anticipated messages aren't received, you don't just lose revenue, you lose your customer's trust. Imagine all the time and effort put into to crafting email content, subject lines, and a great design, just for the inbox provider filter to block the message!

Getting to the inbox requires a lot of attention and effort from any sender. Not only does your sending reputation greatly impact delivery, but your email authentication and infrastructure can make or break even the best email program. This guide will arm you with all the knowledge you need to navigate the deliverability landscape, and get your messages to the inbox.

**NEW FOR 2018**

**Stop worrying about Gmail tabs!**
One of the biggest wins for marketers in 2017 was that we saw Gmail using the promotions tab as a third option outside of "spam" or "inbox." The promotions tab is not a commercial/promotional purgatory where messages are destined to remain floating in obscurity forever. Mail there is checked and interacted with. To learn more, read our blog post, *I Fought Gmail's Tabs, and The Tabs Won.*

# NEW for 2018: GDPR

What may be one of the most hot-button topics concerning email in the last decade, the General Data Protection Regulation (GDPR) is on the minds of thousands of email senders that do business with people in the European Union.

## What is it?

The GDPR updates and replaces the EU Data Protection Directive (1995) and will apply across the European Union as the de facto standard defining how companies can use customer data. EU citizens will get more say over what organizations do with their data. The new GDPR comes into force as of May 25, 2018 across all EU member states.

## Who will be affected by GDPR?

GDPR applies to all EU businesses, regardless of size or industry, that handles personal data. It also applies to any organization doing business in the EU where EU citizens' data is involved.

## What happens if I'm not GDPR compliant?

Failure to comply could mean a €20 million fine or 4% of your organization's global turnover, whichever is ***greater***.

## Where can I learn more about GDPR?

For more details, you can read the full text of the GDPR, or consult the SendGrid resources, below. Also we should note that the information we have provided here does not constitute legal advice. You should seek the advice of a lawyer in cases dealing with domestic or international laws such as the GDPR.

- General Data Protection Regulation (GDPR): What Senders Need To Know
- The GDPR is Coming: How To Prepare
- GDPR: How New Email Laws Benefit Marketers
- GDPR Legislation: What Senders Need to Know

# Reputation: It can open the inbox, or close it...

The first step to better email deliverability is to evaluate sender reputation. These days, your sender reputation is determined by a wide variety of factors, the most important of which, is how recipients are interacting with your emails. When your recipients are opening, reading, and clicking on your messages, ISPs know that your messages are wanted.

Sender reputation includes things like IP and domain reputation, and it provides ISPs with a snapshot of who you are as a sender. Senders with good reputations get delivered, and senders with poor reputations either get blocked at the gateway or, in the best case scenario, their messages land in the junk folder.

A strong sending reputation, like a great brand or personal reputation, is hard to earn, easy to lose, and built over time. The following are key factors that ISPs consider when determining your sending reputation.

> *A strong sending reputation, like a great brand or personal reputation, is hard to earn, easy to lose, and built over time.*

## Recipient Engagement

How are recipients interacting with your email? Opens, clicks, unsubscribes, and spam reports are a big part of this, but there are other types of positive and negative engagement that are harder to track. Some other behavior ISPs track include how many times messages are forwarded, how often messages are deleted without being read, how often a sender is added to a contact book, and how often a message is moved from one folder to another. The ISP definition of engagement hinges on a combination of these metrics that are invisible to a sender, but are critical to the success of every single campaign.

Although the definitions of engagement are based on different sets of insights, the net result is the same: send email to engaged users who want to receive it and you will most likely have good, sustained inbox placement and deliverability. To use an example, if your email is unopened by 90% of recipients, ISPs might start to filter that email to spam, rather than the inbox because recipient engagement has told ISPs that the email isn't wanted.

## Email Content

Your reputation can also be impacted by the content of your messages. Your email layout and template, links included, use of link shorteners (don't!), words in your subject line, and even wording within the body can impact the reputation of your emails. You can build your brand's reputation with engaging content, a professional look and feel, and legitimate links.


**NEW FOR 2018**

**Don't use link shorteners:**
Link shorteners are often used by spammers to obfuscate malicious links that lead to ransomware and other infected pages. ISPs look unfavorably on links in emails that were produced using link shorteners. If you absolutely insist on using a link shortener, consider using a branded or vanity domain instead of the default bit.ly or ow.ly domains as these will most certainly hurt your chances of getting email delivered to the inbox.

## Spam Complaints

There's a lot more to sender reputation than spam complaint percentage; however, a recipient marking an email as spam is the strongest negative signal to ISPs about your email. Spam complaint rates above 0.2% are considered high, and may result in poor deliverability. At other ISPs, like Gmail, a spam rate as low as .08% can "start to affect" your deliverability, which is why you need to keep a close eye on them.

## Spam Traps

Spam traps are email addresses that should never receive email because they're old and haven't been used in a long time, or because the email address has never signed up to receive email. The former is called a recycled spam trap, the latter is called a pristine spam trap (or a honeypot as they're known at AOL), and they're both signs that you aren't keeping your list clean. You can avoid recycled spam traps by removing recipients from your list after long periods of non-engagement. To avoid pristine spam traps, simply avoid purchasing, renting or scraping email addresses.

### Pristine Spam Traps

Pristine spam traps exist solely to identify senders who are using inappropriate means of acquiring email addresses, like purchasing a list or by using a bot to scrape for email addresses. Neither of these practices are "okay" because recipients have not opted into your email campaigns. These addresses are often created and monitored by ISPs or blacklists.

The result of growing your list in this inorganic fashion could mean long-term poor deliverability that is difficult to remediate because of a very negative reputation for your sending IPs and domains.

NEW FOR 2018

### "Typo" Traps

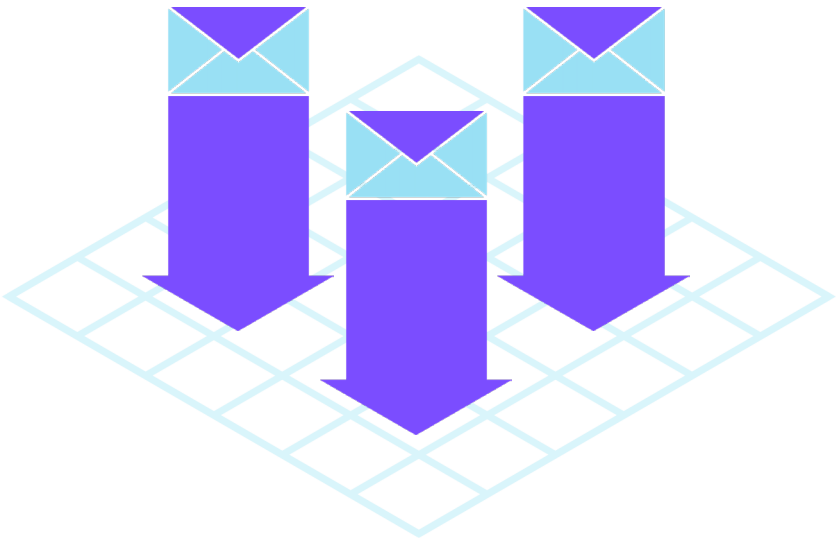
Recently, "typo" traps are the majority of senders' trap types. Make sure your address collection methodology removes typos in email addresses (local@gmall.com vs. local@gmail.com), and make sure recipients interact with some kind of opt-in or a subsequent welcome message before including the address in normal email campaigns.

### Sending Confirmation Emails

One of the easiest ways to avoid invalid addresses, spam traps, and blacklists is to send a confirmation email to new email recipients. This process validates their email and confirms that they want your messages. We can't stress enough how problematic renting, purchasing, or scraping email addresses can be to establishing a good sending reputation.

## Invalid Email Addresses

Sending email to a large number of invalid or non-existent email addresses is a negative signal to inbox providers. Reduce the number of messages sent to invalid email addresses by immediately removing bounced addresses from your active mailing list. Abandoned email accounts can also turn into invalid addresses, so removing long-term, non-engaged addresses from your list is a good habit. Sending an email confirmation message immediately after sign up can greatly reduce invalid address rates as well. This practice is commonly known as double opt-in or confirmed opt-in. You may also use engagement with welcome emails as a way to validate the email address is real and used by the recipient.



## Blacklists

Many inbox providers monitor blacklists to help them determine which senders to block or filter. Most blacklists will list your IP or sending domain if they detect a high number of spam trap hits, spam complaints, or both. Avoid blacklists by sending relevant content to recipients who have recently engaged with your emails.

**NEW FOR 2018**

**Not all blacklists are created equal!**
Simply because you're listed on a blacklist, doesn't necessarily mean your deliverability is being impacted. Some blacklists are much more impactful than others, and if you think you've been listed, we recommend working with our Delivery Experts to determine what to do next. If you're interested in seeing if you've been blacklisted or not, we think MXToolBox is the best free lookup option.

**Links to third parties could be doing more harm than good.**
Even if you're doing everything right, a single link to an unreputable website in the body of your message can prevent your email from getting to the inbox. Similarly, if your domain or website appears in more "spammy" email streams, it can impact your deliverability.

## Domain Reputation

Your domain has a reputation associated with it, and it's just as important as the reputation of your IP address. 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 be filtered.

**NEW FOR 2018**

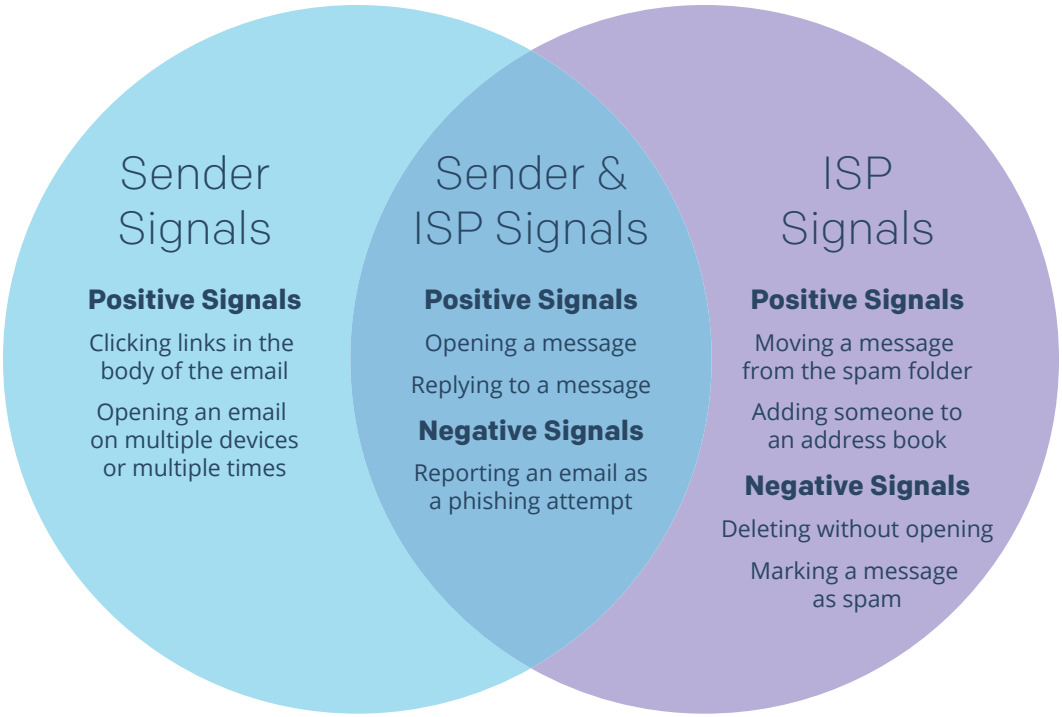
**Recently we've heard from anti-abuse sources that "cousin domains" may be triggers for ISPs.**
This is when, for example, company.com also uses company-mail.com, companymail.com, and companydeals.com to send different mail streams.

We know that you may have two domains set up for corporate vs. marketing email, but when it's overboard, it can appear to ISPs that you're trying to hide the reputation of one stream from another.

## Switching IP Addresses Isn't the Answer - NEW FOR 2018

When deliverability challenges arise, many senders think the quickest route to resolving the problem is to switch their sending IP. Take our advice on this: don't do it. Switching IPs that are having deliverability challenges isn't addressing the problem—he domain reputation will remain unchanged. Further, switching IPs is a common tactic used by spammers and will create even bigger problems for you to resolve.

To recap, here's a list of user actions that affect your reputation and deliverability. Some of these you can control and measure, while others are solely visible to the ISP and is how they measure engagement and your sending reputation.



# Infrastructure and Authentication

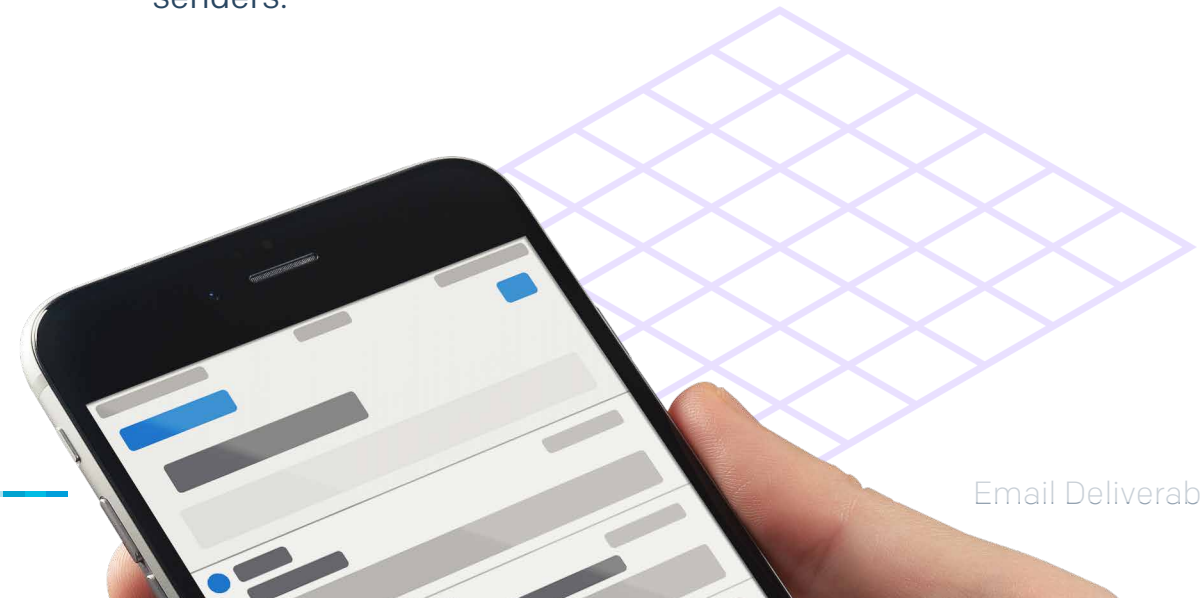
Your email infrastructure is what goes on behind the scenes and helps get your message to your recipient's inbox. Infrastructure often refers to the IP addresses and servers you're using to send email, while authentication refers to the validation techniques you use to show that email coming from you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

- **IP address** - Whether you're using a single address or multiple, or if you're sending from a shared or dedicated IP, your IP address says a lot about you as a sender.
- **SPF, DKIM, and DMARC** - Making sure your email is authenticated in the right ways is critical to your deliverability.

Having a properly configured infrastructure can greatly impact your ability to reach your recipient's inbox. Below are a few of the most important infrastructure questions that all senders should be asking themselves.

## Are you using a dedicated IP address?

If you're a high-volume sender who's working with an email service provider, make sure you have an IP address (or a few) dedicated to your email stream. Sharing IP addresses with other senders means their practices and reputation will have a direct impact on your deliverability. We think that as more focus is shifted toward IPv6, IP reputation will become even more important for larger senders.



For smaller senders who are sending fewer than 50,000 messages per month, sharing an IP address isn't the end of the world, in fact, it's likely the smartest choice. However, you should be careful, sharing a root domain with other mail streams (transactional vs. marketing) will bleed reputations into each other. This means, for example, that poor engagement from marketing campaigns may impact the way a purchase receipt is delivered.

**Why a shared IP isn't always bad**

For smaller senders, a shared IP can be beneficial because they don't always have consistent volume. This inconsistency can raise red flags to ISPs, so sharing an IP address with other senders helps to maintain volume and some reputation. As senders grow and can maintain more consistent volume and frequency, moving to a dedicated IP address is encouraged.

**Experiment with segmentation.**

You can take segmentation as far as you'd like. Some senders segment based on timezone, engagement level, sign-up date, age, and just about anything else you can think of. It's important to think of each recipient as an individual with unique expectations. Segmentation can help you cater to the needs of various types of recipients.

## Are you segmenting your email streams on different IPs?

Larger senders should separate their mail streams by IP address. The most basic separation is at the level of marketing and transactional messages. These mail streams often have very different reputations and must comply to 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 assessments.

**Win-Back Strategy**

Win-back, or reactivation, campaigns can be tricky; special care should be taken before sending a large number of these emails. According to postmasters we've spoken with, reactivation campaigns often have the poorest deliverability and highest spam complaints of any mailstream they see. Consider an ongoing drip campaign of reactivation emails, just a few hundred at a time (or per hour) vs. a large one-time reactivation run to keep the volume of complaints low. Alternatively, you may want to use a different IP for this kind of campaign so as not to affect the reputation of your primary IP/domain.

## Does your sending domain have an SPF record?

An SPF (Sender Policy Framework) record is a simple domain name system (DNS) record that identifies which IP addresses are allowed to send email using your domain. Publish an SPF record and make sure it lists all the IP addresses that will be sending email from your domain.

**SPF Strategy**

ISPs generally don't block email solely because of a missing SPF record. However, it is one more data point that contributes to a sender's reputation and it helps protect your brand. SendGrid requires senders to have an SPF record as a best practice. We also walk you through generating an SPF record during the whitelabeling process.

## Do you sign your email with DKIM?

DKIM stands for Domain Keys Identified Mail. DKIM signatures ensure that the message that arrives at the inbox provider is identical to the message that you sent. DKIM defends against malicious modification of messages in transit, and it carries a lot of reputation weight because a passing DKIM value also means the sender takes responsibility for the content and who they're sending it to. These days, messages not signed with a DKIM signature are very unlikely to see the inbox. Fortunately, SendGrid automatically signs all of your outbound email with DKIM.

**Get started with DMARC now!**

To properly implement a DMARC policy, you have to account for every system that sends email on behalf of your domain and make sure the IP addresses of these systems are present in your SPF record. This can take quite a bit of time and energy, so start thinking about it sooner than later. You can learn all about DMARC in our blog post, *What is DMARC?*

## Have you published a DMARC record?

The purpose of a Domain-based Message Authentication, Reporting & Conformance (DMARC) record is to tell inbox providers what you want them to do with email that doesn't pass SPF and DKIM: allow it, filter it, or reject it. In the near future, publishing a DMARC record will be necessary to ensure good deliverability to reputable inbox providers.

**NEW FOR 2018**

**Did you know?**

We've even seen Gmail rewarding senders that implement a DMARC policy of "reject" by showing the sender's logo in the mobile mail client view if they have a Google + profile setup!


*Glassdoor has implemented a DMARC policy of "reject," and as a result, their logo shows up, rather than the generic "G" that Gmail would display without the policy.*

## Do you have A records and PTR records in place?

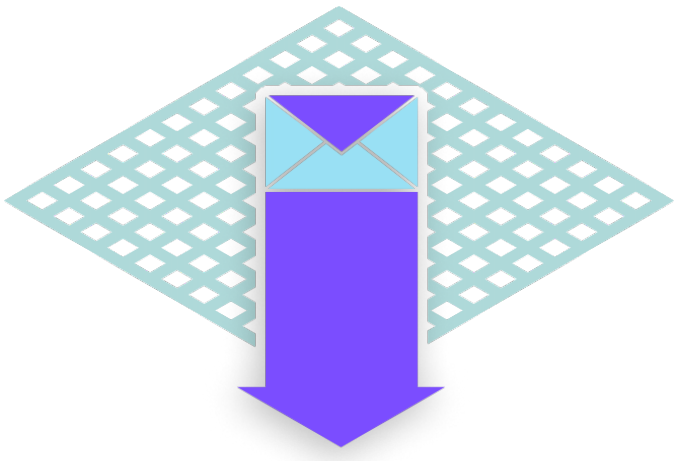
A records point your domain to an IP address, while pointer (PTR) records link an IP to your domain. Having these pieces in place is an important step in building trust between you and the inbox providers. SendGrid walks you through generating these records in the whitelabeling process.

## Is your sending domain able to receive mail?

Your sending domain needs to be able to receive mail, and it must have a valid mail exchanger (MX) record. If not, some ISPs will block your email. SendGrid's whitelabel process generates these records for you. It is as easy as copy and pasting these records into your DNS. We also recommend going one step further and making sure the full "from" address is an inbox that can receive mail (this allows a recipient to respond to that address and not get a failure message).

## Are you using TLS (Transport Layer Security) to send email?

TLS is a means of encrypting email in flight. By encrypting messages in flight, senders can prevent someone reading, or snooping, the mail traffic as it moves between sender and receiver. Most major ISPs are employing TLS, Google even has a Transparency Report that measures the amount of encrypted traffic they receive. Fortunately for you, SendGrid sends using TLS and establishes a secure connection with domains where it is opportunistically available.

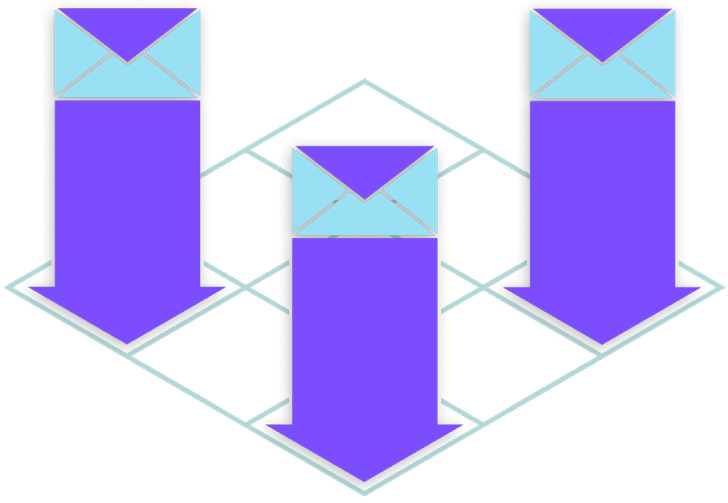


## Are you signed up for feedback loops?

Most major ISPs offer what are called spam feedback loops (FBLs). FBLs let you know when recipients mark messages as spam. Responsible senders immediately remove the addresses of spam reporters from their active mailing lists. Continuing to email recipients who have indicated that they don't want your messages is extremely detrimental to your reputation. With SendGrid, your email is automatically integrated with all the major spam feedback loops—our system will automatically suppress email addresses of spam reporters.

## Do you have "postmaster" and "abuse" mailboxes set up for all your domains?

If yes, are you monitoring them? In addition to being a best practice, many ISPs require you have abuse@ and postmaster@ email addresses set up in order to get access to their FBLs. These are also common destinations for complaints from ISPs that don't have FBLs, so it is a good idea to watch the traffic that flows to them and address any reports of unsolicited email.



**Role Accounts**

Since postmaster@, abuse@, and a few others, are considered standard role accounts, sending anything other than abuse complaints to them is considered an inherently bad practice. You should consider automatically suppressing these envelopes at any domain to ensure compliance with sending best practices. Learn more about role accounts in our blog post *Role Addresses and Their Effect on Email Deliverability*.

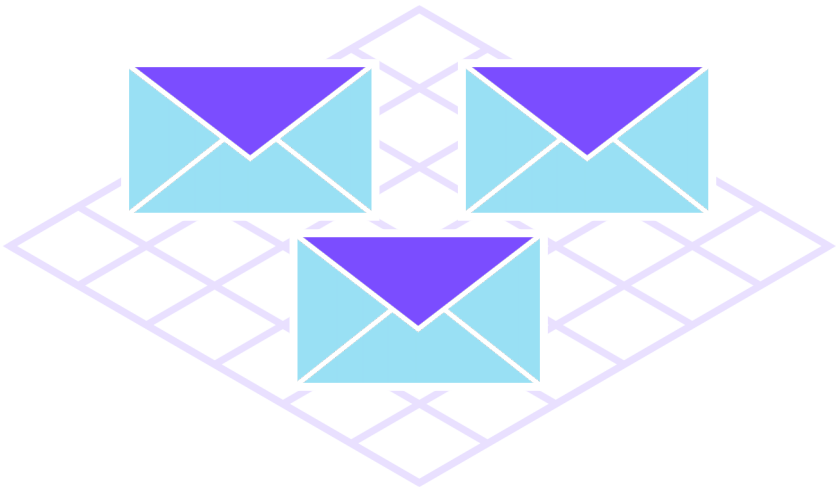
# Your Emails: The Basics for Keeping Your Reputation Intact and Your Recipients Happy

Now that you know what ISPs are taking into account when evaluating your email and what you can do to make sure they accept your messages, it's time to look at your emails themselves. At the end of the day, a lot of what impacts your deliverability is what messages you're sending and how your recipients engage with them. Below are some of our email tips you should keep in mind before and after sending your next campaign.

## Ask permission and respect it

Email is a unique type of marketing in that the recipient of your advertisement gets to decide whether or not they like it, and whether or not they want to receive more of it. You're truly a guest in their inbox. If you aren't a polite guest, or if you wear out your welcome, you won't be invited back. Being a polite guest in the inbox is all about asking permission to email someone, and honoring the terms of that permission. If someone agrees to receive your weekly newsletter, you're asking for trouble if you send offers every day.

**Be a polite guest!**
Set clear expectations at the point of email address collection and honor those expectations. You can learn more in our webcast *Great Expectations: Setting Your Email Marketing Up For Success*.



## Create an email preference center

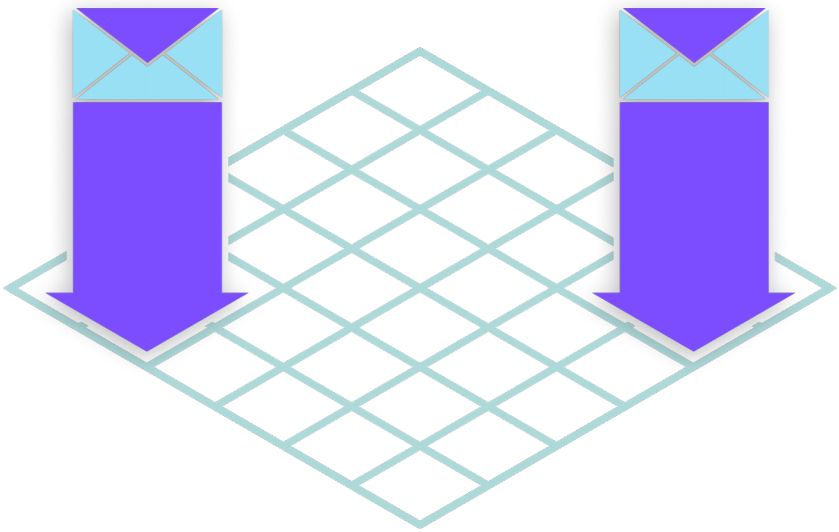
This goes hand-in-hand with being a welcome guest in your recipient's inbox. An email preference center allows users to tell you exactly what types of email they're interested in. The key to a healthy email program is sending email that people are interested in receiving: Take out the guesswork by asking your recipients exactly what they want and how often they want it.

## Send a welcome message

A well-written welcome message helps set the tone for a new email relationship. Your welcome message should remind users why they signed up for your email program. Along with arriving as real-time as possible, it should tell them what types of email they should expect to receive from you and how often they should expect to receive it. Welcome messages should also include unsubscribe and preference center links.

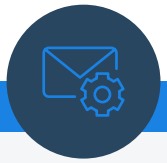
## Removed unengaged recipients

Repeatedly emailing recipients who aren't engaging with your emails can be bad for your reputation for several reasons: Addresses that don't open or click on your messages are much more likely to mark messages as spam. Unengaged addresses may have been repurposed into spam traps. Unengaged recipients can make your traffic look unwanted by lowering your open rate.



## Make it easy to unsubscribe

This sounds counterintuitive, but making your unsubscribe process as easy as possible is a really good idea. The truth is, if someone doesn't want to receive your messages and they don't have an easy way to unsubscribe from them, they always know where the "report spam" button is. Include an unsubscribe link at the top of the message as well as the bottom. Remember, someone who opts out can always opt back in, but a spam complaint can hurt your entire campaign, if not your ongoing ability to deliver messages to those who want to receive them.



**NEW FOR 2018**

### Think about list-unsubscribe

List-unsubscribe is a header that allows end-recipients the ability to be removed from a mailing list without clicking the unsubscribe link or hitting the spam/junk button. Essentially, if you use list-unsubscribe, Gmail and Microsoft will add an unsubscribe link to the header of your emails, allowing people to unsubscribe without opening the message. You can learn more about them in *What You Need to Know About List-Unsubscribe* and in *Don't Fear the New iOS 10 Update*.

### Don't forget about "downsubscribes"!

One of the ways you can use your email preference center to your advantage is by allowing people to "downsubscribe." This is when a recipient chooses to not receive messages that are part of a specific campaign, rather than removing themselves from your lists completely. Allow recipients who click on the unsubscribe link to have the option to continue receiving specific types of email.

## Be conscious of your sending frequency!

If you feel like you're doing all the right things with your email program, but you're still landing in the spam folder, it may be a good idea to examine your sending frequency. Between your regular newsletter, special offers, and other announcements, you could be sending your recipients more email than you think. Exactly what is "too much" email is different for every sender, but if you are being filtered, even moderately reducing the amount of email your recipients receive from you is almost always a good idea.

# Summary

Email delivery isn't guaranteed. There's no magic bullet that's going to get all of your email to the inbox. However, we believe that nearly every piece of advice in this guide can be boiled down to a single principal:

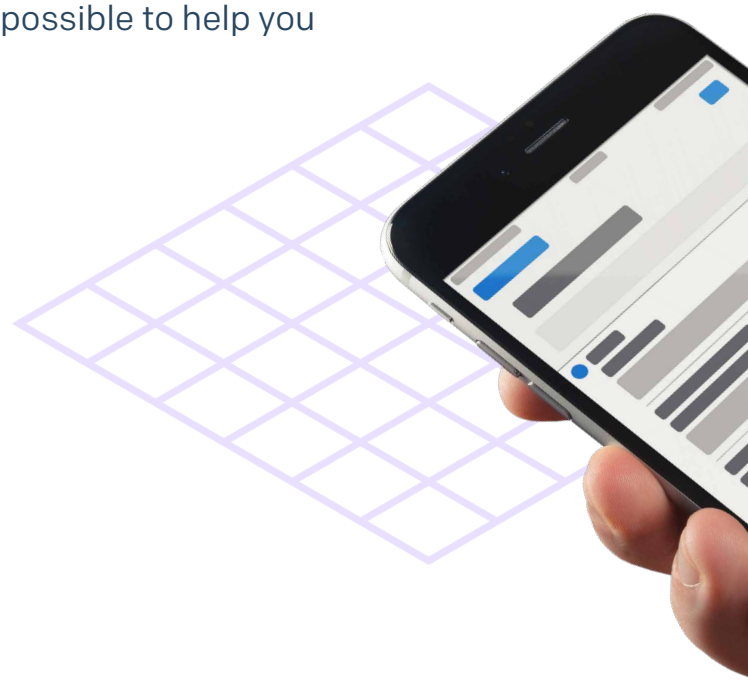
*Send the right message, to the right person, at the right time, with the right frequency.*

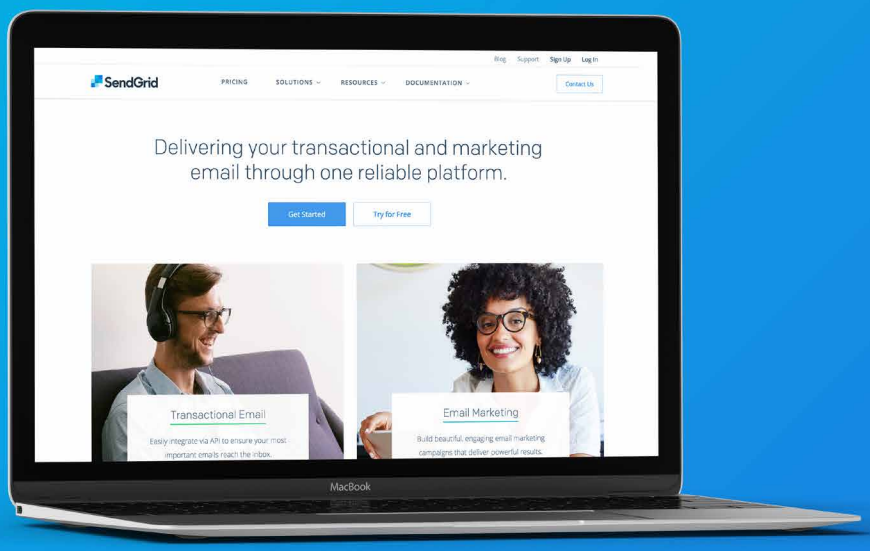
As a sender, you should be attempting to accomplish this with the following process:

- **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 are expecting to receive it.
- **The right frequency**: Don't send too much email to your recipients or email them too frequently.

In addition to this guide, SendGrid has created numerous resources that we update as often as possible to help you maintain a healthy email program:

- Documentation
- Blog
- Best Practice Guides
- Webcasts
- Customer Success Stories






# About SendGrid

SendGrid helps you focus on your business without the cost and complexity of owning and maintaining an email infrastructure. We help with all technical details (from whitelabeling to DKIM) and offer world-class deliverability expertise to help your emails reach the inbox. And with a full-featured marketing email service that offers an intuitive workflow, effortless list segmentation, and actionable analytics, all of your email needs are met in one simple platform.

**Learn More**

**Read Our Customer Success Stories**

**Sign Up**