SendGrid

Top 10 Tips and Tricks to Stay Out of the Spam Folder Guide

Contents

Tips and Tricks to Stay Out of the Spam Folder

If one business goal unites brands across industries, it's that its email–whether transactional or promotional–finds the inbox and stays out of the spam folder. But as anyone who has sent email on behalf of a brand knows, this is no simple feat. Reality check: it's not even 100% possible!

The hard truth of today's email ecosystem is that every sender, no matter how conforming, will experience inboxing and spam issues at some point. At SendGrid, we internalize, preach, and practice our mantra of sending the right message, to the right person, at the right time, with the right frequency. Apply our mantra to your email strategy, while following the tips below to position your email program as one of the good guys, and one that's worthy of the inbox.

> ***"...sending the right message, to the right person, at the right time, with the right frequency."***

Wondering what an acceptable spam complaint rate is? Shooting for a .08% spam complaint rate is as low as you can get today. Don't feel discouraged if your spam complaint rates are higher. Following best practices and constantly monitoring your email program will reduce complaint rates.

① Don't rent, share, scrape or co-register email lists

First, some tough love: sender reputation and email delivery responsibility fall squarely on the sender, not an Internet Service Provider (ISP) or Email Service Provider (ESP). And sending email to those who have not agreed to receive your email sinks your sender reputation faster than any other email offense. Fortunately, there's a lot you can do as a sender to keep your reputation on the right side of the inbox, and it all starts with your email address collection methods.

Take pride–and your time–when collecting email addresses to cultivate a healthy list of recipients who have agreed and look forward to receiving your email. ESPs, such as SendGrid, can certainly help (that's what we're here for!), but ultimately maintaining a solid sender reputation is up to you.

Always and forever avoid the following crimes against deliverability:

RENTING OR PURCHASING AN EMAIL LIST

Paying a third party for a large list of addresses sabotages your email marketing and is possibly illegal (depending on how that third party compiled the list–which is out of your control). Just. Don't.

SHARING YOUR EMAIL LIST

Sharing or using a shared email list hurts your email deliverability–even if you share and swap lists with a trusted business partner. Instead, recommend your partner in your own email and link to their sign up, and vice versa.

CO-REGISTER YOUR EMAIL LIST

When you co-register your email list, you are acquiring leads and specific email addresses that originated from a bulk email opt-in by a customer who agrees to be included in multiple email lists. But, once again, that doesn't mean they have agreed specifically to be emailed by you.

SCRAPING EMAILS

Also known as email harvesting, scraping emails is the worst offense of any email list building crimes. A robot typically collects these addresses, and this practice is most common among spammers.

Your email list is a unique representation of your email marketing efforts. It should never come from a third party. For more on how to grow your email list the right way, and the way that will keep you out of the spam folder, read *How to Authentically Grow Your Email List*.

② Consider your opt-in

Now that you are well on your way to building a reputable email list, you'll want to consider the process in which you opt your recipients into your email program. Setting up a clear opt-in process establishes expectations, defines the relationship with your recipient right from the start, and also avoids spam traps (emails no longer active, but initially set up to catch people emailing to inactive accounts).

SendGrid recommends the following three ways to opt-in your email list:

CONFIRMED OPT-IN

A subscriber receives a confirmation "welcome" email or the start of a welcome series once they opt-in to a particular email list. This affirms the recipient's decision (that they did not unknowingly sign up, or since change their mind). Confirmed opt-ins increase engagement and verify to the sender that the email address is real.

PRE-SELECTED OPT-IN WITH CONFIRMATION

Pre-selected opt-in defaults a signup (usually in a checkbox) so a recipient may not have knowingly signed up to receive your email. A confirmation email is sent to any recipient who has left the pre-selected opt-in checkbox intact to ensure that they did, in fact, intend to sign up to receive email.

DOUBLE OPT-IN

This form of opt-in is very similar to a confirmed opt-in with a caveat that requires action on behalf of the recipient (usually to click a link within a call to action) to double opt-in themselves into an email list.

This is the best method for collecting addresses because a sender demonstrates genuine desire to ensure the recipient absolutely wants their content.

You may also want to consider including a reCAPTCHA feature to your email sign up forms. A reCAPTCHA verifies that the soon-to-be recipient is a human, not a spambot signing up for your email. This will keep your email list clean and safe from spam traps. Learn how to secure your email sign up forms.

3 Authenticate your email

Authenticating your email lends a greater degree of trust to your mail streams. Inbox providers use authentication to verify that a sender is who they say they are. Authenticated email has a much better chance of landing in the inbox than unauthenticated email. SendGrid recommends the following three forms of authentication in today's sending world:

SENDER POLICY FRAMEWORK (SPF)

SPF is an email authentication standard that compares the email sender's actual IP address to a list of IP addresses authorized to send mail from that domain. The IP list is published in the domain's DNS record. For a more in-depth explanation of SPF, read Sender Policy Framework: A Layer of Protection in Email Infrastructure.

DOMAIN KEYS IDENTIFIED MAIL (DKIM)

DKIM ensures that an email has not been tampered with during transmission. DKIM acts like a wax seal on a letter. If the letter's seal remains sealed upon delivery, it was securely transported. Learn more about DKIM.

DOMAIN-BASED MESSAGE AUTHENTICATION REPORTING AND CONFORMANCE (DMARC)

DMARC is a more sophisticated authentication method that leverages both SPF and DKIM (both must pass) to prevent email spoofing (forging a sender address). For a deeper dive into DMARC, read What is DMARC?

If you choose to whitelabel your domain with SendGrid, we ensure that SPF and DKIM are aligned and working properly. Although DMARC policies rely on the customer, SendGrid offers extensive resources outlining the process. We believe whitelabeling your email is crucial to success because it will save you time and resources in the long run while benefitting your sender reputation.

SPAM MYTH 1

You must always avoid using spam trigger words - Not long ago, this tip would top our list. However, ISPs have become more and more sophisticated at deciphering spam from legitimate email. Each particular filtering system depends on the ISP, so monitor your engagement for the major ISPs if you test out new content and wording. Play around with all caps, emojis, and hashtags, but scale back if you see your engagement suffer.

4 Freshen up your email list

A smaller, more engaged email list is better than a massive, but unengaged list. Monitor your email engagement across all users to ensure the highest engaged list possible. Regularly remove inactive recipients (those who don't open your emails) from your list. Properly maintained email lists will also help you avoid more spam traps.

Follow the steps below to tidy up your list:

- Remove bounced emails and role email addresses
- Remove those who are unengaged and never open your email
- If you are changing ESPs, your suppression list should go with you (we help you with this at SendGrid)

Email marketing requires a healthy dose of humility. Accept the fact that some folks just don't want to receive email from you. The *quality* of your list is much more important (and valuable to your business) than the list quantity. So clean up your email list and watch your engagement and sender reputation soar!

Using spam checkers reduces your spam rate - Spam checkers are online tools that will test your emails and let you know how likely they are to be classified as spam. These tools are really only a sanity check because ultimately the ISP has the final say and typically doesn't share specific filtering details.

5 Monitor your reputation and blacklists

An email blacklist is a list of IP addresses, domains, or URLs that are believed to be a source of spam or excessive abuse reports. Most blacklists use spam trap networks to detect unsolicited email. Avoiding spam traps is the best way to ensure your sending IPs and domains don't end up on blacklists.

Even the most cautious senders will occasionally find themselves on an email blacklist. However, there are some strategies for reducing your risk including utilizing:

- Confirmed opt-in
- Engagement-based sunsetting policies
- Real-time address validation

Oftentimes, a sender doesn't realize they've been engaging in dangerous email activities (such as list purchases and poor sunsetting policies). Keeping a close eye on your reputation can help you avoid blacklistings, and quickly identify and triage them when they appear.

Besides following best practices, there are also a number of online tools that will provide you with an accurate picture of your sending reputation. SendGrid works with a variety of these companies. You can check them out on our partner page. Even though getting blacklisted can be scary, your email program can make a comeback even after a blacklist.

6 Give users a clear and easy way to unsubscribe or down-subscribe

The easier you make things for your recipients to take any action with your emails, even if that means to unsubscribe, the better. Achieve friction-free email action by providing a prominent and simple unsubscribe link, as well as a preference center that provides recipients with the ability to manage their email preferences. Perfect your preference center.

Respect your recipient's feelings and remember that unsubscribes always fare better than spam complaints. We suggest designing the unsubscribe feature as close to a "one-click" process as possible. Don't make a user log back in, de-select a page full of individual mail preferences, and reconfirm anything.

For senders who want a second chance to convince potential unsubscribing users to not do so with persuasive copy or more convoluted processes–don't. The best way to think about a user lifecycle is that every time you email your users, that message is another chance to demonstrate your value as a sender. If those opportunities aren't met with an engaged user, that's ok. You don't want disgruntled email recipients on your list anyway.

Follow all applicable legislation: Compliance doesn't equal delivery. The primary pieces of legislation that govern email are CANSPAM (American spam and email law) and CASL (Canada Anti-Spam Law). You should always follow these laws, but realize that just following the law is a bare minimum to stay out of legal trouble.

7 Optimize content — for your recipients

When you're compiling content for your emails, consider that you are serving *two* distinct audiences: 1) your recipients and 2) the machines that enable the email transmission. These are two vastly different concerns! Fortunately, you can serve both successfully. When creating email content for humans:

- **Provide clear/consistent branding** - Your emails should have a distinct brand identifier so recipients instantly recognize your email.
- **Limit scrolling** - the longer your recipients need to scroll down to read your content or take action, the more likely their 8-second attention span will move on.
- **Be responsive** - if an email isn't displaying properly, your recipient will most likely delete it or worse, report it as spam.
- **Be relevant** - You can follow every deliverability rule, but if your content isn't relevant to your recipients, they're not going to engage.

If an email was reported as delivered, it means it got into the inbox - Unfortunately, it's a bit more complicated that. Consider that even if an email is reported as delivered, it doesn't mean it ended up in the inbox. A delivered email simply means that the ISP confirmed successful reception for the message with a 250ok response. However, an inbox delivery and a spam folder delivery are both represented by the same delivery metric.

⑧ Optimize content — for machines

If ISPs can't readily tell what your email contains, it defaults the message into the spam folder–even if your recipient wanted to receive your email. Fight back by following the tips that cater your email content to machines:

- **Don't use free link shorteners (like Bitly) in your messages**—Because spammers commonly use link shorteners, they are a warning sign to ISPs. Link shorteners also dilute your brand prevalence.
- **Optimize all images** - The more clues you provide to ISPs about the content of your email, the more likely it will recognize and categorize your email properly. Add an alt text for each image you use, don't include massive images, and include responsive designs.
- **Host your own images** - Hosting your own images gives you full credit of the alt text within your images.
- **Include responsive design** - Both humans and machines appreciate responsive design when evaluating an email.
- **Practice good text: image ratio** - Providing 2-4 sentences per image helps give context for the ISP and your recipients.
- **Be aware of Gmail clipping** - If your email is too large, it could be clipped by Gmail. Make sure you preview the results in a test email and adjust copy if necessary.
- **Adding link tracking** - Tracking links help senders further assess engagement. When using link tracking, you won't need to use link shorteners, and you should ideally use link URLs that match the from, DKIM, and Return-Path.

Balancing content for both humans and machines optimizes your email program for both sides. Remember that there's no hard rule that if you break or follow guarantees inbox placement. You just need to give the ISP some indication about what the messages includes. Regular experimenting and reflection will allow you to strike the perfect human/machine content balance.

9 Monitor your email program email metrics regularly

Before you begin to monitor your email metrics on an ongoing basis, you'll want to determine a baseline for metrics such as:

- spam complaints
- open rates
- clickthrough rates
- delivery rates

Keep in mind that each ISP provides results based on different proprietary (and usually secret) variables so you can formulate a picture of your performance, not an exact conclusion.

When you do notice a negative trend, such as lower open rates, you shouldn't panic. But by acting as quickly as possible to determine the issue, you'll be able to get ahead of the issues and you will prove to ISPs that you're a considerate sender. And that will net you improved delivery results.

Test your emails with real content: When testing your emails, use real content and send to real recipients. Skip the seed testing as this simulation does little more than provide a false sense of security.

Performing seed testing improves delivery rates - Seed testing is a form of email testing in which you send an email to a list of "test emails" from your larger list with the intention to measure how ISPs respond to the smaller "test" batch. This may make you feel as though you're testing how an email will resonate, but since every ISP weights it differently, it won't provide you with a perfect analysis.

10 Have a plan if when things go wrong

Email is complicated and no email program is perfect. You can follow every tip or piece of email advice, but sometimes things won't go your way. In fact, the hardest rule on this list is that you will, at some point, have email delivery issues.

First things first; slow down and don't panic. Have a plan in place that you can follow when something goes wrong. If you're a SendGrid customer, our Support Team is available around the clock to help you no matter your issue. We also offer a variety of expert consulting services including onboarding and ongoing consulting.

Email is an ever-changing marketing channel that continues to prove itself as one of the most effective ways to communicate with your customers. It pays to get it right. Follow the tips above and enjoy increased inbox delivery rates, fewer spam complaints, and happier customers!

Get Started with SendGrid

Learn More

Read Our Customer Success Stories

Sign Up

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 a flexible workflow, powerful list segmentation, and actionable analytics, all of your email needs are met in one simple platform.

↑Contents