SendGrid
Email Delivery. Simplified.

Tips and Tricks to Stay Out of the Spam Folder

At SendGrid we are very serious about email deliverability. We live and breathe it each day. Similar to how Google keeps adjusting its search algorithm to provide the best results, we must also regularly adjust to ensure that our clients' emails are delivered. Here we offer advice to help you make sure that your emails reach the inbox. Of course, the very best advice we can offer is to use SendGrid to do all the heavy lifting for you.

10 Basics to Avoid Being Categorized as Spam

1 Be Compliant with the CAN-SPAM Act

If you are sending "any electronic mail message, the primary purpose of which is the commercial advertisement or promotion of a commercial product or service," then you must comply with the following 7 main requirements (or face penalties up to $16,000):

1. Don't use false or misleading header information
2. Don't use deceptive subject lines
3. Identify the message as an advertisement
4. Tell recipients where you're located
5. Tell recipients how to opt-out of receiving future email from you
6. Honor opt-out requests promptly
7. Monitor what others are doing on your behalf

If your email contains only transactional emails or relationship content, then you are exempt from these rules; however, you must still not include false or misleading routing information.

2 Avoid Spam Trigger Words and Phishing Phrases

Any email containing a spam trigger word is more likely to end up in your spam folder. Unfortunately, there is no definitive list of trigger words to avoid when constructing your emails.

Phishing emails are designed to steal your identity by getting you to click on a fraudulent link. The most common phishing method is to disguise an email as one from a legitimate service that you trust, such as your bank or a website you visit. By avoiding grammar mistakes and misspellings and never asking for personal information you have a better chance of staying out of the spam folder.

3 Include a Text Version of Your Email if You Are Sending HTML Emails

Most email programs these days support HTML formatted emails, but that doesn't mean you can just ignore the plain text version. Sending HTML only emails is a common cause for ending up in the spam filter.

Making sure to include a text version of your email also covers you in case a recipient cannot view HTML emails. Considering the number of emails now being opened on mobile devices, including a text only version is sure to remain a best practice for a long time.

4 Use Permission Marketing Techniques

Permission marketing, a term coined by Seth Godin, defines permission as the privilege to deliver anticipated, personal, and relevant messages to people who actually want to get them. Permission marketing maintains that treating people with respect is the best way to gain attention, and that you know you have real permission when people miss your emails when they stop arriving.

The most difficult part of permission marketing is making a promise and sticking to it. Tell people what they can expect from your emails and how often to expect them. Once they opt-in, don't change the rules. Permission marketing requires patience and humility, but it will pay off in the long run.

5 Use Spam Checkers before Sending Your Emails

Before sending emails out to your entire list, it's worth the time to utilize a spam checking service. MailingCheck.com offers a free downloadable tool for Windows that uses SpamAssassin to check. If you prefer to avoid downloading any software, you can send email to the IsNotSpam.com service and they will also check a few other items important to email deliverability. Alternatively, ProgrammersHeaven.com uses a form-based solution to test your emails.

6 Get off All Blacklists

A blacklist is a list of addresses and domains that have been identified as spammers and are blocked from sending to mail providers. If your email server ends up on a blacklist, it becomes extremely difficult to reliably deliver email, especially to new people on your list.

To check to see if your email server is on a blacklist, use a free service like Return Path's SenderScore or blacklistmonitoring.com. If you find that you are on a blacklist, you will need to follow up with the site that has added you their blacklist. It can be tedious and time-consuming, but removing yourself from blacklists is crucial to ensuring your emails are received by the users who expect them.

7 Maintain a Good Text to Image Ratio

It is usually best to not include images at all; however, if you must include images, here are some tips:

- Don't send any image-only emails
- We suggest that for every graphic, include at least two lines of text
- Optimize your images the best you can
- Use well formatted HTML for email

8 Avoid Spam Traps

Spam Traps are email addresses that are flagged by ISPs as being no longer used by a human. Since no one is using these addresses, the ISPs know that there was no opt-in for any email those addresses receive.

9 Avoid Large Attachments and Executable Attachment Types

In general, .jpg, .gif, .png and .pdf attachments are safe to send, provided you include some content in the email as well. However, executable attachments such as .exe, .zip, .swf, etc. should be avoided entirely. Generally, you should not send attachments to people on your list that are not expecting them.

If you need to email a large attachment or an attachment type that usually can be flagged as spam or trigger virus scanners, we recommend a service such as DropBox.com. If the attachment contains sensitive data, you may consider using your company's secure FTP server.

10 Make Sure Your DKIM, SPF, Sender-ID and Domain Keys Are Setup Properly

You will want to make sure your email server supports these protocols (DKIM, SPF, Sender-ID and Domain Keys) and that they are properly implemented.

This alphabet soup helps ISPs determine the authenticity of your email from a technical perspective. For more information on email authentication and how to implement these protocols, please refer to SendGrid's Email Deliverability Guide.

Bonus Tip: Use an Email Delivery Service

If this whole process seems daunting and you would rather just focus on your company, we understand! Providing the best email deliverability is the reason we exist. You can either use our SMTP service to get started in minutes or you can utilize our REST API for maximum customization.

Design Tips for Optimal Email Deliverability

The challenge of email design is a significant one. Even the best-designed emails may still have trouble making it to the inbox. Assuming you do earn your way past the spam filters, poor design might inspire the recipient to delete the message, or worse, label it as spam.

Luckily there are some proven best practices to ensure recipients not only receive but also read and interact with your messages:

1. Don't Rely On Images to Communicate Your Email Value Proposition. Often, email readers tend to turn images off by default as a security measure. Therefore, focus on the HTML code and use images sparingly to ensure your emails render properly in the various email readers. You can set up individual email accounts at the different service providers to send test messages or use an email preview tool to check how your email renders with images turned off before you deploy. In this way, you can ensure that you have enough text to entice the subscriber to display images and read your entire email.

2. Use the ALT tag & store images on a web server: Complete the alt tag with a description of each image so recipients will know what the image is that they are missing before they download. If the image contains a special offer, make sure the alt tag communicates that. You want the reader to download your full message and click on the offer. Also, don't embed your images in the email but rather store them on your server and link to them in your email. This will prevent broken images or avoid triggering spam filters that categorize your email as junk.

3. Use Inline CSS. CSS provides ease and flexibility however the support varies among email clients. Some strip it out entirely. It is extremely important not to use external CSS like that which is in a file like a website does. Instead embed it in the email or inline written at the very least.

4. Double check your code. Make sure all of your tags are valid and closed. Spammers make mistakes. You should ensure that your code is a clean as possible to avoid triggering spam filters.

5. Include a browser link to your message. If all else fails, you want to give the recipient an easy way to access your message. Include a link at the top of your message so they can view your email in their favorite browser.

Bonus Tip: Hire an HTML Email Professional:

HTML emails are very tricky as they have certain normal web coding methods and then some coding methods apply only to certain email clients. A good designer will know how to properly meld the two and to thoroughly test before any email is sent out.

Five Things to Check for your Transactional Messages

To take full advantage of transactional email, you need to have a strong messaging strategy along with sound processes and data collection practices that will help ensure your messages are delivered immediately the inbox.

Here are five final things to check to ensure your transactional emails get delivered:

1. Are your messages reaching the inbox? Transactional emails experience higher open and click through rates because customers expect and even welcome them. 20% of legitimate email routinely goes undelivered because ISPs think that email is spam. Therefore, you must continuously monitor your transactional email streams to identify delivery failures and take preventative action before it affects your customers.

2. How frequently are these emails being deployed? Transactional emails need to be timely. If a customer places an order or signs up for an account, they want an instant confirmation of that action. If you wait too long to communicate with them, your customer will lose confidence in your brand. Email deliverability becomes essential here. You may have set your systems to deploy instant notifications, but your emails may still be getting blocked preventing customers from receiving your messages. Invest in resources to ensure systems are compliant with ISP requirements so you can meet your customer's expectations and protect your brand's reputation. Each ISP has a different set of requirements so you'll need a tool to help you out here.

3. Are you designing and coding your emails for optimum deliverability? Image heavy emails and HTML errors trigger spam filters and provide a poor experience for your customer. Consider the user when creating your emails. Even transactional ones. Also remember, that your customers are reading emails on many different platforms. From smartphones to tablets, your customers are on the move. You have a limited time to get your message across. Make sure you use it wisely.

4. Are you using dedicated IPs for your transactional messages? Each IP has its own sender reputation which is what ISPs use to make filtering decisions. In order to truly optimize your email program, isolate your transactional email streams to one or more IPs. This way you can better monitor and diagnose potential delivery failures by email type. If your “friend request” email messages are being junked, then it’s easier to take action and solve your problem quickly.

5. Are your mail servers securing? Make sure you don’t have an open relay or open proxy. Follow industry standard best practices for network and server security. All the best mailing practices don’t matter if you don’t have control of your environment. If you use a third-party tool or system for this, you’re probably in good shape, but check with email deliverability experts to make sure.

Deliverability failure is a little known crisis, the dark secret of email. It may already be a big problem for you and you don’t even know. Make sure you take the time to understand its implications on your business and get the right tools and expertise in place to properly manage and optimize your email streams.

SendGrid was built by developers for developers. There is no other system that can do what we do while providing long term value that is focused on your personal success. Take control of your email and contact SendGrid today at 303-552-0653 or email contact@sendgrid.com