SendGrid
Email Delivery. Simplified.

SendGrid Deliverability Guide

SECTION 1

The Most Important Fact about Email: Delivery is Never Guaranteed

Email is the backbone of the social web, making all the connections work. Can you imagine Facebook without email or any other web application functioning without email? It is the primary – and often the only – channel for communicating with members and customers. Everything from membership confirmations to friend requests and privacy updates – all of these are sent via email.

What happens if your email doesn't arrive in the inbox? Your customers won't receive their purchase confirmations or shipping notifications. That request for a password reset never arrives. They'll never know that someone special from their preferred dating site wants to meet them.

Where does all this email end up? It either gets routed to the junk folder or it goes "missing" which means the ISP blocks it at the gateway, preventing it from reaching a mailbox at all. When this happens you won't receive a bounce alert or an error message from the ISP. You'll not only lose revenue but also risk losing trust as emails that were promised never show up.

How big is this problem? Deliverability is a secret crisis facing any business that relies on email communications. Most companies don't think about deliverability until they have a major issue where thousands or in some cases millions of emails fail to arrive. People assume that an email is delivered if they don't receive a bounce notification. The reality is very different: 20% of commercial email sent never arrives as intended*. If you're an online business you need to take steps today to increase the reliability of your email communications.

So, what is email deliverability? Simply put, successful email deliverability is your message arriving in the inbox of the recipient as intended. Email deliverability failure is when your message is either routed to the junk/bulk folder or goes missing all together.

How do you make sure your emails get delivered? Luckily there are proven techniques to prevent failures and improve your delivery rates for the long-term. This guide offers an overview of the steps most businesses need to take to maximize their email deliverability:

- ***Build your reputation***
- ***Secure your infrastructure***
- ***Authenticate your mail streams***
- ***Monitor your sending data***
- ***Send great content***

What's next? Reputation – A good one will open doors (and inboxes)

*Source: Return Path

SECTION 2

Reputation: It will Open the Inbox – or Close it

Now that you know that some email is not actually delivered and that hitting "send" is no guarantee, you're probably wondering, "What do I need to do to make sure my emails get to the inbox?" The answer is clear and unambiguous: reputation.

But, what is reputation? In the world of email, sending reputation refers to a set of specific metrics directly related to your email sending practices. Senders with good reputations get delivered and senders with poor reputations get blocked at the gateway or their messages land in the "junk" folder instead of the inbox.

What are these reputation metrics? A strong sending reputation, like a great brand or personal reputation, is built over time. Here are the things ISPs look for:

Send Relevant, Properly Formatted Email: Sending good email that your subscribers want to receive is the basis of a great sending (and brand) reputation. Make sure your HTML is properly formatted, as poorly coded emails get caught in filters or don't render properly. Make sure your content is interesting and your emails look great.

Consistent Volume: How much email do you send? High-volume senders are always a red flag, especially when volumes are inconsistent. Do you send approximately the same number of emails each week or month, or is your mailing schedule all over the map? Consistent volumes based on subscriber preferences are a key consideration for ISPs.

Very Few Complaints: Do your subscribers complain or tag your messages as "junk" or "spam?" ISPs have little or no patience for senders with high rates of complaints. Even a tiny increase in complaints can cause your email to be blocked. Keeping your complaint rate very low (less than 1% of mail that is sent and accepted by the ISP) is very important.

Avoid Spam Traps: Sending to even one spam trap or "honey pot" will instantly set back your reputation and cause deliverability problems. When you send to a spam trap (an email address activated by an ISP to catch spammers), it means you're engaging in email address harvesting (an illegal practice) or your list hygiene practices are weak. Either way, ISPs aren't going to deliver your email. Doing everything you can to avoid a spam trap is critical – keeping a clean list is an excellent start.

Low Bounce Rates: A good reputation also means that only a small percentage of your emails "bounce" back or are returned by the ISP because the account is no longer active (hard bounce) or the mailbox is temporarily full or the recipient is out-of-office (soft bounce). If a lot of your mail is bouncing back, it means your subscribers aren't engaged and you're not keeping up-to-date with them. It also indicates that your list hygiene practices are not up to industry standards. This makes your email look like spam to an ISP and your email is not likely to get delivered. Keeping your bounce rate low by implementing procedures to immediately remove "hard" bounces is essential.

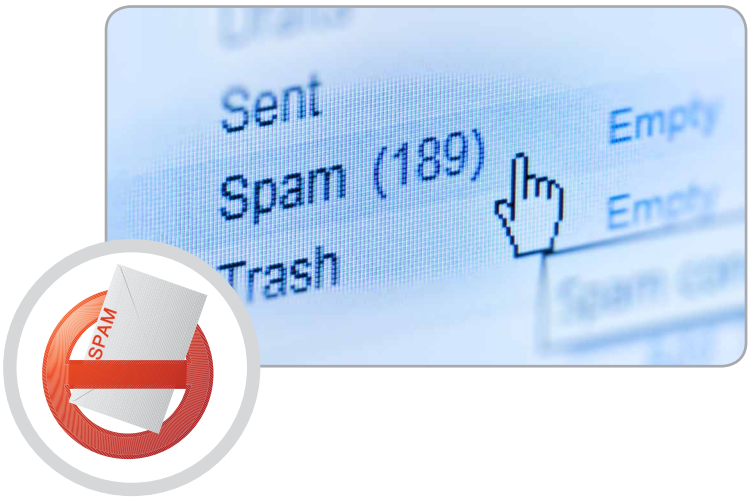
Professionally Configured Infrastructure: Is your infrastructure set up to send high-volume, commercial email? Do you have a team of IT professionals experienced in the issues related to commercial email? The way you send mail based on your set-up tells ISPs a lot about your organization. Make sure your infrastructure reflects that you are legitimate, responsible business.

No Blacklist Appearances: Appearing on just one of the leading blacklists is enough to get you blocked by some ISPs. Senders with low complaints, who don't hit spam traps and send email consistently generally don't get blacklisted. If you do get blacklisted, having a good sending reputation will help convince the blacklist administrator to remove your IPs.

Best Practice Tip

How to Avoid Spam Traps

As we mentioned, hitting just one spam trap is a reputation killer. To avoid including a Spam Trap email in your mailing list, have an industry standard opt-in process, don't rent or buy email lists and keep your list clean.



➡ ***What's next? Your infrastructure – is it part of the problem?***

SECTION 3

Infrastructure: The Foundation of Deliverability Success

Setting up and maintaining infrastructure for high-volume, transactional email is complex, challenging and expensive. It's not as simple as maintaining a corporate email environment, and very different rules and standards apply. You'll need dedicated resources who understand the issues. Incorrectly configured mail servers present a serious risk for ISPs, as they can't tell if it's a legitimate server that has a glitch or a malicious bot, zombie or other harmful machine. In these situations, ISPs always block first and ask questions later.

Can you afford to have your messages blocked for several hours or days? Do you know the current state of your infrastructure? Here are some questions to ask:

1. Are you using a dedicated IP Address? If you're working with an email provider, make sure you have an IP address dedicated to your mail stream. Ideally, have at least two IPs, one for your transactional email and a second for your marketing/promotional email. Sharing an IP address with other senders means their practices and reputation will have a direct impact on your deliverability – and that's not good for any business.

2. Are your mail servers secured or could a hacker use them for spamming? 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.

3. Are you signed up for ISP Feedback Loops? And do you have a process for managing complaints? Not only do you need to get signed up for all major ISP Feedback Loops but you also need a process for rapidly removing email addresses that log complaints. Continuing to mail to people who have reported your email as spam will result in deliverability failures.

4. Do you have "postmaster" and "abuse" mailboxes set-up for all your domains? If yes, are you monitoring them? Many ISPs require that these mailboxes be set-up and working to get access to their Feedback Loops. These are also common destinations for complaints from ISPs that don't have Feedback Loops.

5. Is your sending domain able to receive mail? Your sending domain needs to be able to receive mail, and it must have a valid MX record. If not, some ISPs will block your email.

Best Practice Tip

Resist the temptation to move IP addresses to resolve deliverability problems.

Resist the temptation to move IP addresses to resolve deliverability problems. This is a suspicious practice and ISPs treat new IPs with caution. In fact, all IP addresses start with no reputation and must be "warmed up" by your good practices. Start by sending low volumes of email and work your way up to larger volumes. This helps you build a solid reputation and improve your chances of getting high delivery rates. If your mailing practices are poor or infrastructure is not managed properly these problems (and the bad reputation) will follow you to your new IP address. Need help with your infrastructure and deliverability? Just ask. SendGrid's team of experts is ready to help.

What's next? Email authentication - just take care of it, today.

SECTION 4

Authentication: Secure Your Identity *and* Make the World Safer

Email authentication has a proven track record but a surprisingly high percentage of businesses still haven't implemented it. Authentication is an "ID check" for your mail streams: it validates that the email is actually from you (and not some spammer impersonating you). Authenticating your mail streams does not ensure your email will be delivered but it helps ISPs to further differentiate your business from spammers and other illegitimate senders. As fraudulent "phish" emails and other deceptive practices endanger consumers and businesses, authenticating your email is one positive step you can take today to make the [email] world a better place.

Strong reputation metrics combined with properly implemented authentication can significantly improve your chances of reaching the inbox. If you're sending transactional email, it's even more important since your customers are expecting and anticipating those messages.

How does authentication work? How do I get started? There are three accepted methods of authentication: Sender Policy Framework (SPF), SenderID and Domain Keys Identified Mail (DKIM). The best practice is to implement all three methods, especially if you have high-volume transactional email streams. Here's what you need to do to get started:

Step 1: Get details on the various types of authentication – implementing all three standards is the best practice. You can find detailed information on the following websites:
DKIM: http://www.dkim.org/
SenderID: http://www.microsoft.com/senderid
SPF: http://www.openspf.org

Step 2: Take stock of all systems that send your mail. Identify all machines that send mail for your company. Next, determine the IP addresses (if you're planning to use SPF or SenderID) and sending domains used.

Step 3: Create your authentication records. There are excellent online tools available for SenderID, SPF and DKIM.
Sender ID: http://www.microsoft.com/senderid
SPF: http://docs.sendgrid.com/docs/email-deliverability/spf-records-voila-validation-verisimilitude/
DKIM: http://docs.sendgrid.com/documentation/apps/domain-keys/

Step 4: Publish your authentication records. If you are using SPF, SenderID or DKIM, work with whoever manages your DNS records to publish the email authentication records you've collected. The actual publishing is easy; finding the responsible party who controls your DNS may be the tricky part.

Step 5: Set up your mail server to sign outbound email with DKIM. DKIM requires that your MTA have the appropriate software implementation to sign all outgoing emails. Learn more at: http://www.sendmail.com/sm/wp/dkim/

Step 6: Test your authentication records. SPF, SenderID, and DKIM provide options to publish your records in "test" mode. This provides the opportunity for testing without risking delivery failures. The following resources can also help you test your DKIM signed messages: http://testing.dkim.org/

Best Practice Tip

Avoid phishing phrases that will trigger spam filters.

Make sure your data collection practices are sound.

A good way to start is to quarantine your data until you know it's safe. Use your welcome message or even the first three to five messages to ferret out bounces, ill-formed addresses and even sources with a high likelihood of complaining. With good list hygiene practices and regular data monitoring, you can earn a good reputation and high delivered rates.

➡ ***What's next? Your Emails – are they good enough to get in?***

SECTION 5

Your Emails: Five Basics to Keep Your Reputation Intact – and Your Members Happy

1. ASK PERMISSION, HOST A PREFERENCE CENTER

A good reputation also means that only a small percentage of your emails "bounce" back or are returned by the ISP because the account is no longer active (hard bounce) or the mailbox is temporarily full or the recipient is out-of-office (soft bounce). If a lot of your mail is bouncing back, it means your subscribers aren't engaged and you're not keeping up-to-date with them. It also indicates that your list hygiene practices are not up to industry standards. Sounds like a spammer? Looks like a spammer to an ISP so your email isn't going to get delivered. Keeping your bounce rate low by implementing procedures to immediately remove "hard" bounces is essential.

2. KEEP A CLEAN LIST, AVOID TRAPS

A clean, well-managed subscriber list can be your best asset, whereas "dirty" lists with out-of-date information are a leading cause of deliverability failures and are sure to damage your sending reputation. List hygiene is the process of removing "bad" addresses in a timely manner. Good list hygiene practices are essential to avoiding spam traps and keeping your bounce rates low – key drivers of your reputation. There is no better way to assure consistent deliverability success than by regularly cleansing your list of hard bounces, unknown users and other inactive addresses. SendGrid's real-time Event API is a great start, providing instant information like opens, bounces and unsubscribe requests for individual subscriber records.

3. MAKE A GOOD START, SEND A WELCOME MESSAGE

Welcome messages are the cornerstone of a well-run email program. When was the last time you signed up for a new online service and didn't receive an immediate message confirming the sign-up? Welcome messages (like other transactional emails) are more than confirmations: they're an opportunity to engage with subscribers and start the relationship off on the right foot.

4. FOLLOW THE LAW

Complying with the federal CAN-SPAM law is not difficult. The requirements are straightforward and most legitimate programs were adhering to these standards long before they were legally required. Here's what you need to do:

- Have a working unsubscribe mechanism in the footer and/or header of all email communications. A link to your preference center is also a good idea, but make sure the removal can be done in a few clicks.

- Include your official business street address in the footer of all email communications. This should be your corporate headquarters or another address where official communications are handled. It cannot be a PO Box.
- Handle all unsubscribe requests within 10 business days. This means when someone asks to be removed from your list, you must suppress that email address from future mailings within 10 business days. This is the minimum, and ideally the suppression should occur within 24 hours.

Quick disclaimer, the tips above are not legal advice, you should get professional advice from a lawyer to address any specific concerns around compliance.

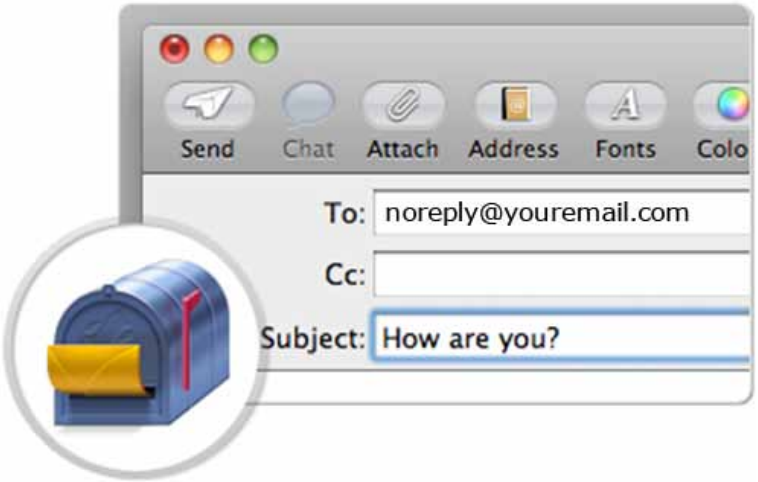
5. SEND GOOD EMAIL

It sounds obvious but it's actually harder than it sounds. There is no secret formula to sending emails that work. First, make sure you're following the four suggestions outlined above. Second, the content of your emails needs to be relevant, interesting and aesthetically aligned with your brand. Ask yourself some basic questions before you hit "send": Will my subscribers want to read this email? Does the email look good? Is it a positive reflection of my brand? Overall, am I getting the right message to the right subscriber at the right time?

Best Practice Tip

Don't Use noreply@domain.com in your emails.

Webmail email providers such as Yahoo! and Gmail automatically add email addresses that users reply to, to their contacts list. Messages from senders in the contact lists won't be marked as spam in most cases. The best way to start is to allow registered users to reply to emails to confirm their email accounts in addition to providing a confirmation link.



What's Next?

We've given you the facts:

- **Email deliverability is a secret crisis that could be affecting your business today.**
- **The only way to ensure that your email is making it to your customer's inboxes is to get access to accurate data about your email activity – information that ISPs can't provide.**
- **Ensuring that your email is delivered is a lot of work.**
- **You need to be on top of your reputation, make sure your mail streams are authenticated, manage a complex infrastructure and monitor your sending activity.**
- **Plus you need to take care of that critical detail: send the emails your customers want.**

SendGrid knows this is a lot to ask of any business. Leave the deliverability to us and focus on sending those great emails to keep your customers happy and engaged. We handle ISP monitoring, authentication (DKIM, SPF), feedback loops, dedicated IP addresses and other services to ensure your reputation is spotless and your deliverability rates are high.

If you have questions about this report or would like to hear how SendGrid can improve your email delivery and performance, please call 303-552-0653 or email contact@sendgrid.com.

Take control of your email, contact SendGrid today.

SendGrid
Email Delivery. Simplified.