Mail Server

35 Best Practices to Improve Email Deliverability

What is email deliverability

Email deliverability can be understood as a likelihood that your email will be delivered to the inbox of your recipient. There are many aspects that influence whether the email will be delivered or not.

Why should you care

Marketing has a huge potential and great possibilities to be creative when reaching your customers (or potential customers).

But in order to reach those people with your top-notch campaign, your email actually needs to land in their inbox.

The global inbox placement rate is around 85% , which means that about 15% of the emails worldwide never reach the inbox of their recipients.

You should pay attention to the following metrics when you track your overall email deliverability:

- 95% and higher is considered to be a good delivery rate on behalf of an email service provider.
- The bounce rate shouldn’t be higher than 3%.
- In terms of the SPAM rate, you shouldn’t be ringing the alarm bells as long as it doesn’t exceed 0.08%.

Infrastructure

1. Use dedicated IP address

Always keep in mind that if you share the sending IP address with the others, their behavior may influence your deliverability too.

If you do not send thousands of emails monthly, it is not a big deal if you use a shared IP address, as it is much less expensive. If, however, you rely on marketing heavily, you should invest in a dedicated IP address to make sure there are no other users who could negatively influence your reputation.

2. Use different IP addresses for different email types

Another thing you might consider is to set separate IP addresses for your emails and transactional emails.

This is a best practice to make sure that your campaigns won’t influence the deliverability of the essential emails such as password recovery or purchase

confirmation.

3. Don’t change your IP address

If you have deliverability issues, the first thing that probably comes to your mind is to change the sending IP address to start again with a clean slate.

However, it may not be a good idea – this kind of behavior is very suspicious and it may not solve your problem at all. Since switching IPs is a common tactic used by spammers, new IPs are always treated with caution. Spam filters always consider the age of the IP as well as the sending permanence.

4. Warm-up your IP address

If you need to change your IP address (or you start with a new one), make sure to warm it up first. This means that you don’t start sending large volumes of emails from the start. Instead, you gradually increase the number of emails in order to establish the initial reputation. Warm-up is usually not necessary if you use a shared IP address.

There isn’t a rule or exact number. It’s a matter of testing and evaluating. If you ever hit Google’s quota , or start seeing bounces higher than 5%, we recommend to step back to the previous limit and wait for another week.

Only companies with huge sending volume that reaches 1.5 M emails per month start using their own dedicated IPs and start warming them by themselves.

5. Secure your servers with TLS

Transport Layer Security is a type of encryption that is applied to the email to protect it from being read by unwanted party during the process of sending (from the moment it leaves the sender until it is received).

Some email servers may prefer the TLS-encrypted emails, so it is always good to have this protocol enabled in order to maximize your deliverability.

6. Authenticate your email

Email authentication is a process of improving the delivery and proving the credibility of emails by implementing protocols that verify the identity of the sending domain.

There are three fundamental protocols that serve to determine who you are – SPF, DKIM, DMARC. They function as gatekeepers who identify you and decide whether you are a legitimate sender.

Sender Policy Framework (SPF) is a DNS record that informs the provider which IP addresses are allowed to send from your domain.

Domain Keys Identified Mail (DKIM) is an encryption method ensuring that the sent and received message is the same, thus preventing the stealing of the identity.

Domain-based Message Authentication, Reporting Conformance (DMARC) record indicates the presence of SPF and DKIM protocols and tells the recipient what to do if these two authentication methods fails. It reduces the exposure to harmful an fraudulent messages.

7. Subscribe to feedback loops (FBL)

This rule is pretty simple and obvious – do not send emails to those who marked you as spam. If somebody marks your message as spam or trash and you send him another email anyway, your reputation score may suffer considerably.

Most internet service providers offer a service called feedback loop (FBL) that will let you know if your email was marked as spam. Once you are alerted, you should remove the contact from your mailing list immediately. Most mailing services (like SendGrid, MailChimp or Zoho) do this automatically for you so you don't have to manually remove the contacts. All in one FBL service .

8. Set up postmaster@ and abuse@ addresses

Having these two role accounts is a best practice and a requirement by some internet service providers. They are used to receive abuse complaints so you should check them regularly and resolve all the issues as soon as possible.

9. Use domain that is able to receive email

Your sending domain should be able to receive emails, otherwise, the ISP may automatically block your email. Therefore, don't forget to have a valid MX record associated with the domain.

Anybody getting an email from you should be able to reply to the same email address. Besides, having a "no-reply" address may evoke an arrogant attitude – "We want you to hear from us, but we don't want to hear from you".

Sending behavior

10. Never purchase emails

Purchasing email lists is a bad idea. People on purchased lists are more likely to mark you as spam and damage your reputation. Spam complaints are responsible for up to 20% of email deliverability issues. Also, purchased lists are full of spam traps.

Not to mention the fact that these people are simply not interested in your product and the engagement level is very poor. There are many better ways how to spend your money.

11. Always have consent

Even if the email address is not purchased but given by its owner, make sure everyone you mail to is happy to receive your messages.

If somebody gives you an email to register to your service, it doesn't mean he is interested in your monthly newsletter. The same applies to giveaways or lead magnets.

Every single subscriber on your list should have given you explicit permission to email them the specific type of email.

Instead, employ ethical email list building strategies. It is better to have a handful of happy recipients that thousands of people who are not interested into your emails.

12. Don't be afraid of unsubscribes

As we mentioned in the previous point, quality is much more important than quantity when it comes to mailing lists. If someone doesn't want to receive your emails anymore, make it as easy as possible for them to unsubscribe – otherwise, they will use other options (junk, spam folder).

The best practice is to have an unsubscribe button at the bottom of every email you send. Do not require login, do not force the contact to fill in a lengthy form explaining why they don't want to hear from you anymore (or at least, make sure the form is optional).

If someone doesn't want your emails, you shouldn't want to have them on your list. An easy option to unsubscribe is good both for you and user.

In fact, 43% of people mark emails as spam just because they can't easily locate the unsubscribe link or the process is too difficult.

13. Use double opt-in

To make sure you are really sending only to those who are interested in your emails, you can go even further and implement a double opt-in. It is considered a best practice in marketing to prevent from sending to people who did not give a clear permission – e.g. if person A signs up person B for a marketing newsletter on a certain website.

Double opt-in simply means a second confirmation of the email preference that is send to the recipient's inbox and has to be confirmed. Only after this action, the contact will be added to the mailing list.

14. Be consistent

It is important to be consistent and stick to the sending schedule, both regarding the volume and frequency.

Create a plan and stick to it. The best practice is to send one or two emails per week. If you select a certain time, people will being inactive for a month and then start sending 3-4 emails a week is very suspicious and may lead to a lower sender score given by the ISPs. The same applies to rapid spikes in the volume of contacts in your sending list.

15. Be careful about spam complaints

Being actively marked as spam by the receiver of the email is one of the strongest signals for ISPs to lower your sender reputation. One of the reasons for being often marked as spam bay be an absence of the unsubscribe link.

You should check the spam complaint statistics regularly and keep the spam complaints low. Of course, it is very hard to keep the rate at 0% but in general, try to keep the spam rate below 0,1% (for example, a spam complaint rate higher than 0.08% already affects your deliverability in Gmail).

Here is an exhaustive article about spam complaints where you can learn about all possible reasons people send complaints, how complaints impact deliverability and how to address them.

16. Avoid being blacklisted

There are hundreds of publicly available blacklists that gather the email addresses that are “confirmed” spammers. Most often, the are based on the spam complaints and spam traps hits.

Some of the blacklists only last for a day or two. Other custom blacklists have longer bans and ISPs check them as one of the ways to find unwanted senders. You can use a blacklist checker tool to see whether your email address is on any of them.

If you’re on a blacklist, think about the reasons why it happened and fix the issue. Then contact the list owner with the request to delist you.

Of course, the best strategy is prevention. Avoid being blacklisted by following the best practices stated in this email deliverability guide.

Assess the quality of your IP here and here

17. Avoid spam traps

A spam trap is an inactive email address owned by the ISPs. They use these accounts to catch and punish malicious senders as they are sure the email address could not have been obtained in a regular, legitimate way.

Sending an email to a spam trap is usually a one-way ticket to a blacklist. You are very unlikely to get one into your email list if you stick to the ethical ways of getting email contacts. Again, never purchase or harvest.

There are two types of spam traps:
• Pristine email addresses
• Recycled email addresses

Pristine addresses are brand new accounts, added to your email lists by spambots. Recycled email addresses have been reclaimed by the ISP, usually after 180-270 days of inactivity. Hitting pristine spam traps means you have bad email collection practices, while hitting reclaimed addresses means you're not cleaning up your mailing list.

18. Keep the bounce rates low

An email bounce happens when an email can't be delivered to an email address.

A hard bounce is a permanent error, meaning that email is not good for the indefinite future. You should remove hard bounce email from your list immediately.

A soft bounce is a temporary error. Some of these can be saved and re-added to your campaign. However, don't resend to soft bounces immediately. Wait for one or two days until those full mailboxes are cleaned and those faulty servers are repaired.

If an email soft bounces too many times, you should treat it as a hard bounce and delete it from your active list.

19. Keep an eye on the engagement

The engagement level of your email campaigns plays a role in your reputation as well. ISPs want to see proof that the messages you send are enjoyed by the people receiving them.

To do this effectively, you must have a deep understanding of your list and what they're looking to get out of your emails. You also must do your best to provide personalized experience for each of your subscribers.

A poor reputation most noticeably manifests itself in low open rates. Take some time and analyze your email data.

If your open rate is significantly below the general average of (usually around 15% – 25%) or steadily declining over your last few campaigns, there's a good chance your sender score has been damaged and you need to change your sending practices.

If you are seeing a low or non-existent click-through rate (the average is 2.5%), then you need to adapt the content within your email.

20. Get rid of inactive subscribers and role accounts

If someone doesn’t open a single email from your for a period of several months or even more than a year, they are probably not interested in your emails or the email address is no longer used.

Set a reasonable time period and clean your lists from inactive contacts to make sure you keep your engagement levels high. The same applies to role accounts such as sales@domain.com or fake emails such as test@test.com.

21. Verify your list

An email verification tool will help you to find and get rid of all spam traps, hard bounces, typos and disposable or catch-all emails.

Studies show that the average email base consists of 60% of dead leads due to subscribers changing occupations, email providers and more. It means that, for most companies, 6 out 10 subscribers will never even receive the emails they send to them.

While you have no control over when a subscriber changes their email address, you can control whether you keep emailing them or not.

Thus, it’s imperative that you clean out your list by removing hard bounce email addresses and email addresses of the recipients who complained.

By using an email verification service like Email List Verify, you can quickly and easily purge these dead addresses from your mailing list so that you receive less bounces and your reputation isn’t constantly being damaged.

Statistically, 30% of subscribers change email addresses once per year.

Pro tip: when you migrate from one marketing platform to another, at first migrate your best contacts who are constantly opening and clicking your emails and start sending to them only.

22. Be careful with the re-engagement campaigns

The re-engagement campaign is an email campaign in which you try to return the contacts that were once active but become unintersted over time.

These campaigns are rsiky – they can have a high spam complaint ratio and very low engagement. It is a good practice to use a separate IP address for these type of campaigns so that their failure won’t hurt your primary sender score.

Content

23. Format your email properly

There is an old debate of plain-text emails vs. HTML emails. Both have some advantages and disadvantages , but people tend to prefer nice, formatted emails with images. HTML emails won't hurt your reputation, but you must make sure the code is clean. Broken HTML tags are easily detected by ISPs and will hurt your deliverability.

As a compromise, you should offer a plain text version of every HTML message you send. This will ensure that email providers like Gmail and Outlook don't automatically place your message in the spam folder

Smart marketers are now switching to a light HTML format for their emails and tend to avoid using images in their emails altogether for two reasons.

24. Balance the image and text ratio

Emails with too many images can damage your email deliverability. First off, some email clients can't read HTML or images in emails. If the prospect can't understand your email, you're not going to convert.

Also, emails solely comprised of one big image are suspicious to ISPs. Many marketers use image-text to try and dodge the spam filter. However, the ISPs have caught on. Spam Assassin recommends a minimum of 60% text and a maximum of 40% images in your email campaigns.

25. Segment and personalize the emails

We already mentioned that it is good to segment the emails into promotional and transactional/administrative emails and use different IP addresses for them.

However, you can take the email segmentation even further. You can segment your contacts based on many other aspects (gender, age, engagement). Divide your list into smaller segments and add a touch of personalization to your emails.

This will increase the open rates of your emails and you won't send exactly the same message to all your contacts, which is something that may alert ISPs, if done in large scale.

Use spin syntax if your lists are bigger than 300 people (e.g. where you have 4 different intro lines and they will spin in random order).

According to Accenture , 91% of people are more likely to buy from companies that send personalized emails.

Use liquid syntax for ultra-personalization (e.g. when you want to automatically change intro lines for different audience verticals).

26. Limit risky words

Spam filters analyze your content. Limit risky words. On that note, don't make

misleading claims either. Under no circumstances should the subject line state that a prize has been won, only for the content of the email to state the conditions for redeeming the prize.

Here is a list of risky keywords you should avoid using in your emails collected by Mailjet .

Here are 455 examples of the phrases you just shouldn't use in your emails.

27. Link to quality sites

Linking to a shady site is one of the fastest ways to be filtered as spam. If you want to link to an external source, make sure to link to a website that has a good reputation.

Another important thing to consider is the number of links in your email message. Too many links may look suspicious.

28. Don't use link shorteners

Don't use link shorteners in your emails. They are great for sites like Twitter, where character count is of importance. However, in email messages, they may lower your sender score as are often used by spammers to hide shady links.

29. Avoid deceptive subject lines

Open rate is an important metric, but you should not try to improve it artificially. If your subject line is "100% Free $50 Visa Gift Card", you're going to get a lot of opens. But if you don't satisfy the reader, you're going to get marked as spam. A strong offer is useless if you betray expectations and trust.

Keep your subject line between 35 to 50 characters long. The longer your subject line, the more likely it will be flagged as spam.

Do not use ALL CAPITALIZED WORDS in your subject line or body.

30. Avoid excessive punctuation

Using caps in your email is like shouting. It's bad practice and it irritates people. It's also not recommended to use excessive punctuation, such as multiple exclamation marks.

31. Copy gets to the point

Customers often scan emails rather than read them in full detail due to busy lifestyles. Use headlines, sub-headlines, call-outs and bullet points that break up text for quick scanning.

Based on eye-tracking we know that most people scan more than they read
• Average time to capture a user’s attention: 2 seconds
• Once you have their attention, average time spent on the email: 51 seconds

32. Messages are formatted for viewing on mobile

Mobile rendering can often be very different to the desktop views. With the number of people reading emails on mobile devices increasing it is important to make sure your message is easily readable and actionable.

65% of emails are opened first on a mobile device, it’s now imperative that you create a mobile friendly version of your email.

It’s also a good practice to not embed video in your emails. It’s better to include the link to the video instead of embedding it.

33. Physical address and phone number in the footer of the email

This is to help demonstrate that you are a real live company, with a real physical presence. Many ISP’s and 3rd Party Authentication companies require this for Whitelisting.

34. Brand Your “From” Field

It's always better to have a friendly text in the "From" field rather than an email address alone. But do not use a generic text like "Customer Service" or "Sales Department."

Include your name instead: "Julia from GlockApps", "GlockApps Customer Service", "GlockApps Sales Department." A "From" field without your brand is automatically suspicious.

Never use an email like noreply@yourdomain.com in your reply email field. It's not illegal, but it's a bad marketing practice that hurts your deliverability.

Some ISPs, network spam filters, and customers' personal email security settings are set up to move messages with "no-reply" addresses to the junk folder.

It's also a question of ethic. By not allowing the recipients to reply to your email campaigns, it makes you look like you don't care about them. It's a one gate play when you can blast them with emails and they can not communicate back. And it increases the likelihood they will report your email as spam.

35. Avoid Base64

If you don’t know what base64 is, you’re probably not using it. If you are using it – STOP.

Mail Server

Spammers use base64 to hide email content from filters. Emails with a base64 encoded body or subject line are much more likely to be flagged as spam.

Unique solution ID: #1019
Author: Kovalchuk Evgeny
Last update: 2024-01-25 07:13