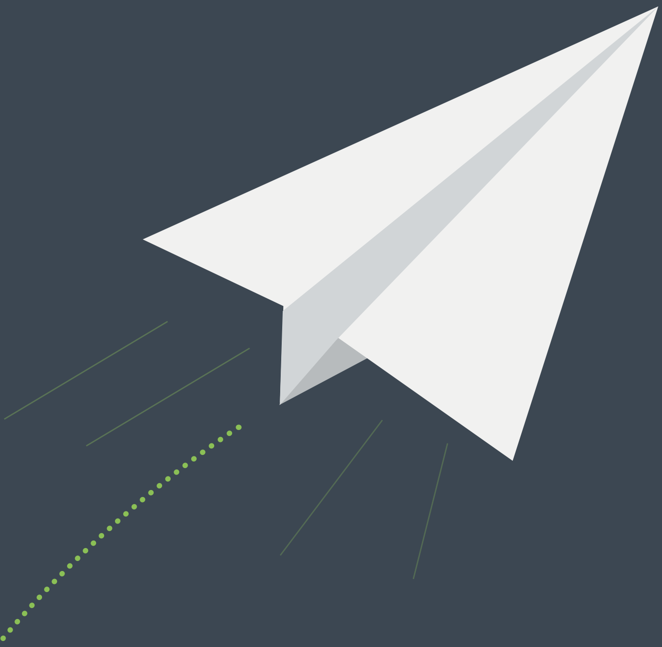

Email Deliverability: A best practice guide on how to avoid spam filters.

engage HUB

Customer Email Guidelines.

No matter how much time and effort you put into crafting your email campaign, it won't succeed if the emails go straight to spam. In other words, email deliverability is key to success.

How do you reduce the risk of getting caught by spam filters?

Not only are there best practices around this, but there are also data protection regulations you must comply with. These guidelines outline the steps you should follow to protect your campaigns, your own reputation and the Engage Hub platform's reputation as an email sender (which in turn protects your delivery quality).

Contents.

1. Permissions & Opt-ins

When you get permission before sending emails (called opting in), your recipients are less likely to unsubscribe or mark you as spam. This improves your reputation as a sender, which in turn boosts your deliverability.

Not only is it best practice, but you're legally required to obtain recipients' consent. If you're collecting opt-ins and storing related data, you should make yourself familiar with the General Data Protection Regulation (GDPR), which comes into effect on 18th May 2018.

GDPR is specific about how to obtain and manage consent (learn more about how to comply). As per the guidelines, you obtain an opt-in by asking people to tick a box when they register on your website or for a service. Historically, people were presented with a pre-ticked box, which they had to un-tick if they didn't want to receive email. However, from May 2018, people must actively tick a box to opt in. Even if you're sending email to people outside the EU, we recommend following this procedure because it means people are less likely to unsubscribe or send your email to spam.

2. Double Opt-ins

Simply having your recipients tick a box isn't enough. You must have what's called a double opt-in. Here's how it works. Once someone has entered their email address, ticked the opt-in box and submitted the form, they receive an automatic email. This email asks them to click a link to validate the opt-in. Only after the recipient has clicked the link is their email address added to your list.

Double opt-in has two benefits. First of all, it ensures people haven't signed up inadvertently (again, reducing the risk of unsubscribes and spam designations). Secondly, it guarantees people enter their email address correctly, keeping your database cleaner. Using a double opt-in process is therefore more effective than a single opt-in one.

3. Opt-in Refreshing

Approximately 20% of email addresses churn every year, so more than 50% of addresses on a 3-year-old list won't work.

Avoid sending emails to lists you haven't used in a while. Not only will you have a high bounce rate, but recipients may not remember signing up. Start by using a list washing method to identify invalid addresses. Then, best practice is to send an email requesting people to opt back in to receive future communications from you.

4. Opt-outs

You're legally required to have a functional opt-out link on every email communication you send. And don't make the link hard to find because this increases the likelihood of email going to spam.

Opt-outs should be erased from your database, not just set aside. We also recommend you set up a robust list management process to ensure opt-outs can't be contacted via another channel.

5. Communication Preferences

You should give your recipients the ability to choose their communication preferences. Not only does this protect your reputation as a sender, but it also leads to higher engagement because people only receive relevant emails.

6. List Acquisition & Management

On the face of it, email can seem like a numbers game – the more people you communicate with, the more opens and clicks you'll get. But this isn't the case, so avoid the temptation to purchase lists. When you use a bought list, you're contacting people who haven't opted in to receive your emails. Therefore, there's a very high chance you'll be caught by spam filters and/or blocked (not to mention the implications for GDPR compliance).

Also, don't continually contact people who don't open your emails, because servers will flag you as a spammer and block you.

7. Spam Traps

Spam traps are a spam control method. They're email addresses that aren't actively used but are actively monitored. They look like real addresses but don't belong to real people and aren't used for actual communication.

Email clients and blacklist providers commonly use spam traps to catch malicious senders, but quite often legitimate ones with poor data hygiene or acquisition practices end up on their radar as well.

If you buy a list or use a scraper to get emails and then encounter a spam trap, your deliverability will plummet.

8. Domain Mismatch

Domain mismatch occurs when the domain on an SSL certificate isn't the same as the URL that appears in the address bar when someone clicks a link. Spam checkers look at links and their domains as part of their scoring process. It's estimated that 45% of emails that go to spam are caught for this reason.

Be sure to check all your links before scheduling an email, including the unsubscribe link (which is frequently overlooked).

9. Email Content

Many elements in the email itself can trigger spam filters. Here are 9 ways to optimise your email content for deliverability.

- Make sure the sender is recognisable: If recipients can't work out who's sending the email, they're more likely to assume its unsolicited and mark it as spam.
- Keep your subject lines clear and concise: If they're too long, they risk being cut off (80 characters is a general guideline), and that increases the risk of being seen as spam because people aren't clear on what your email is about.
- Avoid trigger words: These are words and phrases that spam filters look for. Examples are free, £££,100% satisfied, investment and winner. Also avoid using all uppercase letters and over-using punctuation. There are many lists of trigger words readily available online.
- Personalise subject lines and content: Where possible, use CRM data you have, like first name, account number or package plan.
- Optimise preheader text: This is a short summary you see alongside the subject line before opening the full email. Many mobile, desktop and web email clients use them to give you a quick preview of the email contents. The preheader is usually limited to around 100 characters and is a way to boost open rates (and decrease the likelihood of people marking your email as spam).
- Avoid attachments: Not only does this slow the throughput of your email campaign, but it also makes you more likely to be caught by spam filters. Best practice is to include a URL within the email instead of an attachment.
- Avoid image-only emails: These are generally very large, take a long time to download, aren't well indexed and don't render well on multiple devices. And remember: some email clients block images by default, so even if the email does get through, people may not see them. It's therefore best to have a good image-to-text ratio and to ensure the email is comprehensible without images.
- Remember to add alt text for all images: This is a short description that appears when an image doesn't display. When you have alt text in place, it's easier for recipients to understand your message when the images aren't there.
- Spell-check your emails before sending: It sounds obvious, but emails with misspelled words are more likely to be marked as spam (in addition to reflecting badly on the brand).

10. IP Reputation

According to Return Path, 83% of email delivery failures are caused by problems with reputation, so protect yourself from the very beginning. Don't send thousands of emails at once because you will instantly trigger spam filters, especially with top service providers. Instead, start small and scale up – send your email to 100 people in the first batch and 200 people in the second. This will warm up your IP so you don't damage your reputation. If you need multiple IP's you should follow the same warm up process for all IP's. Starting small provides a chance to pause or slow down sending and adjust the strategy before any reputation is seriously impacted.

The following table is a schedule which we recommend as a safe approach for IP warming. On day one the send includes 5,000 emails and this amount is doubled every second day.

Day	Volume
1	100
2	200
3	300
4	500
5	800
6	1,300
7	2,100
8	3,400
9	5,500
10	8,900
11	14,400
12	23,300
13	37,700
14	61,000
15	98,700
16	159,700
17	258,400
18	418,100
19	676,500
20	1,094,600

The above table is a blanket safe approach and assumes an even distribution of service providers within the data base. If the data base does not have an even disruption of service providers and favours one over the many others then naturally this table schedule will change. We recommend that if there is any doubt on how best to warm up your IP that you speak with the Engage Hub team who will review your data base and provide a recommended schedule for you.

11. Domains & Sub-domains

Your chosen domain and sub-domains need to be dedicated to your campaign, so they're free from previous or current usage. A domain or sub-domain that's already been used can create issues with reply handling because you may have difficulty determining which replies are for which campaign.

12. Hard & Soft Bounces

There are two different types of bounce: hard and soft. Typically, a hard bounce is when there's a permanent delivery failure, whereas a soft bounce is when the failure is temporary.

Hard bounces include:

- Recipient email address does not exist
- Domain name does not exist
- Recipient email server has blocked delivery

Soft bounces include:

- Mailbox is full
- Recipient email server is down or offline
- Email message is too large

To help avoid spam filters, you should apply rules to reduce the amount of bounces. For example, one hard bounce and the email address is automatically blacklisted. Or it's automatically blacklisted after five soft bounces.

13. Litmus Testing

People open emails on many different devices, so
you should ensure your emails render correctly on all of them.

Engage Hub has integrated with Litmus, a global leader in device testing, to make this easy. Litmus scans your email, testing it for different devices and major spam filters. It then flags potential issues, so you can fix them before sending. We strongly recommend you use this functionality.

engageHUB

sales.enquiries@theengagehub.com
+ 44 (0) 20 7183 3860
www.engagehub.com