

8

Tips To Prevent Emails Ending up in Spam

■ TABLE OF CONTENTS

Introduction	pag. 3
Don't buy mailing lists	pag. 4
Periodically clean up your contact list to not end up in spam	pag. 6
How to use opt-ins to avoid ending up in spam	pag. 8
Email authentication to avoid ending up in spam	pag. 10
Take care of your IP reputation	pag. 12
Write good content to avoid ending up in spam	pag. 13
Track the emails you send, and consult the statistics to improve your results	pag. 14
Use a professional SMTP like turboSMTP	pag. 15

INTRODUCTION

Whatever kind of work you do, whether you're sending out large email marketing campaigns on behalf of a retailer or pushing out pitches for a non-profit, you want to be able to **keep your emails out of the spam folder**.

So why do some emails end up in that spam box?

There are two possible reasons. Either the recipient has marked your message as spam; or the email client has identified something suspicious in your message, perhaps because you've sent a generic and massive mailout without professional support.

Making sure that your message reaches the recipient's inbox safely is essential for the success of any communication, especially commercial emails. If your contacts aren't receiving your newsletters, offers, and campaigns, it might be because you're not practicing these eight simple tricks to **prevent your emails from ending up in spam**. Let's see together how to prevent your messages dying unseen in the spam folder.

DON'T BUY MAILING LISTS



Buying contact lists is a bad idea for three reasons:

- The list won't be structured or targeted, with profiled contacts divided in groups and chosen in a coherent manner.
- You can't find spam traps among purchased addresses.
- It increases the chances of your message ending up in the spam folder.

Building a contact list is an important preliminary activity that guarantees high returns for your communication campaigns. It's why you need to take the time to collect ethically contacts who are really interested in your services, brands, and products. User reports and an encounter with a spam trap (an email address that seems normal but is actually a trap to identify spammers) could permanently affect your sending reputation and your deliverability.

Why is buying email lists a mistake that can put your message in the spam folder?

Your IP or domain reputation depends on your behavior. When you buy a mailing list you are choosing to send messages to users who have not consented to receive them. That choice increases the chance of email recipients marking your content as spam. You will no longer have access to their inbox, and your emails will go straight to the spam folder.

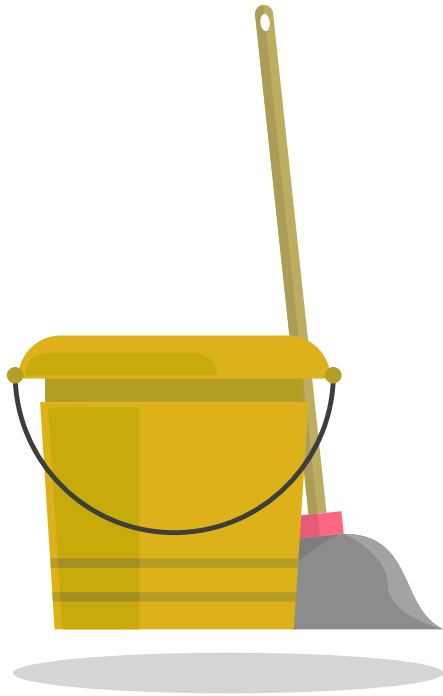
Collecting email contacts for your lists is a long and tiring job. But to get results, you must do it correctly. There are no shortcuts and any attempt to speed up the process can be harmful. **To prevent your emails ending up in spam** due to “unauthorized” contact lists, not only should you not buy mailing lists, but you should also avoid:

- Sharing your lists
- Email scraping

Sharing lists can seem harmless behavior, especially if you do it with a “trusted” business partner. In reality, it is not a good way to avoid spam and is unethical. It violates the agreement you made with subscribers and increases the risk of your emails being marked as spam. A valid alternative is to recommend your partner in the text of your newsletters, insert their subscription link, and suggest that they reciprocate.

Email scraping (or email harvesting) is one of the most dangerous email marketing activities, and is often carried out by spammers. It involves collecting and extracting email addresses from websites through bots. It’s clearly wrong and will harm the reputation of your sending address.

PERIODICALLY CLEAN UP YOUR CONTACT LIST TO NOT END UP IN SPAM



Because your contact list is so valuable, you should create and grow it with the right methods. Above all, keep it under control so that it contains contacts that can guarantee the highest engagement rate. We recommend that you periodically clean up your list by deleting:

- Inactive contacts (people who do not open your emails).
- Generic contacts that indicate a “role” rather than a physical person (such as support@, admin@, and so on).
- Invalid or non-existent addresses that generate hard bounces.
- Contacts who rarely interact with your content.

Your contact list must obviously also be free of wrong addresses and spam traps. To find these emails and delete them, use professional cleaning tools such as the [turboSMTP email validator](#) that let you perform a complete screening of your lists.

The advantages of cleaning your lists are clear. Spam traps may land you on the world’s major blacklists. Non-existent addresses, such as misspelled addresses, can make you waste turboSMTP credits. The reduction of soft and hard bounces will improve your deliverability.

You can use the [tracking feature](#) to identify people who never open your emails. You'll be able to remove inactive contacts such as subscribers who rarely interact with your content, or who didn't open any of your last ten emails. You don't need to email people you haven't contacted for more than six months.

So how often should you clean your email list? The frequency will vary from list to list but every three to six months is a good rule of thumb— and definitely not longer than a year.



So how *should* you collect contacts for your mailing list? By ensuring that users voluntarily subscribe to your list by completing the appropriate form on a dedicated landing page on your website. Voluntary subscription to a newsletter takes place through a process called “opt-in.” It’s a path that, with one or more steps, allows the user to enter their data then authorize you to send them email communications. There are four types of opt-in:

- Single Opt-in
- Pre-selected Opt-in
- Notified Opt-in
- Double Opt-in

The **Single Opt-in** is a simple registration. The user enters their email address into a signup box. This is the least secure method to acquire contacts because it does not require any confirmation from the user. Because you can’t be sure that the subscriber really wanted to receive your communications it increases the chance that your messages will be marked as spam.

For **Pre-selected Opt-ins**, the registration checkbox is pre-selected. The user just needs to click to confirm. They'll then receive a confirmation email at the address provided.

The **Notified Opt-in** provides for the sending of a “welcome email,” or a series of welcome emails. These generally guarantee a good engagement rate and help assess whether the contacts collected are really interested in your content.

The last option is the **Double Opt-in**. The user signs up, then receives an email with a link they must click to confirm their registration for your newsletter.

In order to **avoid your emails ending up in spam**, the Double Opt-in is the best choice. The double confirmation lets you collect contacts who are really interested in your emails and who are unlikely to report them as Spam.

To further increase the security level of your list's contact collection, you could also consider using a **reCAPTCHA**. The extra step will verify that the subscribers are real and **not spam bots**.

Remember, to have a clean and safe contact list, users must be able to sign up easily but also unsubscribe with equal ease. Many people think that by making the UNSUBSCRIBE button almost impossible to find, they'll have a much richer and more profitable mailing list. That's wrong. Better lose an uninterested user than win a spam report!

You can design and activate an **unsubscribe link** in your email footer. A contact who no longer wants to receive your communications can just click the link, and [turboSMTP will automatically](#) stop sending emails to their address. It makes your **list management** very easy.

EMAIL AUTHENTICATION TO AVOID ENDING UP IN SPAM



Email authentication lets you increase your sending reputation and improve both deliverability and server security. Because inbox providers use an authentication system that verifies the sender's identity, it is much easier to pass a provider "test" with an authenticated email address.

Email authentication protects you and your recipients from spam, phishing, and spoofing. With the addition of SPF, DKIM, and DMARC records, you get an even more secure system.

SPF

SPF (Sender Policy Framework) is a standard authentication that guarantees that the sender is reliable and not a copy created to harm the recipient with spam and phishing.

DKIM

DKIM (Domain Keys Identified Mail) allows a domain to associate its

name with an email through a digital signature that guarantees that the message, including its content and any attachments, has not been modified.

DMARC

Once a message has passed the SPF and DKIM checks, the DMARC (Domain-based Message Authentication Reporting & Conformance) protocol intervenes and acts as the last “controller.” It verifies that the DKIM signature is valid and that the FROM field matches the name of the domain and the IPs declared in the SPF records.

TAKE CARE OF YOUR IP REPUTATION



A number of factors can affect your IP reputation and cause it to risk blacklisting. If you send a lot of emails (for example, if you are struggling with an email marketing campaign) you could risk having your emails marked as spam. You might send emails to addresses that do not exist, and stumble on spam traps. All of this could cause your IP address to be blacklisted, with serious consequences for your deliverability. What can you do to **prevent your emails from ending up among the junk**? In addition to cleaning your contact list and not buying lists, you can also take these three precautions:

- Choose the Double Opt-in registration method with instant verification of the email address provided by the subscriber.
- Take care of the content and form of your messages, and avoid spam trigger words such as exaggerated claims or excessive promises, capital letters, and too many exclamation marks.
- Send emails focusing on the engagement goal, profiling the contacts you have available, and structuring customized content that they find genuinely interesting.

Paying attention to your IP reputation will help you reduce the spam reports and avoid the spam folder.



To ensure that your recipients do not mark your email as spam, try to offer them original and interesting content. Avoid too much text; users will only devote a few seconds to deciding whether to read your email. And create responsive emails that are easily displayed on any mail client or device.

To optimize the content for the provider and increase your chances of avoiding the spam folder, consider these simple tips:

- Make sure you give your emails a responsive design. That will earn you points as a respectable and aware sender even for the ISP.
- Contextualize your message. Try to give the ISPs as much information as possible about your content. Optimize and describe your images, for example.
- Choose a dedicated service, such as turboSMTP, that maintains stable relationships with Internet providers to avoid being blacklisted and protect your deliverability.

Remember, the more you can contextualize your message, the more the provider will be able to recognize and categorize it without putting it in the spam folder. Content incorrectly presented might not reach inboxes, even if the recipient wants to receive them, because of action taken by the ISPs!

TRACK THE EMAILS YOU SEND, AND CONSULT THE STATISTICS TO IMPROVE YOUR RESULTS



To evaluate the success of your communication strategy, track your results with a professional tool. Note who interacts the most with your content, delete inactive contacts and, in particular, follow the trend of these metrics:

- Opening rate
- Delivery rate
- Click-through rate (CTR)
- Spam score

If you want to avoid **ending up in spam**, it is important that you have a clear idea of the number of people who receive your email in their inboxes, how many people read those emails, and how many click on the internal links or your attachments. Only by periodically analyzing this data will you be able to clean your contact list, improve your content if they do not guarantee you a certain engagement, and try another registration method, such as the double opt-in, for better data collection.

USE A PROFESSIONAL SMTP LIKE TURBOSMTP

Every email matters but the emails that actually reach the recipient matter even more. If most of your emails end up in spam, it will be difficult to make your offers known to potential customers and give your contacts the right impression of your brand.

Trust between brands and subscribers is essential for the success of any email marketing campaign so you need to take care of your reputation, and avoid actions that can cost you credibility. Professional services can help you choose the best strategies to reach mailboxes and touch your customers' hearts.

You should know that the SMTP servers of standard ISPs are sometimes unreliable. They send your emails through random IP addresses that might be blacklisted. If you want to **make sure that your emails don't end up in the spam folder**, rely on **turboSMTP**. We monitor blacklists and we maintain good relationships with the major providers so that our servers always remain whitelisted.

What are you waiting for?

Reach the inbox, communicate better.

Try it for free now



emailchef.com



newslettercreator.com



sendblaster.com



serversmtp.com



turboexecutive.com



Delivery Tech Corp.
4411 Morena Blvd #230
San Diego, CA 92117