

Why Your Emails End Up in Spam...and How to Keep Them in the Inbox



You [depend on email](#) to send personalized marketing and reach a large number of customers quickly. However, if your emails end up in spam instead of hitting the inbox, you have wasted money and effort. Even more importantly, landing in spam frequently can harm your [business reputation](#).

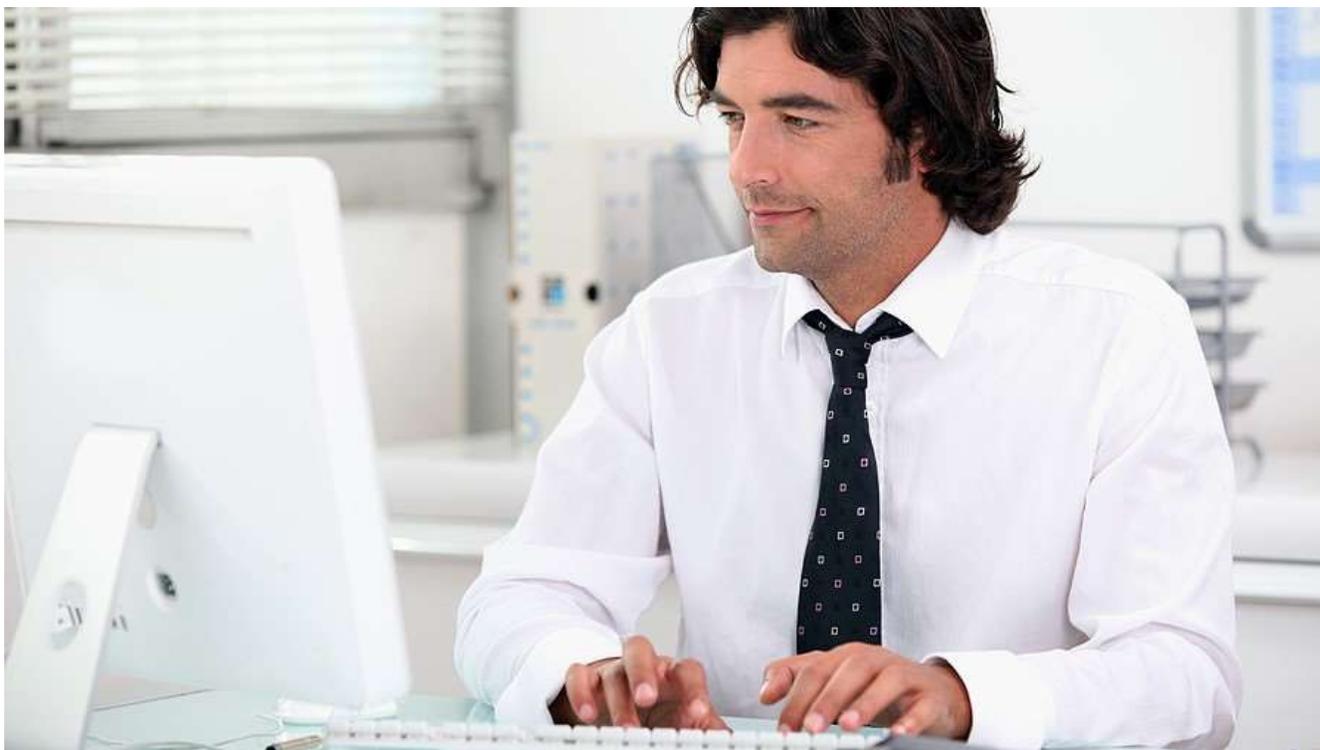
To ensure that future email marketing campaigns deliver results, learn why your emails end up in spam folders. Then follow a few basic guidelines to help keep you in the inbox and promote customer engagement.

6 Reasons Why Your Emails End Up in Spam

Users hate spam. Consequently, governments and email services have begun to crack down. Spam filters look at not only the structure of the email itself but also the sender identity and previous engagement rates. If your emails keep going to the spam box, one of the following may prove the reason.

1. **You have violated spam laws** – The Federal Trade Commission (FTC) rules require marketing emails to include an unsubscribe option. Additionally, “From” lines and subjects must be accurate and relevant, and the email must include a legitimate physical address.

2. **Your email looks like spam** – Certain design and copy elements will alert spam filters. This includes poor spelling or grammar, as well as the use of too many images or trigger words like “free gift” or “earn \$.”



3. **Your email list needs attention** – When emails bounce or recipients unsubscribe or mark an email as spam, spam filters notice. An outdated email list will likely produce too many bounces. Likewise, purchasing email lists spells trouble.
4. **Links and attachments in email send a red flag** – Hackers frequently use attachments and links to trick users into downloading viruses or sharing sensitive information. As a result, spam filters will look for attachments and suspicious links.
5. **Your emails generate low or negative engagement** – The more users engage positively with your emails, the better. However, when users delete your emails without opening them or, worse yet, mark them as spam, that spells trouble.
6. **You have not set up proper authentication** – Email services like Google and Outlook prioritize email from senders with proper authentication through the Sender Policy Framework (SPF).

Get Permission Before Sending

Never send unsolicited emails. This means that recipients need to give permission first. Many businesses include an opt in checkbox when users create an account. Additionally, popup forms on a website home page or product page allow potential customers to sign up for emails. Resist the temptation to purchase email lists.

Include Unsubscribe Option

In addition to getting permission before sending emails, make sure every marketing email includes an unsubscribe option. Typically, the unsubscribe link appears in the email footer, but you can also include it in the header, as well. Not only do FTC rules mandate inclusion of an unsubscribe option, but customers expect and appreciate it.



Follow Email Best Practices for Copy and Design

The [wording and design of your email](#) plays a critical role in user engagement and can make the difference in avoiding spam filters. Keep in mind these basic best practices:

- Word your subject line carefully – The subject line delivers a critical first impression for both recipients and spam filters. Avoid suspicious trigger words, exclamation points, dollar signs or excessive capital letters. And do not include misleading statements.
- Include correct sender information – The display name that appears next to the sender email address must clearly indicate the person or business sending the email.
- Use [professional email writing](#) – Edit email content for spelling and grammar. As in the subject line, avoid trigger words and misleading statements or overly pushy content.
- Avoid attachments and shady links – Only send attachments if absolutely necessary. If you include links, avoid linking to disreputable websites. And make sure that the display URL matches the destination URL.
- Include a valid physical address – According to FTC rules, business emails must include a physical address or PO box.
- Watch your image to text ratio – Using images with little to no text or the use of too many images will both alert spam filters and decrease user engagement.

Conduct Regular Email List Maintenance

Take time to regularly clean up your email list. Remove any bounced emails or recipients who have not opened your emails in a long time. Also remove any purchased email addresses or those that are obviously fake.

Ensure Proper Authentication

Proper SPF, DKIM and DMARC authentication provides assurances to recipients that your emails are legitimate. A reputable email delivery service will help you set up and monitor your [email authentication](#) to maximize email deliverability.

Never Again Ask Why Your Emails End Up in Spam

Emails can play a significant role in your [marketing strategy](#). Choosing the right email tools and services helps to secure your business reputation and get the most out of your email marketing. Contact eMazzanti today to improve [email deliverability](#) and [email security](#) and never again ask why your emails end up in spam.