

e-Mailing: good practices

 **Fix Me!** A1 proofreading not yet effective for this page. In the meantime, you can ask any questions on the [forum](#).



Gestan can send emails to groups of your contacts. Beyond 100 identical emails sent to different recipients, we can start to talk about “mass mailing”.

To send an email, it is necessary to use an email sending service made available to you most often either by the provider of your internet connection, or by the provider of your domain name: this is the service SMTP, or SMTP server.

It is important to respect a certain number of rules when it comes to e-mailing, in order to prevent your recipients from complaining. If you generate too many complaints from your recipients, your SMTP provider may cut off your access to the service.

We therefore strongly recommend respecting the following good practices:

1. **“Confirmed Opt-In”**: you can only send a message to a private recipient if your recipient has expressed prior consent (from the monk in France, and in many other countries). You therefore need a registration process that provides for obtaining this explicit agreement (generally, a registration form followed by explicit confirmation from the recipient).
2. **Maintenance of your address list**: delete any incorrect address from your lists. The higher your error rate, the worse your reputation becomes.
3. **“One-Click-Unsubscribe”**: Provide a link in each message through which the recipient can unsubscribe, if possible with a single click.
4. **Format**: If you send emails in HTML, add a part formatted in text only to ensure that your messages are readable by all your recipients (Gestan does this automatically if your HTML coding is correct).
5. **Message origin**: Specify Insert the location of the recipient's registration. Example: 'You are receiving this message because you registered at www.votredomaine.fr <<http://www.votredomaine.fr>>. In case you no longer wish to receive them, please click here (link).'
6. **Weight of messages**: make sure that you do not send messages that are too heavy. For a mass mailing, a message of 300 KB is a limit that should not be exceeded. 100 KB is a reasonable value. If your message includes images, prefer to include them in your messages in the form of an address. The same goes for attachments.
7. **CNIL registration and collection of personal data**: in France, the possession of any personal file is subject to declaration to the CNIL. It is prohibited to collect personal data without the consent of the person concerned: as such, email tracking is theoretically not authorized

(Gestan does not do this).

Before sending to a large number of addresses (>100), we recommend that you check with the SMTP service you are going to use that everything will go well. Indeed, many SMTP servers are limited in the number of emails that can be sent within a given time frame.

Why are your emails arriving as spam? 7 possible reasons!

Source: codeur.com

1. You use a free domain for your emailing campaigns

Gmail, yahoo, outlook, and other hotmail are not recommended for your email campaigns. Indeed, Internet Service Providers (ISPs) reject grouped emails from these free domains.

They prefer domain names registered by an individual sender, which they can find and whose reputation they can assess.

What to do ? Use your domain name to create an email address dedicated to your emails. This should look like: customerservice@mycompany.com.

So you can build your own sending reputation with ISPs. Not to mention that this practice gives a more professional image to your newsletters.

2. You have not authenticated your emails

One of the main reasons for spam is the lack of proper authentication. It's like when you reject a call because you don't recognize the calling number.

There are technologies to authenticate your emails and increase your deliverability rate. This practice makes your domain trustworthy in the eyes of spam filters. The main email identification technologies are:

- DKIM (Domain Key Identified Mail): provides an encryption key and digital signature to verify your emails.
- SPF (Sender Policy Framework): checks if the sender IP address is trusted.
- DMARC: You must already be using DKIM and SPF.

If you are using a custom domain name, you can implement these authentication methods by adding TXT records in your domain's DNS management.

3. You use words associated with spam

To protect their users from scams, ISPs have a list of spam trigger words. Here are a few :

- Check
- Free or no charge
- Exceptional offer
- Guarantee
- To increase the sales
- Order now

- Without risk
- Special promotion
- Winner
- Money

Text in all capitals, exclamation points and overuse of emojis, as well as grammatical errors, are also reasons to end up in the spam box.

Contact your provider to find out which words raise red flags and make a list of terms to avoid in the subject line.

In general, avoid items that make fantastic promises or offer exceptional offers. Stay measured and factual in your comments.

4. Your emails are not HTML compatible

When you send emails to friends or family, the content is mostly text.

As a business, you should include visuals, animations, one or more call-to-action buttons, and other graphic elements to drive engagement. To do this, you need to write your emails in HTML.

However, you must follow good practices to prevent the design from becoming an excuse to end up in spam:

- Use a maximum width of 600 to 800 pixels for your emails.
- Make sure the HTML code is as clear and simple as possible. Avoid Javascript and Flash languages which are no longer supported by many ISPs.
- Maintain a low image-to-text ratio.
- Optimize and lighten your images.
- Optimize your email for mobile with small images and easily readable fonts.

5. Your emails contain too many attachments

Attachments are often used to spread viruses. Thus, they trigger an alarm with anti-spam filters, in particular `.exe` files.

Your email campaigns should not contain attached files. If you must include one, make the document available on your website or through a cloud storage service like Dropbox or Google Drive.

6. Your emails do not include contact details or unsubscribe links

Physical addresses and unsubscribe buttons help improve the deliverability of your emails. Furthermore, they are essential in managing your brand image.

At the bottom of the page, remember to indicate the contact details of your head office. Same for the unsubscribe link. This must be visible at the top or bottom of your message. If you make it difficult to unsubscribe, subscribers will then mark you as spam so that they no longer receive your messages.

7. You are sending too many emails at once

If you usually send emails to 10,000 subscribers and suddenly jump to 200,000, you risk triggering ISP spam filters. This spike is considered unexpected behavior or even a malicious attack.

So, if you plan to increase the rate, do it gradually to warm up your IP address.



Other Technical articles

[Automatic Application Features \(AAF\)](#)

[Configure Gestan](#)

[Configure the search](#)

[e-Mailing: good practices](#)

[Gestan CS - Client/Server mode](#)

[Gestan data backup](#)

[Gestan on a MAC](#)

[Google SMTP Server](#)

[libcef.dll file not found](#)

[Mail outsourcing](#)

[ODBC on HFSQL](#)

[Online payment](#)

[Reports and Queries](#)

[Rounded](#)

[Send emails with Gestan](#)

[Specific developments](#)

From:

<https://manuel.gestan.fr/> - **Le manuel de Gestan**

Permanent link:

<https://manuel.gestan.fr/en/wiki/tech/emailing>

Last update: **2025/06/24 21:16**