Dialog Insight

PRACTICAL GUIDE ON **EMAIL DELIVERABILITY**

INTRODUCTION

Reaching the inbox is a process much more complex than just hitting the “Send” button. Many systems are designed to filter emails and decide which ones will reach the recipient or not. According to Return Path, only 89% of emails really reach the inbox of targeted recipients. Companies are therefore missing 11% of communication opportunities with their clients. And the explanation for this situation is based on many factors.

The purpose of this guide is to demystify the email delivery process and provide you with solutions to improve your results.

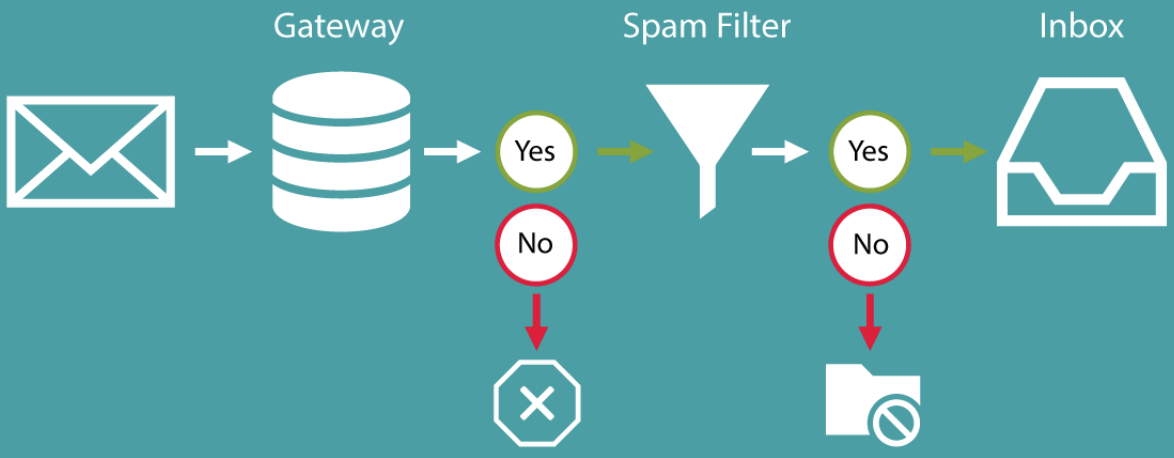
11% of your emails don’t reach the targeted inbox.

– Return Path “2018 Deliverability Benchmark Report ”

REACHING THE INBOX

Many factors can explain why some emails never reach their destination. Here's a diagram that shows the obstacles that an email meets before reaching the inbox.

Emails stopped at the first step (Gateway) will simply never be delivered. This is a server installed on a company's network that works as the first defense against spam. If an email makes it through step 1, it will then be confronted by a spam filter that will decide whether it will be placed in the recipient's inbox or spam folder.



The sender reputation is the main reason why your emails do not reach their destination. This element breaks down into several factors that can be analyzed more precisely to get a better idea:

The engagement ratio of email accounts is one of the most frequent reasons to explain inbox placement problems. Filters analyze and compare the ratio of active and inactive email accounts that receive promotional emails. Engagement is then determined by the number of times a user logs into his account and his activity level (opens and clicks) while connected. Therefore, sending a message to a large amount of inactive email accounts or sending an email to an active account that never takes action on your emails could both result in blocking your subsequent campaigns.

Another main cause of low inbox placement rates is the number of spam complaints received. Spam filters register complaints made by users and directly place future campaigns from the same sender in the spam folder when complaints exceed a certain percentage. Therefore, the more email complaints you generate, the more your reputation is affected and the less likely your emails will be delivered.

Another way your email could be blocked before being received by the recipient is by sending non-responsive emails. So be careful to adapt your mailings so you will not be penalized for it.

Moreover, most email clients use algorithms to compare incoming messages to spam messages, and to detect similar senders, links and contents. Too many similarities could suggest that the email is spam.

Several other elements can also be the cause of poor email deliverability. Among others, we find: a bad email infrastructure, non-certified sender, the ratio images vs.. text in email content, no unsubscribe link, purchased contact list and many others.

IMPROVE DELIVERABILITY

Here are a few suggestions to put delivery performance on your side.

No 1 – SUBSCRIPTION DETAILS

On your subscription offer, specify the type of content you will send and how frequently. This way, recipients will know exactly what to expect by subscribing and will be less likely to mark your emails as spam.

No 2 – DEDICATED IP ADDRESS

A dedicated IP address will ensure control over the quality of all emails you send from this IP address, unlike a shared address. You will therefore be certain that your reputation will not be altered by a careless third party.

43% of email recipients click the Spam button based on the email's "From" name or email address. – Convince&Convert

No 3 – AUTHENTICATION PROTOCOLS

Authentication protocols are used to confirm the sender's identity and therefore pass more easily through the various filters. All legitimate senders should have authentication protocols. The most common are DKIM (DomainKeys Identified Mail), SPF (Sender Protection Framework), and DMARC (Domain-based Message Authentication, Reporting & Conformance).

No 4 – ENGAGING CONTENT

Irrelevant content will decrease the engagement rate, or worse, result in complaints. Send emails that read quickly and contain calls to action. Email providers such as Gmail, Outlook and Yahoo often use open and click rates to determine if emails from a particular sender are legitimate or not. Consequently, an email that is never opened or clicked is very likely to end up in the spam folder.

Also, try to avoid unduly marketing terms (free, offer, promo, urgent, etc.). The content should remember your branding, however, be sure to use images only to support your text (do not abuse it).

No 5 – A INVOLVING EMAIL OBJECT

The email subject is one of the first things the recipient sees when they have to decide to open your email or not. Do not exceed 50 characters because your object will be cut off. Moreover, adding customization provides better opening results. Also test special characters or emojis as it helps you stand out.

No 6 – GOOD LIST HYGIENE

It is very important to keep a close eye on your contact list and to track delivery errors in order to remove non-existing or abandoned addresses. Abandoned addresses are sometimes used by Internet service providers to trap unscrupulous senders. It is recommended to target less people who will be more engaged to maintain a good reputation.

69% of email recipients report email as spam based solely on the subject line. – Convice&Convert

WHAT'S A SPAM TRAP?

Spam traps are used by Internet service providers (ISPs) to curb or reduce spam messages. These addresses can be specifically created to catch culprits that collect email addresses fraudulently, or be recycled addresses that were real addresses before but have been long abandoned by their owners. These existing addresses are used to trap senders that don't keep a clean email list.

Depending on the kind of spam trap the email is sent to, the consequences are different.

The worst thing that can happen to you is to send emails to a spam trap created specifically for that purpose. If that happens, your IP address, or even your domain, will be immediately blocked by Internet service providers. Your delivery rate may decrease drastically upon your first offence.

If you send a message to a recycled spam trap, consequences are less severe. In most cases, your emails will simply be placed in the spam folder. A first offence acts as a warning signal. However, if you continue to send messages to this address, your delivery rate may suffer.

UNDERSTANDING DELIVERY STATISTICS

When your email service provider informs you that your email has a good delivery rate, this, unfortunately, doesn't mean that all recipients got the email, but only that the recipient's server received the message.

The sending server has the task to generate the emails and to send them to each recipient server. Once the message is sent, the recipient's server has 2 choices:

Accept and deliver the message

Reject the message and return an error code

In the first case, the message is considered as delivered when the recipient's server has accepted it. From this moment, the email is no longer on the sender's server. The "signal" is momentarily lost because the email becomes under the responsibility of the recipient's server (Gmail, Outlook, Yahoo, etc.), which will process it and deliver it in the recipient's inbox.

Servers have spam filters, and computers have antiviruses and security configurations. These are all elements that can block email delivery. It is therefore possible that an email gets blocked somewhere between the recipient's server and the recipient's inbox, but that your statistics show a completed delivery.

The delivery time is therefore the time at which the recipient's server accepted the message and not the time it was really delivered in the inbox; this data is actually impossible to get.

The email service provider will be able to recover and provide behavioral data from opens and clicks only when recipients open the email, download images or click links in the message.

In the second scenario (Reject the message and return an error code), the recipient's server returns an error code and, if applicable, the email is identified as a delivery error and an error code, or message provided by the server, is sent. Your email service provider can't do anything else but receive the error and send it to you.

IP addresses appearing on just one of the 12 major blacklists had email deliverability 25 points below those not listed on any blacklists.

– Convice&Convert

CONCLUSION

Email delivery is complex and the rules that can block emails are constantly evolving.

The points described in this guide will help you better manage various delivery issues. It is also important to closely monitor your delivery results in order to react quickly if problems arise.

Dialog Insight has all the necessary resources and expertise to help you improve your email delivery rates. Do not hesitate to contact our team for advice and support.

ABOUT DIALOG INSIGHT

Dialog Insight develops customer acquisition, data analysis and personalized communication solutions that improve the effectiveness of your digital marketing programs.

Our main objective — Offer a successful and top-notch solution that can assist you in increasing your clients' engagement through personalization.

To learn more, visit www.dialoginsight.com

Canada: 1 866 529-6214
France: +33 1 86 76 69 96
Russia: +7 (499) 978-79-36
info@dialoginsight.com