PREDICTIVE™

HOW TO AVOID YOUR EMAILS GOING TO SPAM

by Predictive Response

EMAIL DELIVERABILITY

Best Practices in 2020

EMAIL DELIVERABILITY IS A MOVING TARGET, AND THE PREDICTIVE TEAM STRIVES TO HELP YOU ENSURE THAT YOUR MESSAGES ARE DELIVERED TO YOUR AUDIENCE'S INBOXES EVERY DAY.

There are several steps you can take to keep your email bounce rate low. First let's look at why email messages bounce.

Why do emails bounce, and what can you do to lower your bounce rate?

To protect their users, all major Email Service Providers (ESP) (Gmail, Hotmail, Yahoo, Outlook, etc.) take steps to verify that incoming email messages contain quality content from reputable senders--in other words, they screen content to ensure that their users receive emails that they want to see, with spam, dangerous content, or irrelevant messages filtered or blocked.

Each ESP uses its own internally determined rules to assess incoming messages, and the rules change over time, because spam and junk mail creators find new ways to get around filters designed to block them. Most email providers do not share all of their filtering policies publicly, because this can help them to stay a step ahead of spammers.

While we don't always know the specific reasons for a particular bounced email, there are steps that you can take to maximize your overall deliverability and lower your bounce rate. It's easiest to think about this by taking the perspective of the Email Service Provider, who has the email recipient's needs and safety in mind.

REASONS

EMAIL SENDER REPUTATION

If a message is sent from an untrustworthy sender, it could be flagged by an ESP as unsafe.

EMAIL LIST QUALITY

ESPs are on the lookout for senders who buy email lists or who are sending unsolicited bulk mail to their users.

EMAIL CONTENT AND FREQUENCY

ESPs scan email content to protect their users from dangerous, offensive or annoying content.

TIPS

Email Sender Reputation

SPF VERIFICATION: Adding Predictive Response to your SPF record lets ESPs know that you have authorized the email messages being sent from your domain by Predictive. Check with the Predictive support team and your webmaster to make sure that Predictive Response has been added to your SPF as an allowed sender for your domain.

DMARC: Talk to your webmaster about setting a DMARC policy for your domain. DMARC can monitor and alert you about messages being sent from your domain without authorization, so that you can proactively investigate any suspicious activity.

Blacklisting: Blacklists are publicly available lists of domains that might be untrustworthy or sending spam. Even if you are not sending spam, your domain could occasionally be added to a blacklist if email recipients complain about your content or move it to their spam folder (even accidentally). Note that there are many public blacklists and each ESP makes its own decision about whether to block your messages based on a blacklisting. You can use a search tool to verify that your domain has not been added to a blacklist. Specific reasons for a blacklisting are not usually available, but if your domain is added to a blacklist in error, you can reach out to request removal.

Return path alignment: A return-path is the “invisible” email address where bounce replies and other system notices are sent. Some ESPs prefer that the sending domain and return path domain are the same. By using a return-path address on your own domain, to match your send-from domain, you reduce the likelihood that your messages will be caught in a spam filter. If you have not set up a return path address on your own domain, please reach out to Predictive Support to create one.

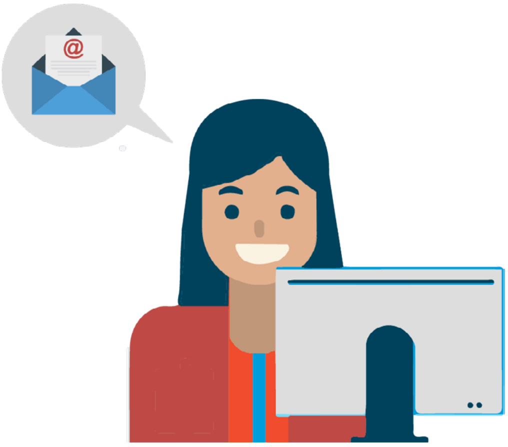
Sending IP address: Even if your domain has a great reputation, you could experience bounces if you send from an IP address that has been flagged as an untrustworthy sender. This is why Predictive proactively monitors the reputation of all our sending IPs, keeping IP sending reputation score excellent (above 90). Occasionally a complaint event or a low quality list send can temporarily damage sender score, and on those occasions we shift customers to a new IP to keep bounces low. As a Predictive customer, you do not need to monitor your sending IP reputation.

Email List Quality

ESPs are on the lookout for senders who buy email lists or who are sending unsolicited bulk mail to their users. Even if you are initially sending from a domain and IP with a great reputation, your sender reputation can be damaged by sending to a bad email list. Things to consider:

Inactive email addresses/typos: These addresses will generate an immediate permanent bounce, and Predictive will add them to your permanent do-not-mail list. However, if a send goes to a large number of bad addresses in a short period of time, ESPs will likely suspect that you are not maintaining list quality and may be more likely to block your mail in the future. To avoid this:

- Never buy email lists
- Gather emails for your mailings using an opt in or double-opt in process to confirm the recipients are active addresses and want to receive your messages
- If you are adding a large volume of new addresses to your mailings, do so in small batches over time to avoid a sudden spike in permanent bounces.



Spam traps: A spam trap is an invalid or inactive email address that ESPs monitor to catch senders who are not keeping their lists clean. If you send to a spam trap the ESP may be more likely to flag your future sends as spam. To avoid this, follow the steps above for inactive addresses.

Lack of engagement: If an ESP sees that their users are not opening messages from a sender over time, that is a signal that the messages are not wanted, and the ESP may block or filter future messages. To avoid this, monitor your open rates, and consider removing unengaged recipients from your email campaigns. Although you will be sending to fewer addresses, you will be sending to people who want to hear from you, and this will improve your reputation as a sender.

Email Content and Frequency

ESPs scan email content to protect their users from dangerous, offensive or annoying content. Things to consider:

Flagged content: Some elements of email content can trigger a spam filter-- for example, a large number of dollar signs or exclamation points may cause a message to be filtered as spam. The criteria for these filters varies over time and among ESPs. To make sure your content avoids these filters, use the Litmus test tool in your Predictive Email editor.

Complaints from recipients: If an email recipient complains about the content of a message, future messages from that sender may be more likely to be blocked or filtered. The ESP may or may not inform you of the complaint. If a complaint report is sent, Predictive will mark the email address in question as a complaint and will block all future sends to them.

In order to avoid complaints:

- Consider the guidance provided above for Lack of Engagement, and remove unengaged recipients from your list
- Vet content with your team and consider whether it is suitable/interesting to your audience

Frequency of mailings: If you are sending multiple messages to the same list each week, this can also lead to blocking or filtering by ESPs over time (it can also lead to complaints, see above). Consider the frequency with which you are reaching out to your audience, and if possible avoid over-mailing. Note: if you are sending messages frequently but you also have a great open rate, your sender reputation is not likely to be affected, because engagement with your messages is evidence that your content belongs in the inbox.

Questions?

Contact us if you have any questions.

Predictive Response Support Team:

1. Submit a case on our Help Center

2. Email them at support@predictiveresponse.com

3. Chat with them during EST business hours:

www.predictiveresponse.com