February 2024: Gmail and Yahoo inbox update

Deployteq - Suzanne Martens - 2024-01-11 - Comments (0) - Deliverability

Gmail and Yahoo are set to tighten requirements for email senders

Starting in February 2024, marketers must make their sent emails comply with a new set of rules. For example, emails must have email authentication that meets the tightened requirements of Gmail and Yahoo. There should also be an easier way to unsubscribe from the emails and a maximum number of “spam” emails you can deliver to an email address. With these security updates, Gmail and Yahoo are ensuring that the number of spam messages in consumers’ inboxes is reduced.

Spam goes beyond attempts by hackers and scammers to ransom your credit card information or your login information. Emails the audience doesn’t need or hasn’t signed up for are also considered Spam. It’s already something we bang on about, but now more than ever, a clean mailing list has become even more crucial.

What is Gmail & Yahoo updating?

Around February 2024, bulk senders will have to comply with the following requirements:

Simple unsubscribe process

A simple unsubscribe process helps optimise the user experience. Recipients should soon be able to unsubscribe from commercial emails with a single click.

As an email marketer, this means you will have to standardise and automate a simple campaign behind your unsubscribe process. Are you still processing unsubscribes manually? We’d recommend looking for a provider to help you start automating your unsubscribes to ensure a seamless experience.

Lower spam rates

As a second restriction, Gmail and Yahoo updates state that there will be a stricter policy on the number of emails sent per day to a specific email address. There are already many tools out there to keep unwanted messages out of the recipient’s inbox, but to optimise this protection, Gmail has implemented a “spam threshold” that senders must stay below. This spam threshold is 0.3%.

Email authentication

Perhaps the most vital development in this story is that Gmail and Yahoo are becoming stricter on the security measures you take as a sender. Strong email authentication is even more crucial to ensure that emails actually end up in the recipient’s inbox and not in the dreaded junk folder. SPF, DKIM and DMARC will be required as of February 2024 if you are a bulk sender (more than 5,000 emails per day).

In short, what does SPF, DKIM and DMARC mean?

Most email marketers among us will be familiar with these acronyms. These three terms have long been the standards for email security, but sometimes we forget just how important they are. A quick refresh

SPF, or Sender Policy Framework, is a text line you can add in your domain name settings that helps establish the authenticity of emails received into the inbox. So, if someone sends an email on behalf of your domain name, but that sender is not in your SPF record, the email will not arrive in the recipient’s inbox.

The abbreviation **DKIM** stands for Domain Keys Identified Mail. With DKIM, a kind of digital signature is set up, stating that the email came from you.

DMARC stands for Domain-based Message Authentication, Reporting and Conformance. DMARC is actually a continuation of the above steps. When an email arrives, it checks to see if all checks by SPF and DKIM match. If not, the email will not be forwarded to the recipient’s inbox. A nice feature of DMARC is its reporting function.

You will be notified when an email has not passed all checks, so you will know immediately if you have become a victim of phishing or spoofing.

Quick tips & tricks

This may make perfect sense to some, but the importance of a “clean” database is undeniable. Working with an email list with active email addresses will prevent a lot of unnecessary bounces when sending. Filter your email list for typos, bounces and, for example, prolonged inactivity. This will prevent a negative effect on your deliverability.

Another tip is to personalise your emails. Email clients and spam filters value personalisation because it shows that the email comes from a legitimate source as well as being relevant to the recipient. So, your email is less likely to be marked as spam.

Need help?

At Deployteq, we make standard use of a simple and automated unsubscribe process in our mailings and campaigns. This functionality is added to every email sent. To stay below the issued spam threshold, it is important to have a clean mailing list, maintain a healthy sending frequency and send as many personalised emails as possible. Deployteq can also assist in adding the required email authentication.

It might sound like a lot of work... So we’re happy to help you set up, adjust or optimise the above points. Please contact us via support@deployteq.com

Email validation

When email authentication with DKIM is not properly configured on your domain, Deployteq will display an error message for this. In this case, it is important to add information to the DNS of the domain to facilitate DKIM signing. You can find the required DNS settings in our manual.