



2024 Sender Requirements

**A Guide for Marigold Engage by Sailthru
Customers**

December 2023





Keep Inboxes More Secure

We're here to be your partners, ensuring you are empowered to create marketing gold.

In October 2023, mailbox providers Google and Yahoo announced sender requirement changes in an effort to keep email a reliable source of communication, as well as continue to protect inboxes for their consumers. These changes will go into effect as of February 1, 2024.

To best support you, we have created a step-by-step guide for the actions we recommend you take to avoid any disruption to your email strategy.



Sender Requirements: 3 Themes

Authenticate your emails

Confirm DNS records with DKIM, DMARC, and SPF protocols

Our Deliverability team will reach out if needed.

If your account requires attention, we will be reaching out to prior to January 5th.

Make unsubscribing easier

Make it easier to unsubscribe with the option in the email header

Marigold will make this standard within our platforms

Marigold will make these changes in mid-January 2024

Stay below the spam threshold

Stay below a 0.3% spam complaint rate

We'll work on this together

This work should be ongoing

SENDER REQUIREMENTS

WHO WILL BE RESPONSIBLE

WHEN TO TAKE ACTION

Configuring your DNS

At this point, there is no action required on your part. If we determine that your account requires attention, a member of our Deliverability team will be reaching out to prior to January 5, 2024.

If you have not heard from our team before January 5, 2024, it means your account meets the new requirements and no changes to your account are necessary. You are all set!



Sender Requirements: 3 Themes

SENDER REQUIREMENTS

WHO WILL BE RESPONSIBLE

WHEN TO TAKE ACTION

Authenticate your emails

Confirm DNS records with DKIM, DMARC, and SPF protocols

Our Deliverability team will reach out if needed.

If your account requires attention, we will be reaching out to prior to January 5th.

Make unsubscribing easier

Make it easier to unsubscribe with the option in the email header

Marigold will make this standard within our platforms

Marigold will make these changes in mid-January 2024

Stay below the spam threshold

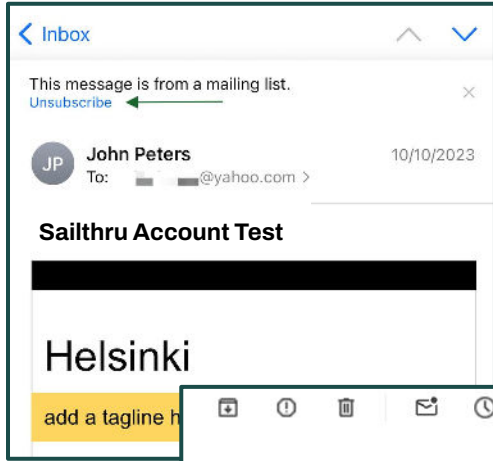
Stay below a 0.3% spam complaint rate

We'll work on this together

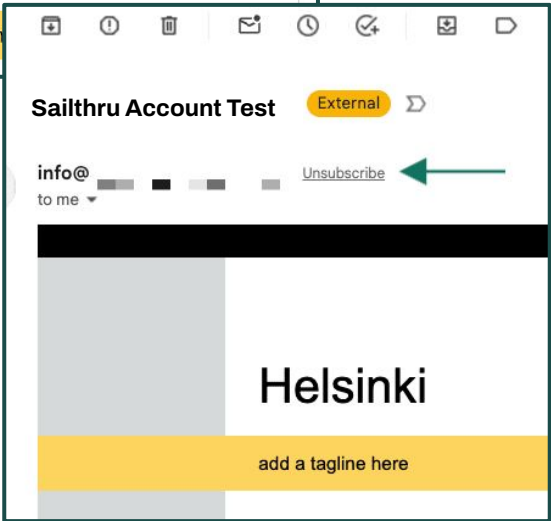
This work should be ongoing

New Unsubscribe Feature Coming

Make unsubscribing easier



Yahoo Mobile



Gmail Desktop

Unsubscribe links have been a legal requirement for over two decades, however, one-click unsubscribe functionality is a new requirement.

Marigold Engage by Sailthru will be further enhancing our existing unsubscribe headers to comply with an additional one-click requirement. There is nothing for you to do with this, Sailthru will handle the entire process.

The existing unsubscribe link in the body of the message is still required and will continue to work.

Join our January 2024 Roadmap Webinar for this new release, plus other new releases, coming to Engage by Sailthru.



Sender Requirements: 3 Themes

SENDER REQUIREMENTS

WHO WILL BE RESPONSIBLE

WHEN TO TAKE ACTION

Authenticate your emails

Confirm DNS records with DKIM, DMARC, and SPF protocols

Our Deliverability team will reach out if needed.

If your account requires attention, we will be reaching out to prior to January 5th.

Make unsubscribing easier

Make it easier to unsubscribe with the option in the email header

Marigold will make this standard within our platforms

Marigold will make these changes in mid-January 2024

Stay below the spam threshold

Stay below a 0.3% spam complaint rate

We'll work on this together

This work should be ongoing

*Stay below the spam
threshold*

0.3%

(or below) Spam Complaint
Rate

**Avoid spam by
staying below the
'clear spam rate'
threshold**

GOOD NEWS! This isn't new.

Google and Yahoo have always had a spam complaint rate threshold, and the penalty for violation has always been restricted email delivery.



*Stay below the spam
threshold*

Reduce Spam Complaints

- Manage the registration process to meet future expectations
- Always respect unsubscribe requests
- Make sure your emails are clear and well branded
- Use appropriate mail frequency
- Stay consistent & relevant
- Customize and personalize messaging
- Sunset dormant contacts



More resources from Marigold

Supporting you every step of the way

- Contact our [Support team](#), for in-person help and guidance.
- Plan to join our January webinars, where our experts will walk through each step of this process.
- Check out our help article in Get Started, linked below
 - [Configure your DNS Records](#)
- Review the appendix slides, included, for even more insight into the new sender requirements.



Appendix



The New Gmail and Yahoo Deliverability Rules

Effective February 2024



Why are Gmail and Yahoo Making this Change?

Gmail and Yahoo seek to deliver messages that consumers want to receive and filter out the messages they don't.

A pivotal aspect of this involves sender validation using email authentication standards to guarantee the email sender's identity to prevent malicious actors from exploiting resources.

How is Marigold Responding

- Our team is actively investigating the potential implications from the recent Gmail and Yahoo announcement.
- As a portfolio, we already have several of these requirements fully or partially in place, as we constantly work to offer deliverability best practices.
- We'll share additional recommendations in the weeks and months ahead.

What Requirements are Changing?

- Authenticate your email using industry standards like SPF, DKIM and DMARC.
- Make it easier for audiences to unsubscribe, using one-click unsubscribe.
- Keep your average spam rates below 0.3%.



Who Needs to Take Action?

Everyone!

If you have contacts with Gmail and Yahoo email addresses in your subscriber and customer lists, this change will impact you.

Also affected are domains that are hard to spot – like those using Google Workspace for custom domains like meetmarigold.com.



Verify your sender identity with standard protocols

1

Set up SPF

Sender Policy Framework (**SPF**) is a mechanism by which a receiving domain can check whether an email has originated from a sending IP that is authorized to send emails on behalf of the admins of a given domain.

Platform specific SPF instructions will be provided.



2

Set up DKIM

DomainKeys Identified Mail (**DKIM**) is a form of email authentication that helps verify that an email's sender address is legitimate and is not being spoofed by a third party.

Platform specific DKIM instructions will be provided.

3

Establish DMARC

Domain-based Message Authentication Reporting & Conformance (**DMARC**) uses both SPF and DKIM to authenticate email. It lets domain owners choose how receiving servers should manage unauthorized/unauthenticated messages.

Policy = "None"

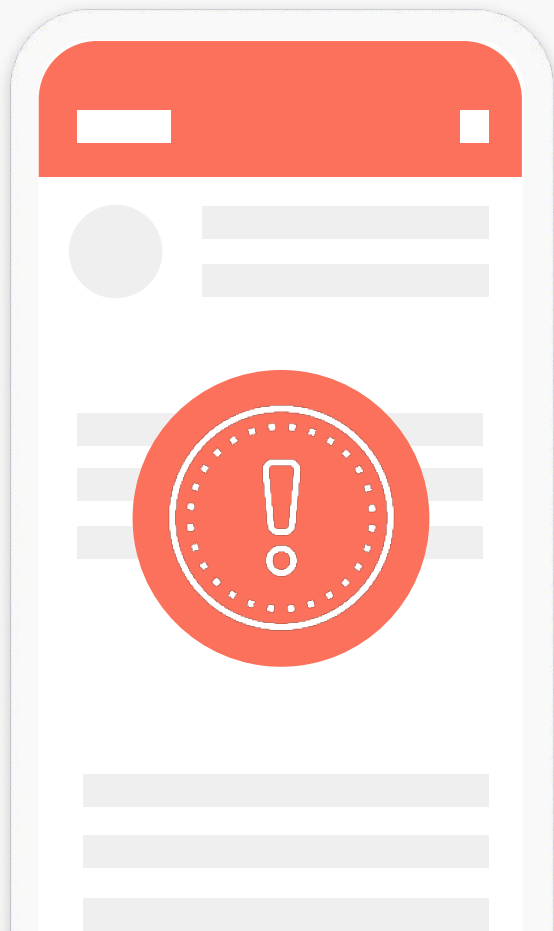


Don't send from Gmail.com

Don't impersonate other domains or senders without permission. This practice is called spoofing, and Gmail may mark these messages as spam.

Don't impersonate Gmail from: headers.

- Gmail will begin using a DMARC quarantine enforcement policy, and impersonating Gmail From: headers might impact your email delivery.
- If you don't own the domain you should not send the email from the domain. Own and authenticate properly.



*Thank
you!*