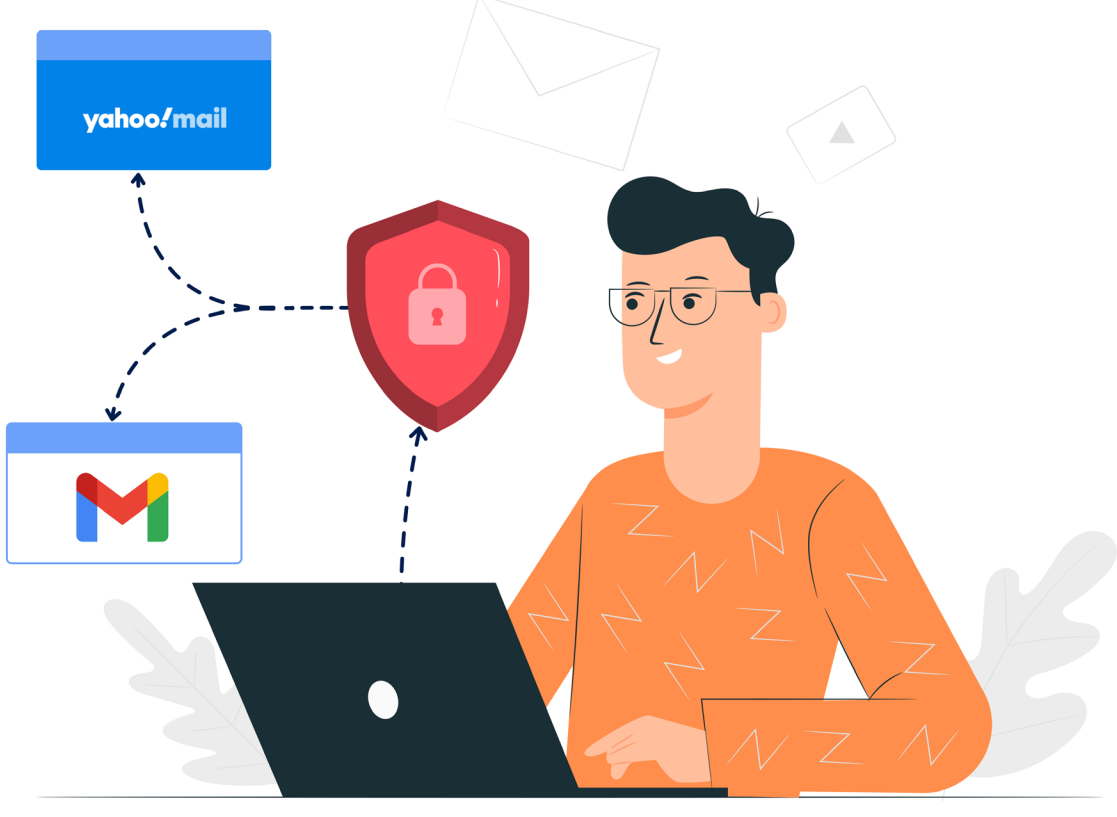
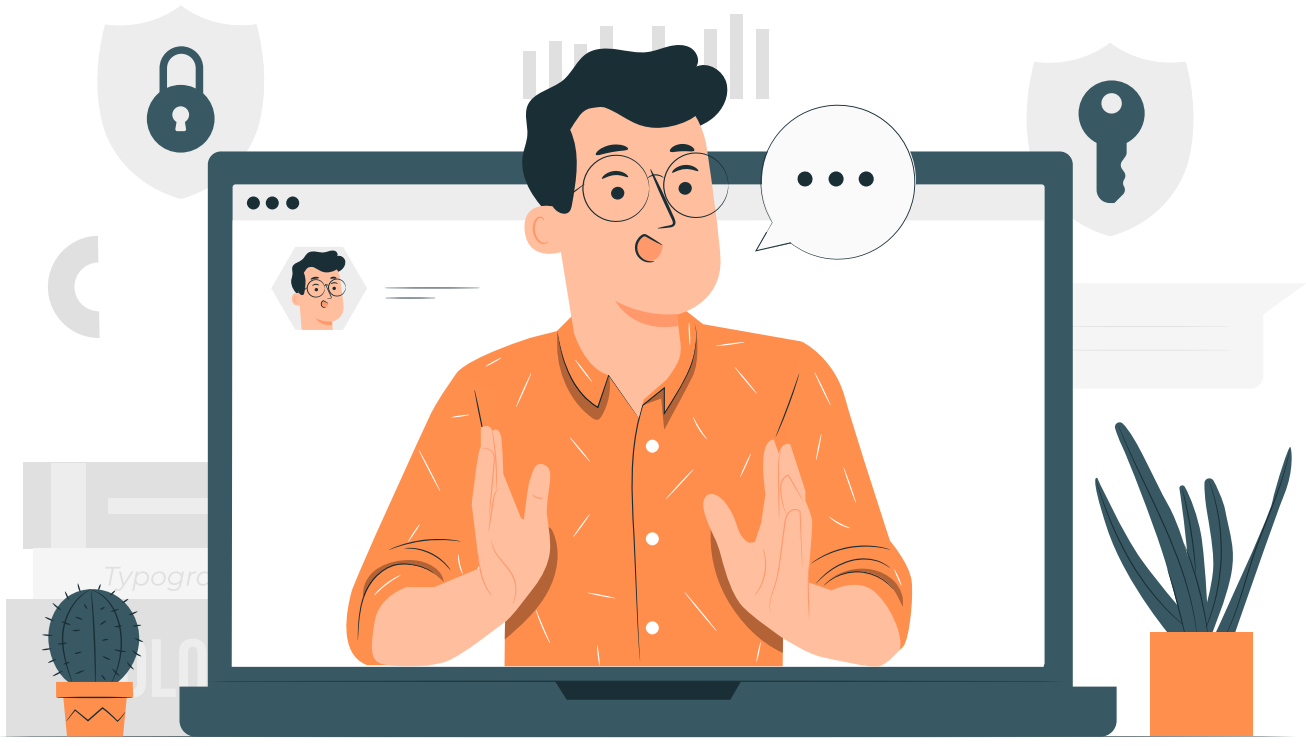
Zoho Campaigns

Securing Your Emails

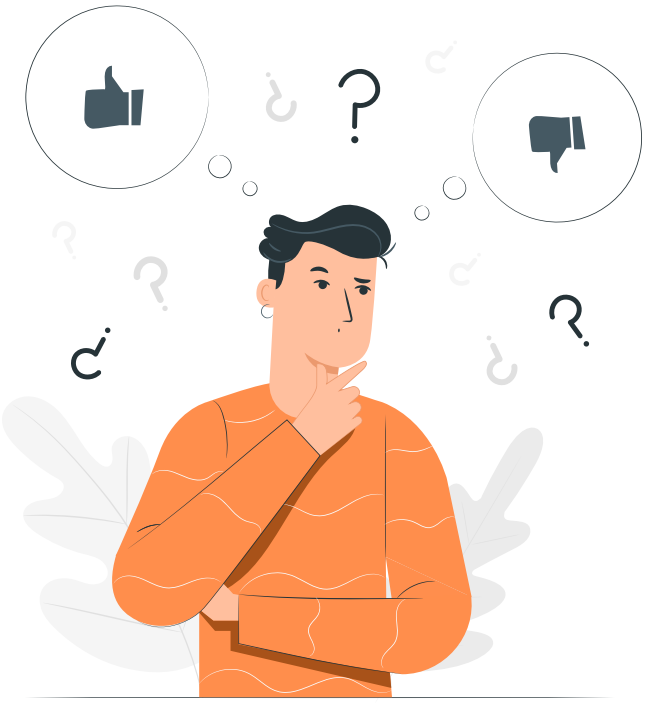
Google and Yahoo's 2024 Authentication Requirements





A little background

Starting February 2024, Gmail has rolled out stringent email authentication requirements for bulk senders, in order to combat malicious messages, reduce inbox clutter, thwart phishing attacks, diminish spam, and bolster data security. But does it matter?



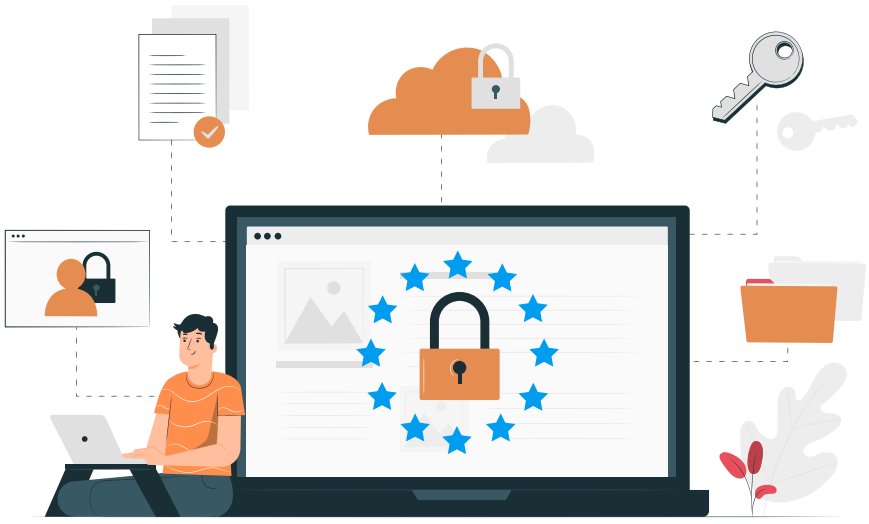
It really does

The current update is as important as GDPR, because failing to comply with Gmail's requirements will directly impact your email deliverability, reach, and revenue.

Gmail has introduced the new email authentication requirements on the back of introducing similar requirements in 2022. To quote from google's blog,

> "Last year, we started requiring that emails sent to a Gmail address must have some form of authentication. And we've seen the number of unauthenticated messages Gmail users receive plummet by 75%, which has helped declutter inboxes while blocking billions of malicious messages with higher precision."

Therefore, the new requirements are in continuation with Gmail's renewed attempt at safeguarding its users' inboxes against spam and phishing attacks. Let's take a look at some of these requirements



Ushering a new era of security

Implement SPF (Sender Policy Framework): Sender Policy Framework (SPF) is an authentication technique that helps receiving email servers identify legitimate email senders and prevent spam from entering the inbox of email recipients.

Enforce DKIM (Domain Keys Identified email) : DomainKeys Identified Mail (DKIM) is an email authentication mechanism that is deployed to prevent emails from being tampered with in transit. DKIM is widely adopted by businesses to protect their emails from spoofing and phishing attacks.

Here's a video from Google, explaining what SPF and DKIM are. You can also refer to our Help documents on SPF and DKIM to learn more about these.

Maintain Low spam rates

Google wants the senders to maintain a spam rate below 0.3% (as measured by Google's postmaster tools) to ensure that your emails don't get flagged as unwanted or fraudulent.

Implement DMARC (Domain-based Message Authentication, Reporting, and Conformance) policy:

DMARC builds upon SPF and DKIM and allows businesses to publish policies that provide instructions to mailbox provders' recipient servers on how to handle unauthenticated emails sent from their domain.

Implement DMARC alignment

Ensure that messages pass DMARC alignment, which checks whether the sending domain's authentication methods (SPF and DKIM) align with the domains used in the email headers.

One-click unsubscribe

Include list-unsubscribe message headers and a clearly visible unsubscribe link in the message body for subscribed messages. Unsubscribe requests must be processed within two days.

At Zoho Campaigns, we already have a spam threshold of **0.1%**, which adheres to the new guidelines Google and Yahoo are establishing.

Follow Best practice

Use business domain : Do not use publicly available domains like “gmail.com” as they cannot be authenticated. Always use a business domain

Maintain a hygiene list: Ensure that your mailing list contains only regularly engaged and interested contacts and regularly prune invalid and idle contacts.

Avoid spam traps : Spam traps negatively impact your deliverability. Use a double opt-in while adding contacts. Here is a detailed document on spam traps.

Ensure email authentication : Implement SPF, DKIM and ensure that your messages pass the DMARC alignment.

Maintain a low spam rate : Ensure that your spam rate is less than 0.3% . A higher spam rate can negatively impact your domain reputation.

Refer to the document to understand about the best practices in detail.

Contact Us

Zoho Corporation

4141 Hacienda Drive, Pleasanton,

California 94588, USA

+1 (888) 900 9646 (USA)

+44 (20) 35647890 (UK)

Support@zohocampaigns.com

https://www.zoho.com/campaigns/

Zoho Campaigns