EASYDMARC

Get Your Emails Delivered In 2024

An Easy Guide To The New Requirements

Table of **Contents**

Introduction: Adapting to the New Email Standards of Google and Yahoo

In an unprecedented move, Google and Yahoo have jointly announced a major shift in email policy, effective from February 2024. This change primarily affects organizations that send over 5,000 emails in a single day to Gmail or Yahoo Mail users.

To ensure uninterrupted email delivery, the following criteria must be met:

DMARC Implementation:

All marketing and transactional emails must authenticate via DMARC (Domain-based Message Authentication, Reporting, and Conformance) protocols.

DMARC Policy Enforcement:

Emails should be sent from domains that have a DMARC policy in place, with a minimum setting of “p=none”.

DNS Verification:

It’s essential to have both forward and reverse DNS configurations properly set up to improve email deliverability.

Streamlined Opt-Out Process:

Incorporate an easily accessible one-click unsubscribe option in all commercial and promotional messages.

Low Spam Rates:

Maintain a minimal spam rate to protect the integrity and reputation of your email sending domain.

Starting in February 2024, non-compliance with these standards will result in temporary delivery errors, marked with specific error codes, for offending email traffic.

By April 2024, Google and Yahoo will begin rejecting a certain percentage of non-compliant emails, with plans to escalate the rejection rate progressively.

Additionally, there is a firm deadline of June 1, 2024, to integrate the one-click unsubscribe feature in all commercial and promotional emails.

This guide is designed to answer the critical question: How can you align with these new standards to ensure your emails are delivered successfully in 2024? We will explore the intricacies of these requirements and offer practical solutions. But first, let's dive into the mechanics of email and why these changes are essential for a healthier digital communication environment.

How Email Works

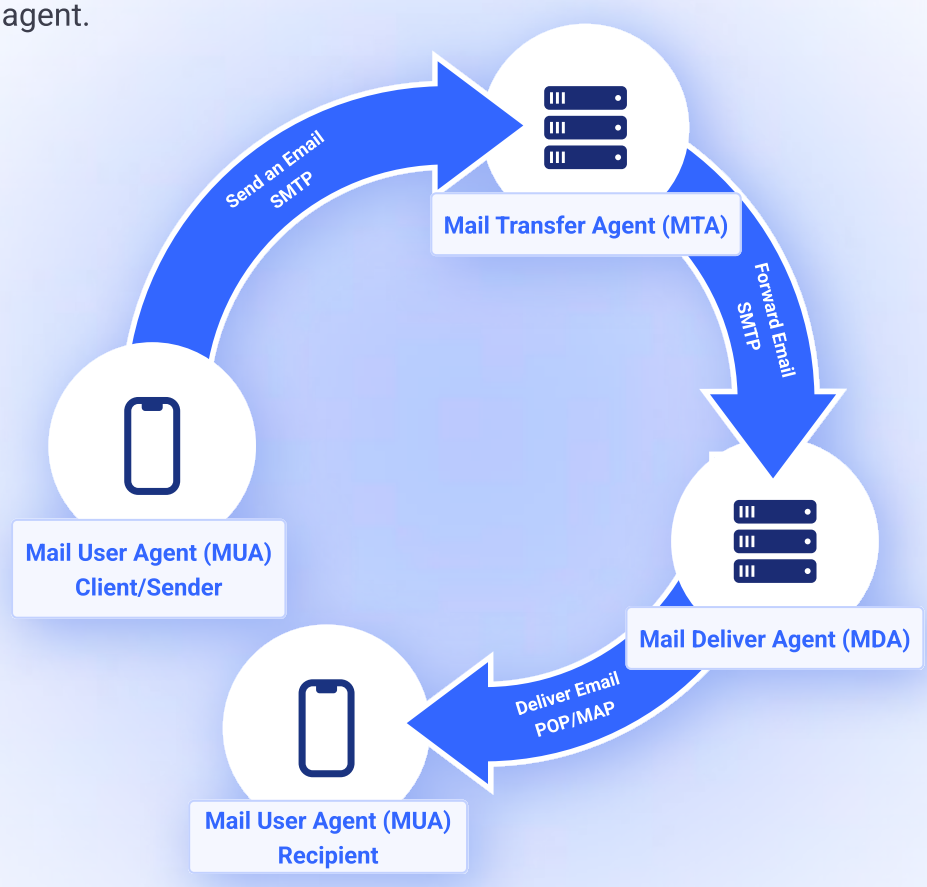
In 1965, the Massachusetts Institute of Technology (MIT) researchers pioneered electronic messaging for internal academic purposes, marking the inception of the first email service. However, it wasn't anything like the email we use today.

Several years later, in 1971, Ray Tomlinson invented email, the so-called personal digital mailboxes we know today. This innovation allowed individuals to communicate using the "@" sign, enabling them to reach specific persons or computers within the US Defense Advanced Research Projects Agency (DARPA).

So, how does email actually work?
Well! The process begins with the user using an email client, which is a software application or web-based service that allows users to send, receive, and manage their emails.

Once the user specifies the recipient's email address, subject, and content of the message and hits the "send" button, the email client communicates with the SMTP server (Simple Mail Transfer Protocol).

SMTP is responsible for sending the outgoing mail to the recipient's mail server. It acts as a mail transfer agent.



What Happens Next

1. The recipient's email address contains a domain (e.g., example.com). The email client queries the DNS to find the mail server associated with that domain.

2. The recipient's mail server, also known as the Mail Transfer Agent (MTA), receives the incoming email. The email is stored temporarily on the server until the recipient retrieves it.

3. The recipient uses an email client to connect to their mail server using either POP3 or IMAP (Post Office Protocol 3/Internet Message Access Protocol). POP3 downloads the email to the recipient's device, removing it from the server (usually used for single-device access). IMAP allows multiple devices to access and manage the same mailbox, keeping the email on the server.

4. The email is now in the recipient's inbox and can be read, replied to, or stored in folders. The process is similar if the recipient chooses to reply or forward the email. The email client communicates with the SMTP server to send the response.

What Is Email Authentication?

When people discovered email, they couldn't anticipate phishing becoming a global issue for many businesses and people. Year by year, the number of fraudulent emails started to increase.

The growing number of phishing attacks drove experts to dig deep into the problem to find appropriate email protection solutions. And the need for email authentication arose.

Email authentication operates through various methods, each with its own advantages and drawbacks. Despite the method-specific implementation, the underlying concept remains consistent.
Here's a brief overview of the email authentication process:

- **Initially, a business or organization establishes a policy that outlines how email servers authenticate messages originating from their email sending domains.**
- **The email sender then configures the mail server to implement and publicize this authentication policy.**
- **Upon receiving a message from this sender, the email receiver authenticates the message by cross-referencing its details with the rules stipulated by the sender.**
- **Based on the authentication results, the email receiver may choose to flag, deliver, or reject the message.**

Why Do These Changes Happen?

Actually, when we say email authentication, we mean 3 main concepts of it:

SPF

DKIM

DMARC

These protocols are inventions of different periods but work together to prevent the delivery of fraudulent phishing, spam, and spoofed emails.

Already, several leading countries have made DMARC implementation mandatory or recommended for national government organizations, including:

The USA

The Netherlands

Australia

The United Kingdom

Canada

New Zealand

Denmark

And now, the technology giants like Google and Yahoo! join forces to announce the best way to secure a domain against phishing attacks with DMARC.

Let's dive deeper into what SPF, DKIM, and DMARC are and how they work.

Setting Up Your SPF Record

SPF, or Sender Policy Framework, allows you to specify which mail servers are authorized to send emails on behalf of your domain. Creating an SPF record involves adding a specific DNS TXT record to your domain's DNS settings.

Use our SPF Record Generator tool to create and generate your SPF record. Here is an example of an SPF record:

v=spf1 include:_spf.example.com ~all

- **v=spf1** specifies the SPF version.
- **include:_spf.example.com** includes the SPF records from the domain **_spf.example.com.** You would replace "example.com" with your actual domain.
- **~all** indicates a soft fail. It means that if the sending server is not listed in the SPF record, the email will still be accepted but marked as potentially suspicious.

Once you've created and generated your SPF record, you need to publish it in your domain's DNS zone. This is usually done by adding a TXT record with the SPF information.

Example SPF TXT record in DNS:

example.com. IN TXT "v=spf1 include:_spf.example.com include:mail.anotherdomain.com -all"

Update your DNS records through your domain registrar or DNS hosting provider to verify your SPF record. It may take some time for DNS changes to propagate. You can use our **SPF Record Checker** tool to confirm that your SPF record is correctly set up.
In our advanced **Knowledge Base** center, you can find step by step guides on how to set up your SPF record for every service provider you're using to send emails.

Setting Up DKIM Record

DKIM, or DomainKeys Identified Mail, allows you to place a unique digital signature on any email sent from your servers. These signatures are also called keys, and there are two keys in DKIM - a public key and a private key.

Each time you send an email from your domain, the receiving server retrieves the public key in your domain's DKIM record. It then uses the public key to verify the DKIM signature in the email's DKIM header.

With our free DKIM Record Generator tool, you can create a DKIM record for your email sending domain(s) quickly and easily.

Here's an example of a DKIM record:

Name: _domainkey.yourdomain.com
Type: TXT
Value: "v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC2G9t9YgH9f0aJl0ZBs
yjObvv0F6OHZjEg4aUfnm0k4GE5FGPjo7hYshRz2aRf+Xxv4S1z4dmKzFLs3z3r
45j9yNQsKkS5VsQgZBYyQKIZwP3uQbXpIvGJdIvO2rE7RxLW1/4LsR6HS0B2L
6/D/4unV+vmEi/O3UzCujW6bjk9QIDAQAB"

The actual value includes the DKIM version (**v=DKIM1**), the key type (**k=rsa**), and the public key (p=), where:

- **v=DKIM1:** Indicates the version of DKIM being used.
- **k=rsa:** Specifies the public key's encryption algorithm (in this case, RSA).
- **p=:** Contains the public key itself.

After implementing your DKIM record in your DNS, you can check if everything is set up correctly with our free DKIM Record Checker tool.
In our advanced Knowledge Base center, you can find step by step guides on how to set up your DKIM record for every service provider you're using to send emails.

Setting Up DMARC Record

DMARC, or Domain-based Message Authentication, Reporting, and Conformance, takes SPF and DKIM standards to the next level by ensuring that emails reach those standards before letting them through. As a result, legitimate emails are passed through, and fraudulent emails, or emails that appear to come from your domain but actually came from an unscrupulous individual, will be blocked.

To create a DMARC record, visit our free DMARC Record Generator tool and generate your record.

Here's an example of a DMARC record:

_dmarc.yourdomain.com. IN TXT "v=DMARC1; p=none; rua=mailto:your.email@example.com; ruf=mailto:your.email@example.com; fo=1"

Let's break down the components of this DMARC record:

- **v=DMARC1:** This specifies the DMARC version being used.
- **p=none:** This sets the policy for email that fails DMARC authentication. In this example, it's set to "none," which means that no action should be taken if the email fails DMARC checks. You should have a "quarantine" or a "reject" policy to block unauthorized emails sent from your sending domain.
- **rua=mailto:your.email@example.com:** This specifies the email address to which aggregate reports (XML files containing information about the email authentication results) should be sent.
- **fo=1:** This indicates the message format for the forensic reports. The value "1" indicates that the reports should be in the "Afrf" (Authentication Failure Reporting Format) format.

Once you've configured your DMARC record, make sure to monitor the reports to identify any potential issues and improve your email authentication by leveling up your policy to "quarantine" and then to "reject."

In our advanced Knowledge Base center, you can find step by step guides on how to set up your DMARC record for every service provider you're using to send emails.

Now that you know the most complicated and important part of Google and Yahoo!'s new sender requirements, let's speak about the other aspects, which are:

- DNS infrastructure configurations
- Subscriptions
- And spam

DNS Infrastructure Configurations

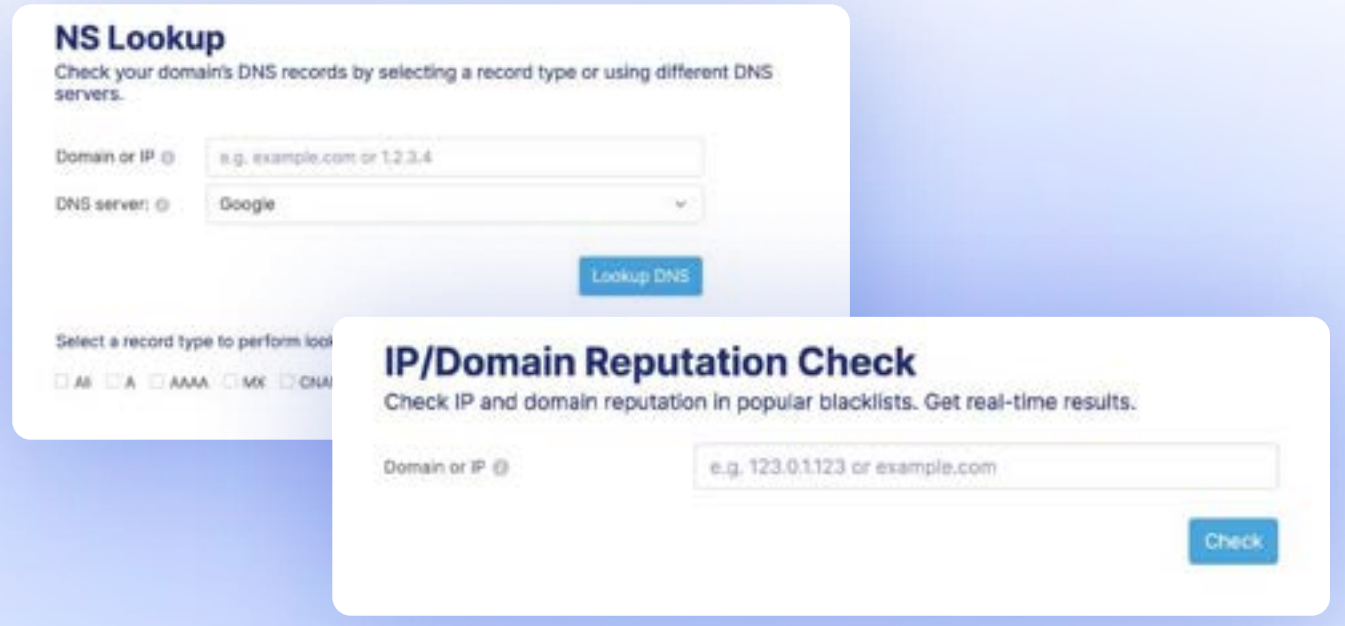
Ensure the legitimacy of your email communication by confirming that your sending domains or IPs possess valid forward and reverse DNS records, commonly known as PTR records.

But what does this mean exactly?

Reverse DNS plays a crucial role in enabling mailbox providers to authenticate the sender's identity through a reverse DNS lookup upon receiving your emails.
Here's how it works: when you update your DNS provider with a record and subsequently send emails over your IP, the recipient's email service provider conducts a reverse DNS lookup (rDNS) using an A Record (address record).

An A Record essentially establishes a link between your domain and its corresponding IP address. As the mailbox provider queries your A Record, they will find the rDNS that aligns with your A Record. This reciprocal verification serves as evidence, establishing the connection between your sending IP and your domain, as well as affirming the association of your domain with your sending IP.

In short, your sender and domain reputation depends on the IP addresses you use to send emails. So, practice to have your IPs monitored carefully.
Use our free DNS Record Checker tool to check your domain's DNS records by selecting a record type or using different DNS servers. Also, you can run an IP Reputation Check to get real-time information about the status of your IP addresses.



Subscriptions

Ensure that you only send emails to individuals who have interest in receiving messages from you. This helps minimize the chances of your domain's emails being reported as spam.

If your domain is frequently flagged as spam, it can negatively impact your reputation, ultimately leading to more of your messages being marked as spam.

To keep your recipients engaged, make subscription simple by following these guidelines:

- **Ensure that recipients opt-in to receive messages from you.**
- **Verify each recipient's email address before adding them to your subscriber list.**
- **Periodically send confirmation messages to verify that recipients still wish to remain subscribed.**
- **Consider removing recipients who don't open or read your messages to maintain engagement.**

Make “unsubscribe” easy and simple.

- **Always provide an effortless method for recipients to opt out of receiving your messages.**
- **Allowing people to unsubscribe can improve open rates, click-through rates, and overall sending efficiency.**
- **Implement a one-click unsubscribe option if you are a bulk sender (AKA, you send more than 5,000 messages per day).**

Effective Spam Management: Striking The Right Balance

In the world of email communication, managing your spam rate is crucial. Google's guidelines suggest keeping this rate below 0.10% and definitely avoiding exceeding 0.30%.

Why is this important?
A high spam rate can lead to your emails being more frequently classified as spam, affecting their deliverability and your domain's reputation.

Regarding open rates, it's worth noting that major providers like Google, Yahoo!, and AOL don't actively monitor these metrics, nor do they fully endorse third-party open rate data. So, a low open rate doesn't necessarily signal a deliverability problem, but it does warrant a review of your content's relevance and engagement.

Navigating DMARC With EasyDMARC

EasyDMARC is a platform designed to simplify the complexities of DMARC implementation for better email deliverability. It's user-friendly and effective, making it a solid choice for those seeking to enhance their email security without requiring extensive technical knowledge.

Here's how EasyDMARC stands out:

- **Prioritizing Privacy:** EasyDMARC is committed to maintaining high privacy standards. Your sensitive data remains secure throughout the DMARC implementation process.
- **Streamlined Setup:** The platform is designed for easy adoption, removing the usual complications associated with email security measures.
- **Accessible Tools and Guidance:** EasyDMARC offers a straightforward dashboard, along with practical tools and guides that make understanding and managing email authentication more accessible.

For further information or a demonstration of how EasyDMARC can help in your specific context, feel free to reach out.

Explore EasyDMARC

Introducing EasySender By EasyDMARC

EasySender, the latest innovation from EasyDMARC, is specifically designed to boost your email deliverability and enhance your marketing return on investment (ROI).

Key Features of EasySender:

1. **Email Optimizer:**

   With an impressive 98.6% accuracy, our email verification tool ensures the reliability of your contact databases. Whether processing emails individually or in bulk, EasySender streamlines this process with efficiency and precision.

   - **Manual Verification:** Easily upload your contact lists in CSV or XLS(X) formats for bulk verification, or opt for quick, instant verification.

   - **API Verification:** Utilize our API for real-time email verification, keeping your customer databases free from invalid or bounced addresses.

2. **Email Optimizer:**

   Connect your mailbox to EasySender to enhance the deliverability of your domain or IP address. Within weeks, you'll notice a significant improvement in how your emails are received.

3. **Inbox Placement Testing:**

   Our tool sends test emails to a range of email platforms, tracking their journey to provide insights on deliverability. This helps you understand how different mailbox providers handle your emails, whether landing in inboxes or spam folders and guides you in optimizing your email performance.

4. **Google Postmaster Integration:**

   Leverage the power of Google Postmaster tools within EasySender. Monitor key metrics like domain/IP reputation, spam rates, and authentication status; all consolidated on an easy-to-use dashboard.

Maximize Your Email Impact With EasySender

EasySender is not just about ensuring deliverability; it's about transforming your email strategy into a powerful tool for building relationships and driving conversions. Spend more time engaging with your audience and less time worrying about your sending reputation.

Ready to elevate your email game?

Get Started With EasySender

EASYDMARC

www.easydmarc.com

sales@easydmarc.com