Teamspring TECHNOLOGIES

EASYDMARC

New Email Security Requirements for Top Email Providers in 2025

Table of **Contents**

From Emails to Authentication

Since its inception in 1971, email has evolved dramatically. In the early days of email, few could have predicted that phishing would become a widespread cybersecurity threat. As phishing attacks grew in volume and sophistication, security experts began exploring targeted solutions to protect email communication, leading to the emergence of **email authentication protocols**.

Organizations and individual users alike must now adhere to stricter authentication requirements and more comprehensive security standards to ensure the integrity of email communications. Those who don't adapt risk email delivery and deliverability issues. These changes reflect the growing recognition that **email remains one of the primary mediums for cyber attacks**.

Over the last two years, there has been a **fundamental shift as major email providers have implemented stricter security standards** to combat these threats.

The Provider-Led Email Security Shift

Google, Yahoo, iCloud, and, most recently, Microsoft, have all strengthened their email authentication requirements. What began as recommended best practices has evolved into mandatory policies that now **require proper implementation of authentication protocols for bulk senders, or those sending a minimum of 5,000 emails per day**. While the threshold seems high, it affects countless businesses, educational institutions, and government agencies.

However, while bulk senders are specifically targeted with this framework, these email providers **recommend authentication protocol implementation for all types of senders** in order to keep up with email best practices.

But what exactly does email authentication entail?

Email Authentication Fundamentals

Email authentication is the **process of verifying that an email message comes from a legitimate source and hasn't been forged, tampered with, or sent by an impersonator**. It helps protect recipients from phishing and spam.

This verification process is made possible by implementing three key protocols:

Sender Policy Framework (SPF)

SPF is a DNS-based email authentication protocol that allows domain owners to specify which IP addresses are authorized to send mail on behalf of their domain. It works by checking the envelope sender address (RFC5321.MailFrom) during the SMTP transaction.

DomainKeys Identified Mail (DKIM):

DKIM lets the sender add a digital signature to the email headers and body using a domain they control (specified in the "d=" tag of the DKIM-Signature). The recipient uses a public key from that domain's DNS to verify the signature and check that the message wasn't altered in transit.

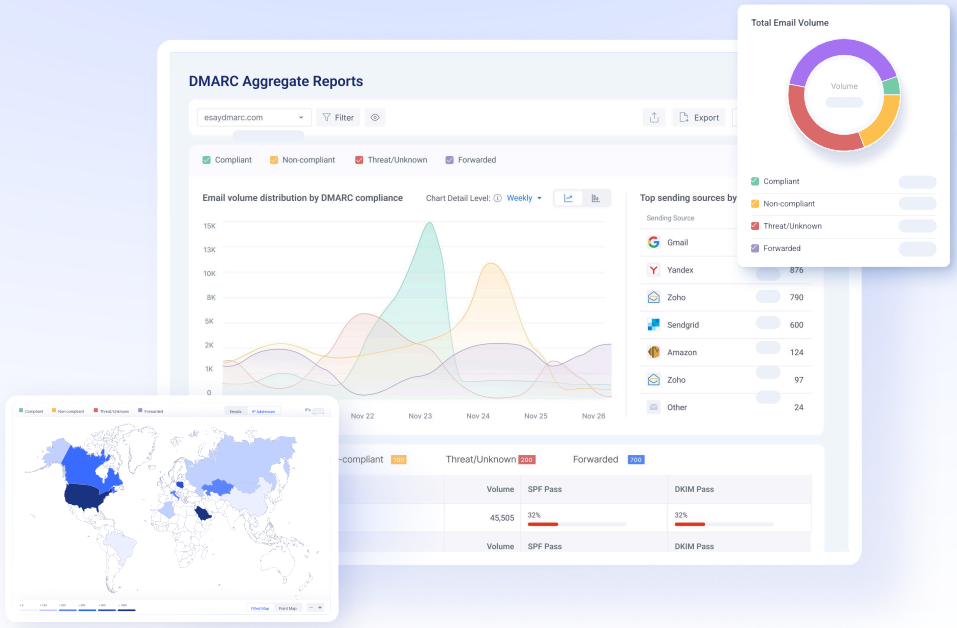
Domain-based Message Authentication, Reporting, and Conformance (DMARC)

DMARC is a protocol that helps protect organizations and their email recipients from fraudulent emails.

DMARC is not only about authentication. As its name suggests, iit consists of three pillars–**authentication**, reporting, and conformance. The authentication pillar works by checking whether a message passes SPF or DKIM with alignment to the domain in the "From": header. Without alignment, even a passing SPF or DKIM result does not count toward DMARC pass.

The second pillar, **reporting**, provides detailed insights into email activities, allowing domain owners to identify the unauthorized use of their domain. This includes aggregate and forensic reports that highlight whether emails pass SPF and DKIM. Finally, **conformance** involves specifying how senders should deal with emails that do not pass these checks.

Based on the authentication results, the **email receiver may choose to flag, deliver, or reject the message**. This is known as the DMARC policy.



DMARC Policies: Enforcement

DMARC's importance lies in its ability to close security gaps left by SPF and DKIM. It consists of three policy levels:

- p=none Monitors and provides feedback reports without affecting email delivery; to but fails to actually protect receivers against spoofing attacks
- p=quarantine Sends suspicious emails to spam folders
- p=reject Blocks non-compliant emails entirely

While p=none provides valuable visibility, it offers no actual protection. Today's standards increasingly require p=reject as the only truly effective defense against domain spoofing and impersonation attacks.

The transition to these stricter requirements has created challenges for organizations still operating with antiquated email systems. Migration timelines have been accelerated by major providers setting firm deadlines for compliance, fostering a rapid industry-wide shift toward more secure email infrastructure.

Let’s review some of the recent changes affecting the industry and what these strategic shifts mean for users.

The Ultimate Guide to Email Security Protocols

The recent sendee requirements introduced by Google, Yahoo, Microsoft and Apple focus on several key areas to enhance security, improve trust, and protect users from phishing, spam, and other malicious activity.

The regulations imposed by these providers include:

- SPF and DKIM Authentication
- DMARC Implementation (p=none)
- DMARC Alignment
- Valid rDNS (PTR)
- TLS Encryption
- Spam Complaint Threshold
- List-Unsubscribe Header and One-Click Unsubscribe
- Unsubscribe Processing Timeline
- Valid “From” and “Reply-To” Address
- Bounce Handling and List Hygiene

Requirement	Google	Yahoo
SPF Authentication	Required (All Senders)	Required (All Senders)
DKIM Authentication	Required (All Senders)	Required (All Senders)
DMARC Implementation	Required for Bulk (p=none OK)	Required for Bulk (p=none OK)
DMARC Alignment	Required for Bulk	Required for Bulk (Relaxed OK)
Valid Forward and Reverse DNS (PTR)	Required (All Senders)	Required (All Senders)
TLS Encryption	Required (All Senders)	Not Mentioned
Spam Complaint Rate	Must be < 0.3% (Postmaster Tools)	Must be < 0.3%
One-Click Unsubscribe	Required for Bulk	Required for Bulk
List-Unsubscribe Header	Implied by one-click requirement	Required (mailto: or POST)
Unsubscribe Processing Timeline	Not Specified	Must honor within 2 days
Valid “From” / “Reply-To” Addresses	Required	Required
Bounce Handling / List Hygiene	Required	Expected for Deliverability

Requirement	Microsoft (Outlook)	Apple (iCloud Mail)
SPF Authentication	Required (Bulk Senders Only)	Required (Bulk Senders)
DKIM Authentication	Required (Bulk Senders Only)	Required (Bulk Senders)
DMARC Implementation	Required for Bulk (p=none OK)	Required for Bulk Senders
DMARC Alignment	Required for Bulk (prefer SPF & DKIM aligned)	Not Specified
Valid Forward and Reverse DNS (PTR)	Not Mentioned	Required (Bulk Senders)
TLS Encryption	Not Mentioned	Not Specified
Spam Complaint Rate	Not Specified	Not Specified
One-Click Unsubscribe	Recommended	Required for Bulk Senders
List-Unsubscribe Header	Recommended	Not Specified
Unsubscribe Processing Timeline	Not Specified	Immediate
Valid “From” / “Reply-To” Addresses	Required for Bulk	Required for Bulk Senders
Bounce Handling / List Hygiene	Recommended for Bulk	Required for Bulk Senders

1. SPF and DKIM Authentication

SPF (Sender Policy Framework)

SPF is a DNS TXT record that **declares which IP addresses or hostnames are authorized to send emails on behalf of a domain**. This is tied to the `RFC5321.MailFrom`, also known as the envelope sender. SPF validation is done by checking the return-path domain against the connecting IP.

To set up SPF, analyze your DMARC aggregate reports, investigate the sending sources used, and adjust your SPF record to allow the necessary hostnames and IP addresses using EasyDMARC’s SPF Generator tool.

DKIM (DomainKeys Identified Mail)

DKIM is used to digitally sign emails with the help of asymmetric cryptography. The sender signs the message with a private key, and the recipient verifies the message with the public key, which is published in the DNS. **DKIM signs email headers and parts of the email body to ensure the content wasn't tampered with**.

SPF and DKIM make sure the message is authenticated, but they cannot provide protection for the domain used in the "from" address.

This is where DMARC and alignment come in.

Note:

The best approach to adjusting your SPF and DKIM records is to analyze your DMARC aggregate reports to understand all the sources sending on behalf of your domain. These reports help you identify authorized and unauthorized senders by IP address. However, reviewing raw DMARC XML files can be complex, as they often lack readable source names.

2. DMARC Implementation (p=none)

DMARC builds on SPF and DKIM to **give domain owners control over what happens when authentication or alignment fails**. It also provides visibility into your domain's email traffic through reporting.

All major email platform providers require a p=none policy. This is the monitoring mode of DMARC and represents the first step in a domain's DMARC journey. These providers do not currently require a RUA (Reporting URI for Aggregate data) tag, but it's strongly recommended.

What are Aggregate Reports?

DMARC aggregate reports are **XML documents providing authentication status information for your email traffic**. These reports offer essential visibility into all sources using your domain, help identify spoofing attempts, reveal configuration issues affecting deliverability, verify compliance, and build confidence for implementing stricter policies.

By analyzing this aggregate data, organizations can better protect their email domains while ensuring legitimate messages reach their destinations.

Why a RUA Tag is Recommended

Without a RUA tag, domain owners have no visibility into who is sending emails on their behalf. DMARC reports sent to an address utilizing a RUA tag can identify misconfigurations in SPF or DKIM, unaligned senders, and spoofing attempts. **These reports are essential for analyzing alignment, understanding real-world email behavior, and moving toward enforcement** (p=quarantine or p=reject).

Note:

The p=none designation is a monitoring mode, not enforcement, but it's still the safest way to begin DMARC implementation. DMARC works at the domain level, so even one misconfigured service can lead to mail delivery issues. With p=none, you can to observe authentication and domain alignment without risking mail loss.

As you understand your authentication and alignment more, you can move towards implementing p=reject. EasyDMARC helps by offering segmentation, traffic classification, source validation, and policy recommendations, so you can enforce DMARC safely.

3. DMARC Alignment

DMARC requires domain alignment between the domain specified in the "from"' header (`RFC5322.From`) and the domain associated with either SPF (the RFC5321.MailFrom) or DKIM (indicated by the "d=" tag in the signature). **Alignment can be either relaxed by default or strict**. Default alignment means subdomains are allowed (`mail.example.com` can align with `example.com`), while strict alignment requires domains to match exactly. While DMARC only mandates that either SPF or DKIM pass and align with the "From" domain, employing both is best practice.

Some providers handle bounce messages using their own return-path, which breaks SPF alignment. In those cases, DKIM alignment becomes critical.

Note:

Passing SPF or DKIM doesn't mean DMARC will pass. For DMARC to pass, your domain (**`From:`**) needs to align with the domain used in SPF (**`Return-Path`**) or DKIM (**`d=`**).

For example, if you're using SendGrid but haven't set up your own domain's SPF and DKIM, their default will be set to **`sendgrid.net`**. SPF and DKIM may pass, but alignment will fail, and so will DMARC. Email service providers provide CNAMEs setups to fix alignment and make DMARC work on your domain.

4. Valid rDNS (PTR)

The sending IP must have a valid PTR record (reverse DNS, or rDNS), meaning that **the IP should resolve to a fully qualified domain name**, and that domain should resolve back to the same IP address. This requirement applies mainly to senders using self-hosted MTAs (Mail Transfer Agents) and dedicated servers or IPs.

5. TLS Encryption

TLS (Transport Layer Security) encryption makes sure that emails are encrypted during transmission between sending and receiving servers. While SPF, DKIM, and DMARC verify the sender's identity, TLS secures the delivery path by preventing interception and tampering.

- Providers like Google, Yahoo, Microsoft, and Apple expect all senders to support TLS encryption during transmission.
- Your mail server must offer and accept secure TLS connections when sending and receiving email.
- TLS enforcement is different, and involves MTA-STS (Mail Transfer Agent – Strict Transport Security).

MTA-STS allows domain owners to ensure incoming emails are only accepted if sent over a secure TLS connection. If TLS cannot be established, the message will be rejected or deferred based on the policy. This prevents downgrade attacks and ensures encrypted delivery by default.

TLS-RPT (TLS Reporting)

TLS reporting provides reports on successful and failed TLS negotiations. It **helps identify misconfigurations, invalid certificates, or gaps in secure delivery**.

> **Note:**
> Most ESPs already have TLS enabled, but if you're running your own mail servers, make sure STARTTLS is properly configured. Email without TLS is like shouting your message across a crowded room; anyone can listen.

6. Spam Complaint Threshold

Mailbox providers are now actively monitoring spam complaint rates with a maximum allowed threshold of 0.3%. **This means that if you send 1,000 emails, you must receive fewer than three complaints**.

Spam complaints are user-generated, meaning they occur when a recipient manually clicks “Report as spam.” They are not related to technical bounces. Maintaining a healthy complaint rate involves only sending to opted-in recipients, honoring unsubscribe requests, and using consistent sender identity and content.

You can use the Google Postmaster integration in our EasySender platform to monitor your spam complaint rate and other important parameters.

Note:

Spam complaint thresholds are one of the most difficult things to control. Gmail, Outlook, and Yahoo all have their own thresholds. Keeping a spam rate under 0.10% is recommended, though most industry players agree that you need to stay under 0.3% to avoid deliverability issues. That's three complaints per 1,000 emails (per provider, not overall).

If you're getting too many complaints, you're either targeting the wrong audience or not segmenting your lists properly. Make sure to review your email strategy and hygiene

7. List-Unsubscribe Headers and One-Click Unsubscribes

Gmail, Yahoo, Microsoft, and Apple all recommend or require marketing and bulk senders to support one-click unsubscribes via headers, not just links inside the email body. This feature enables email clients to display a native unsubscribe button next to the sender in the user interface.

To comply, two headers must be included:

```
List-Unsubscribe: <mailto:unsubscribe@yourdomain.com>,
<https://yourdomain.com/unsubscribe>

List-Unsubscribe-Post: List-Unsubscribe=One-Click
```

- The `List-Unsubscribe` header provides one or more unsubscribe methods: a `mailto:` or HTTPS link.
- The `List-Unsubscribe-Post` header tells the client that the HTTPS endpoint supports one-click HTTP POST unsubscribe.

Google, in particular, explicitly requires both headers. If `List-Unsubscribe-Post` is missing, Gmail won't trigger one-click unsubscribe. The HTTPS link in the `List-Unsubscribe` header must respond to a POST request without redirects or confirmation pages. Failing to support this properly will increase your complaint rate, and Gmail will treat the sender as non-compliant.

Note:

Beyond appearing legitimate, Unsubscribe headers and one-click unsubscribes are about avoiding spam complaints. Adding **`List-Unsubscribe`** headers helps mailbox providers identify you as a safe sender, with Gmail supporting "one-click unsubscribe," which users can trigger directly from the interface. This improves trust and reduces frustration.

If you use the same "From" address for both marketing and transactional emails, unsubscribing from one might block the other. Segment your sender addresses accordingly.

8. Unsubscribe Processing Timeline

In addition to one-click unsubscribe support, email service providers are enforcing unsubscribe processing deadlines. Yahoo requires senders to honor unsubscribe requests within two business days, while Apple iCloud requires near-immediate action. Gmail and Outlook track whether senders honor unsubscribe requests in a timely manner, but do not specify any timeframe.

The header must be present, and unsubscribes must be automatically and reliably handled. Failing to process requests promptly can lead to compliance violations and increased complaint rates.

Note:

Despite Yahoo offering two business days and others not specifying a timeline, best practices dictate processing immediately. Some ESPs let you customize suppression logic, while others enforce it instantly. If you're running your own system, your unsubscribe logic must take effect immediately, or you risk getting marked as spam. If someone unsubscribes and still receives emails, even by accident, that's a red flag for your domain reputation.

9. Valid "From:" and "Reply-To:" Address

The "**From:**" and "**Reply-To:**" headers must use **valid, routable, and monitored email addresses**. They must not bounce, they should be able to receive replies, and they should be actively monitored by support or marketing teams. Using invalid or non-existent reply addresses can damage trust and trigger delivery failures or spam filtering.

Note:

Using **`no-reply@`** is now outdated and can hurt engagement. Always use a real email address in your **`"From:"`** and **`"Reply-To:"`** headers and continuously monitor it. It shows you're open to feedback and improves your trust score.

10. Bounce Handling and List Hygiene

Proper bounce handling is important for reputation management. Hard bounces where the user is not found must result in immediate removal from future sends. Soft bounces, where the email was delivered properly but could not enter the receiver's mailbox due to other reasons (server failures, full inboxes, message was too long, etc.), should be tracked and monitored. Repeated soft bounces should be temporarily suppressed.

List hygiene stipulates removing inactive users, avoiding purchased or scraped address lists, and confirming opt-ins. **Sending to outdated or unverified lists increases bounce rates and spam complaints**, as well as reducing engagement, all of which negatively affect inbox placement.

Note:

If you're using an email service provider, bounces are auto-handled. If you're self-hosting, you need to track hard and soft bounces, as ignoring hard bounces can destroy your sender score.

Implement a sunset policy by removing users who haven't opened an email in 90 to 180 days. A bloated list looks good for numbers, but hurts deliverability. **It's better to have 1,000 engaged users than 10,000 inactive ones.**

Steps to Securing Email Deliverability

With email providers enforcing stricter authentication rules, businesses must take proactive steps to comply, or they risk email deliverability issues. If your domain lacks DMARC, SPF, or DKIM, or if you're using unauthenticated third-party services, it’s time to take action.

Here’s a step-by-step guide to ensure your emails stay secure and reliably reach inboxes:

1. Activate DMARC Reporting
2. Authenticate All Legitimate Sources
3. Reach DMARC Enforcement
4. Customize Tracking URLs
5. Include Unsubscribe Options
6. Monitor Bounce Rate

1. Activate DMARC Reporting

The first step is visibility. Set up a DMARC record with a policy of **p=none** and include an RUA (Aggregate Reports) address. This allows you to start receiving XML reports from ISPs, giving you visibility into who is sending emails using your domain and whether those sources are passing SPF and DKIM checks. These reports are essential for understanding your full email ecosystem before making changes.

2. Authenticate All Legitimate Sources

Once you have DMARC reports, the next step is analysis. Investigate which sending sources are legitimate and make sure they are properly authenticated with SPF and/or DKIM. Any misconfigured or missing records should be fixed to ensure these sources become DMARC-compliant.

3. Reach DMARC Enforcement

After confirming that all legitimate senders are authenticated correctly, gradually move your DMARC policy from p=none to p=quarantine, and eventually to p=reject . This protects your domain from spoofing and phishing by blocking unauthorized senders.

4. Customize Tracking URLs

If you're using marketing or automation platforms, make sure the tracking URLs are customized and aligned with your domain (e.g., click.yourdomain.com). Generic tracking links used by many other senders can negatively impact deliverability and domain reputation.

5. Include Unsubscribe Options

Include list-unsubscribe headers and clear opt-out options in your emails. This improves engagement rates and reduces the chance of your messages being marked as spam. It’s also a growing requirement among major mailbox providers.

6. Monitor Bounce Rate

Regularly monitor your bounce rates and remove invalid or inactive email addresses. Keeping your email list clean reduces delivery failures, improves sender reputation, and boosts engagement metrics.

Key Takeaways

From Monitoring to Enforcement: The Next Step in Email Security

It’s clear that email security is becoming non-negotiable for more email security providers. The move towards enforcing protocols like SPF, DKIM, and DMARC aims to reduce phishing, spoofing, and spam, making email safer for everyone. For businesses, this means adapting to new industry standards, improving deliverability, and protecting your brand’s reputation.

However, simply having a DMARC record in place isn’t enough.To fully benefit from DMARC, organizations must move beyond passive monitoring and commit to active enforcement.

Only a policy set to p=reject can truly block malicious emails pretending to be from your domain. Organizations must now progress beyond monitoring-only DMARC implementations (p=none) to actively enforcing p=reject policies that protect their domains and their recipients from increasingly sophisticated email-based attacks.

EASYDMARC

James Sanford

james@teamspring.us

www.teamspring.us