Become a Verified Email Marketing Sender

A complete guide to better your understanding of how to comply with the NEW Gmail and Yahoo DMARC Requirements, even for novice users.

About This Guide

This guide is designed for business owners, operators, marketers, and anyone managing email campaigns who want to improve their email deliverability and comply with Gmail and Yahoo's updated DMARC requirements. It's especially helpful for non-technical users who might feel overwhelmed by email authentication processes.

Who is this guide for?

- ✓ If you send marketing or transactional emails, failing to comply with these requirements could result in your messages landing in spam folders—or being rejected entirely. By following this guide, you'll ensure your emails reach your audience, maintain your sender reputation, and protect your domain from being used in phishing or spoofing attacks.

Complying with the NEW Gmail and Yahoo DMARC Requirements

This checklist simplifies the technical steps to comply with Gmail and Yahoo's new DMARC (Domain-based Message Authentication, Reporting, and Conformance) requirements, ensuring your emails land in inboxes—not spam folders.

Disclaimer: This guide is for informational purposes only and does not guarantee compliance, accuracy, or specific results. Please check with your email marketing platform provider for further assistance and guidance on the most up-to-date information to ensure you follow best practices.

1. Understand the Basics

What is DMARC?

“DMARC” is a policy that tells email providers how to handle messages that fail authentication checks. It helps reduce spam and phishing.

DMARC, which stands for “Domain-based Message Authentication, Reporting and Conformance,” is an open email authentication protocol that provides domain-level protection of the email channel.

Why Does DMARC Matter?

If you don’t comply, your emails could be automatically flagged as spam, or rejected altogether by your recipients’ email servers.

Beginning in February 2024, Yahoo has been enforcing certain standards for all senders, including properly authenticating your mail, and keeping complaint rates low. The requirements for bulk senders will be more strict, including, enabling easy, one-click unsubscribe, authenticating with both SPF and DKIM, and publishing a DMARC policy.

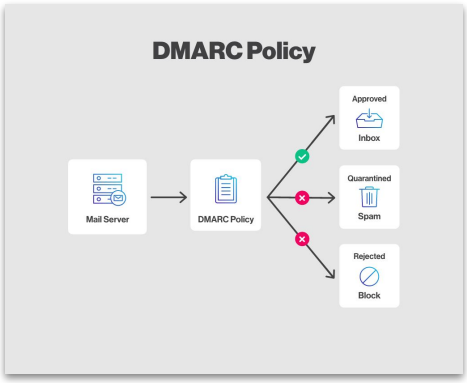

Image Source: CyberImpact

2. Gather What You'll Need

In order to begin this process, you'll need:

- ❏ Access to your domain registrar or DNS hosting provider (e.g., GoDaddy, namecheap.com SiteGround, Cloudflare, Squarespace Domains, etc.)

  Note: If you're unsure, this is likely whoever you pay annually for your domain registration.

- ❏ Admin-level access to your email marketing platform (e.g., Klaviyo, Mailchimp, Constant Contact, or wherever you send your subscribers emails from).

- ❏ Your domain name (eg. yourdomainexample.com)

  Note: Your domain name does *not* include "www" or "http://"

If you do not have all of the above, please do not proceed with this process until you do. Contact your website developer or host, or email marketing platform for help, if needed.

3. Check Your Domain's Current Email Authentication

1. Use a free tool like MxToolBox to check your domain's existing DNS records for SPF, DKIM, and DMARC.

   MxToolBox DMARC Check Tool can be found here: https://mxtoolbox.com/dmarc.aspx

2. Note any missing records—SPF, DKIM, or DMARC—these will need to be added or updated.

3. Recommended step: Copy all DNS records into a spreadsheet for future reference. This is also helpful if you accidentally alter or delete records.

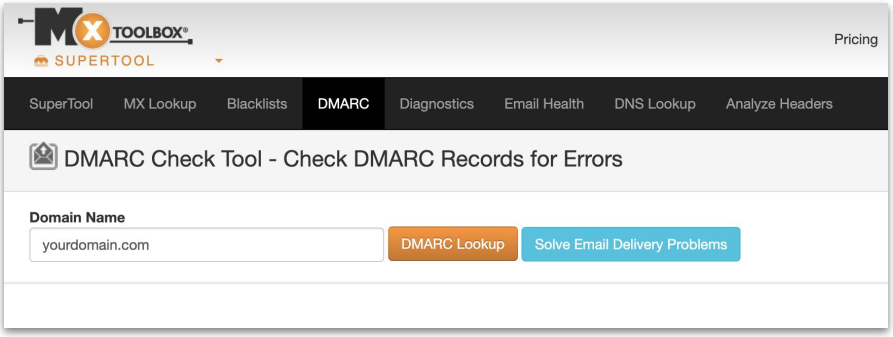

Image Source: MxToolBox

4. Set Up SPF (Sender Policy Framework)

1. Log in to your domain registrar or DNS hosting provider.
2. Navigate to where you can manually manage, add, or edit DNS records.
3. Add or update the SPF ‘TXT’ record for your domain:

    Example SPF record:

    i. Type: TXT

    ii. Name or Host:

    iii. “v=spf1 include:your-email-provider.com ~all”
4. Confirm that the record includes all authorized email services (e.g., your email marketing platform and transactional email providers).
5. Note: If required to enter a TTL value for any DNS record, you can use “3600” as a default setting.

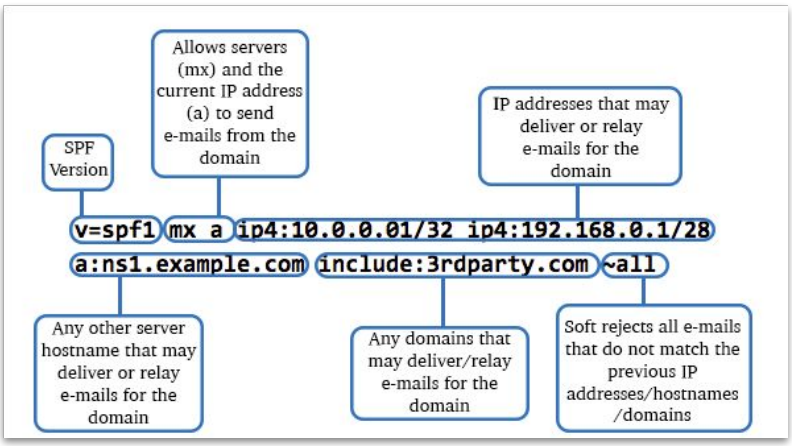

Image Source: Easy DMARC

5. Set Up DKIM (DomainKeys Identified Mail)

1. Go to your email marketing platform and locate the DKIM settings (often found under domain authentication or email sending settings).
    a. Your email marketing platform may require you to first enter a branded domain (your domain) before DKIM keys are provided. Once this has been added successfully, your email marketing platform usually provides records for you to add in your DNS Zone. Start adding the records in order, from top to bottom.
2. Copy the DKIM keys provided by your platform.
    a. These records will likely be CNAME type DNS records.

    Example:

        1. Type: CNAME
        2. Name or host: send
        3. Value: u8552959.we029.sendgrid.net

    b. And include TXT type DNS records as well.

    Example:

        1. Type: TXT
        2. Name or host: default._domainkey
        3. Value: v=DKIM1; k=rsa; p=YourPublicKeyHere
3. Save and verify the DKIM setup in your email platform.
4. Note: If required to enter a TTL value for any DNS record, you can use “3600” as a default setting.

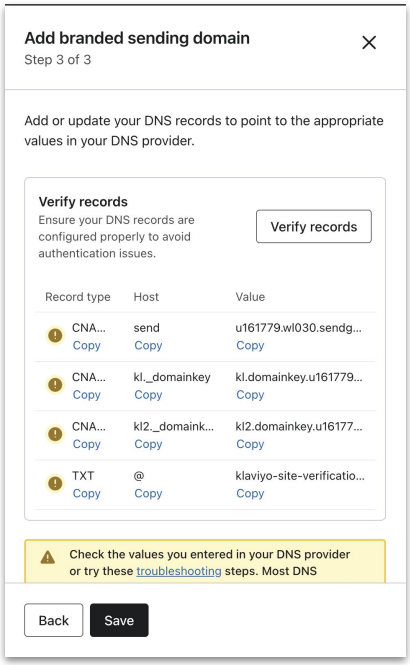

Image Source: Easy DMARC

6. Implement DMARC

1. Decide on your DMARC policy:
    a. “None”: Monitors emails but doesn’t enforce policy (good for testing, or for beginners if you’re unsure if you’ve correctly set up your DMARC record).
    b. “Quarantine”: Sends failed emails to spam.
    c. “Reject”: Blocks failed emails (best for compliance).
2. Add the DMARC TXT record to your domain:

    Example:

    Type: TXT

    Name or host: _dmarc

    Value: “v=DMARC1; p=quarantine; rua=mailto:your-email@domain.com; ruf=mailto:your-email@domain.com”
3. Note: Replace “your-email@domain.com” with your email address for receiving DMARC reports.
4. Note: If required to enter a TTL value for any DNS record, you can use “3600” as a default setting.

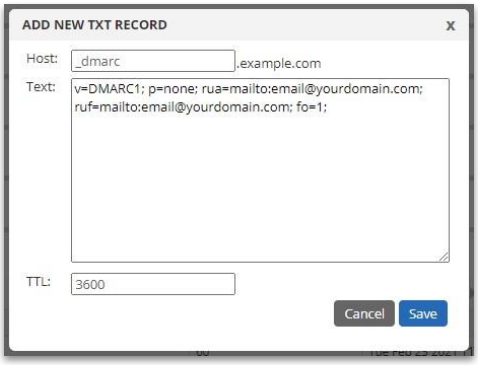

Image Source: Easy DMARC

7. Test Your Configuration

1. Use an email testing tool like Mail Tester or GlockApps to ensure SPF, DKIM, and DMARC are working.

   Mail Tester can be found here: https://www.mail-tester.com/

2. Send test emails to check if they pass authentication.

3. Note: If your test emails don't pass authentication, please review all previous steps in this guide or follow prompts in the Mail Tester response feedback. You can also try following steps in the Troubleshooting Help section, located toward the end of this guide.

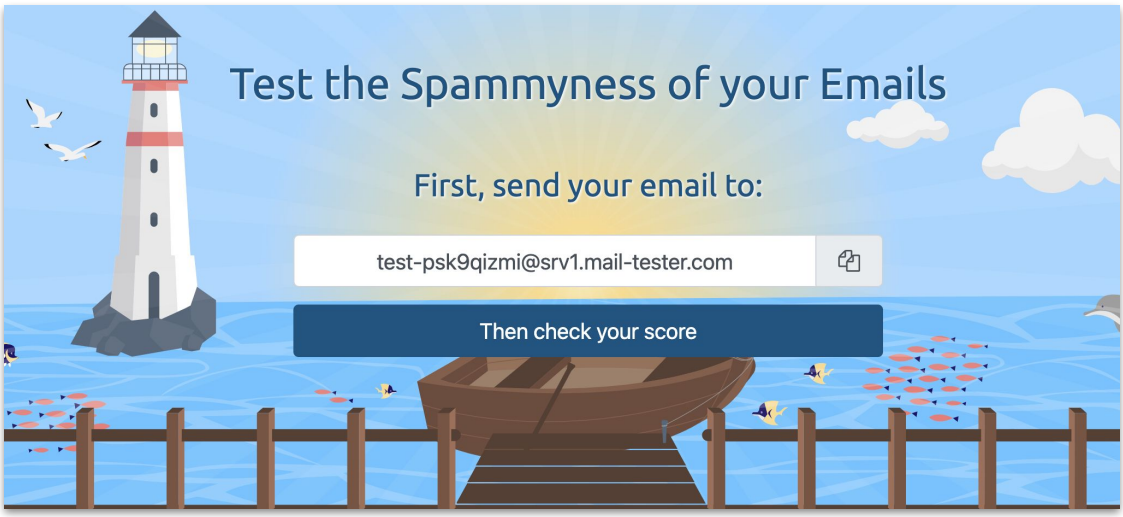

Image Source: Mail Tester

8. Keep Your Records Updated

1. Regularly review your DNS records to ensure they are up to date with your email service providers.
2. Adjust SPF and DKIM records as you add new email platforms.
3. Note: As a best practice, anytime you add or edit DNS records of any type, keep track of these changes in a spreadsheet for future reference.

Congratulations!

You've completed this guide and tested your DMARC settings! You're now a verified email marketing sender, and on your way to better compliance and email deliverability results.

By following this checklist, you've ensured your domain complies with Gmail and Yahoo's DMARC requirements, improving email deliverability and reducing spam complaints.

Troubleshooting Help

1. **Misconfigured Records:** Double-check for typos or incorrect DNS entries.
2. **SPF Record Too Long:** Avoid exceeding the 255-character limit by combining entries or using subdomains.
3. **Forgetting to Verify:** Always verify SPF and DKIM after adding them.

External Resources

Below are external resources to help you complete the checklist process.

MxToolBox DMARC Check Tool

✓ https://mxtoolbox.com/dmarc.aspx

WhoIs DNS Records Check Tool

✓ https://who.is/

Mail Tester

✓ https://www.mail-tester.com/

Easy DMARC Step by Step Guide

✓ https://easydmarc.com/blog/klaviyo-spf-and-dkim-setup-step-by-step/

Disclaimer

This guide is for informational purposes only and does not guarantee compliance, accuracy, or specific results. Please check with your email marketing platform provider for further assistance and guidance on the most up-to-date information to ensure you follow best practices.

Settings described for SPF, DKIM, and DMARC DNS (Domain Name Setting) records are typical for most use cases, but may conflict with valid settings or records and may impact your email or website's performance. If you are unsure, please contact your webmaster, website or DNS host, or email marketing expert.

Any third-party tools, links, or websites referenced (e.g., MxToolBox) are provided solely for convenience. Arbuckle Media does not endorse these tools or guarantee their functionality, accuracy, or the outcomes of using them. Always use your discretion and consult with a professional if needed.