DMARC - Important Update and Implications for Email Compliance

What is it?

If you send 5,000 messages a day or more to either of the world's largest mailbox providers (**Gmail and Yahoo**), starting February 2024, your email domain must have a DMARC policy in your DNS.

These messages must pass DMARC Alignment or they will not be delivered.

This includes messages sent on behalf of your organization by third-party email service providers (ESPs) like Constant Contact and MailChimp that use your email domain.

Why is it important?

To help understand why this is important, please review these reference sites.

Why is it crucial for Third-Party Senders to comply with DMARC? (skysnag.com)

Making Sure Your Third-Party Email Services use DMARC | Mimecast

How To Make My Third-party Vendors DMARC-compliant? (powerdmarc.com)

Steps to DMARC compliance

- Set up SPF or DKIM email authentication for your domain.
- Ensure that sending domains or IPs have valid forward and reverse DNS records, also referred to as PTR records. Learn more
- Use a TLS connection for transmitting email. For steps to set up TLS in Google Workspace, visit Require a secure connection for email.
- Keep spam rates reported in Postmaster Tools below 0.10% and avoid ever reaching a spam rate of 0.30% or higher. Learn more about spam rates.
- Format messages according to the Internet Message Format standard (RFC 5322).
- 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.

https://support.google.com/a/answer/81126?hl=en-#zippy=%2Crequirements-for-all-senders

How can I check my setup is compliant?

There are many tools out there you can use to check however, a couple that our team have found to be most useful are -

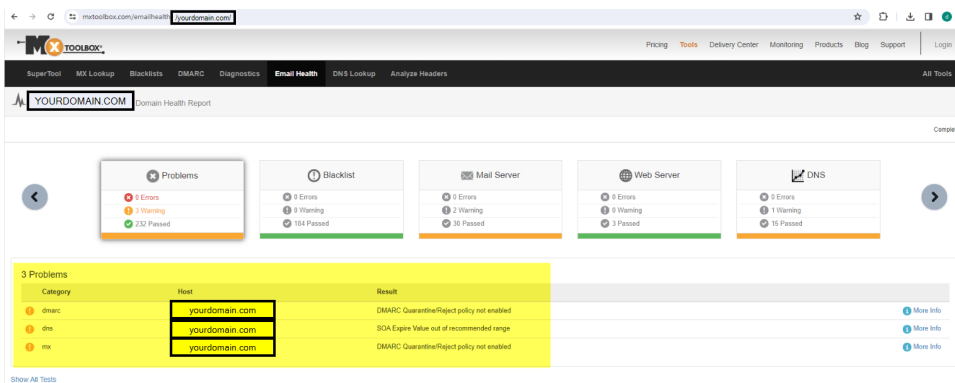Domain Health Check - Online Domain Tools - Blacklist, Email, Website, DNS - MxToolBox

DMARC Inspector - dmarcian

We found mxtoolbox.com to be simple to use and provide lots of useful information in a pretty easy-to-read format. Below are the steps taken to demonstrate the usage:

1. Load the browser and navigate to https://mxtoolbox.com/

2. Click on [Email Health] then enter the domain or email address that you want to check (e.g. www.yourdomain.com), and click [Check Email Health]
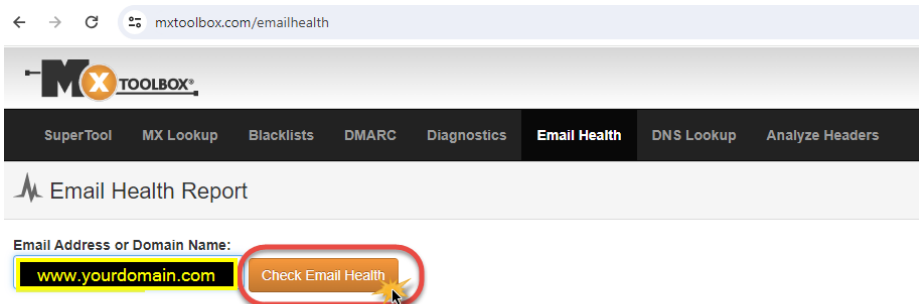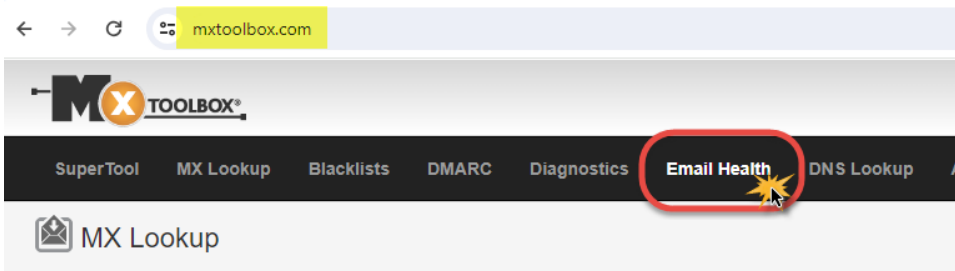
3. The site then helps assess the deliverability of emails sent from the domain by performing tests and analyzing factors that can impact successful email delivery. Any problems found will be displayed:

4. Click on [Mail Server] to display detailed results:

5. Here you can see that while DMARC record has been found on the domain, the Quarantine/Reject policy has not been enabled, i.e. it is still set to NONE.

6. Now try repeating the above steps for http://ZoomInfo.com

7. You can see that DMARC record is found and DMARC Quarantine/Reject policy is enabled

Support

If you require assistance, please reach out to our support team for additional help from our team.

Want to learn more?

https://support.google.com/a/answer/81126

https://dmarcian.com/yahoo-and-google-dmarc-required/

- Email Template List
- Widget-Based Email Templates
- Review sent emails
- Sender Policy Framework (SPF) Record
- CC Order Confirmation emails