Are You Aware Of That Your Emails To Gmail And Yahoo! Could Be Rejected Effective February 1, 2024 If You Don't Set Up Your DMARC, SPF & DKIM Email Authentication For Your Sending Domain?

Dear Email Sender, **Google** and **Yahoo!** have implemented mandatory strict new rules on electronic security.

On October 3, 2023, **Google and Yahoo** announced **A Mandate** **requirements that bulk senders** **must have DMARC in place beginning February 2024**.

What happens if you ignore Google and Yahoo's mandate requirements to Authenticate DMARC?

Ignoring DMARC (Domain-based Message Authentication, Reporting, and Conformance) in your email security strategy can pose several risks and vulnerabilities. DMARC is designed to combat **email phishing** and **fraud** by providing a way for email senders to authenticate their emails and protect recipients from malicious activities. Here are some dangers associated with ignoring **DMARC**:

Increased Phishing Attacks:

- Without DMARC, cybercriminals can exploit the lack of authentication and send phishing emails that appear to be from legitimate sources. This increases the risk of recipients falling victim to phishing attacks, leading to credential theft, malware infections, or other malicious activities.

Brand Impersonation:

- DMARC helps prevent domain spoofing and brand impersonation. Ignoring DMARC leaves your domain vulnerable to abuse by attackers who may impersonate your brand in phishing campaigns, potentially harming your organization's reputation.

Email Fraud and Business Email Compromise (BEC):

- DMARC plays a crucial role in preventing email fraud and BEC attacks. Without DMARC, attackers may successfully carry out scams that involve financial fraud, unauthorized access to sensitive information, or fraudulent activities on behalf of an organization.

Lack of Visibility and Reporting:

- DMARC provides reporting mechanisms that allow domain owners to gain insights into who is sending emails on their behalf and how those emails are being handled by email providers. Ignoring DMARC means missing out on valuable visibility and reporting capabilities, making it harder to monitor and analyze email activities.

Impact on Email Deliverability:

- Email providers increasingly use DMARC policies to determine whether to deliver or reject emails. If your domain lacks a DMARC policy or has a weak policy, legitimate emails may be at risk of being marked as spam or rejected by email filters, impacting your overall email deliverability.

Regulatory Compliance Issues:

- In some industries, regulatory compliance requires organizations to implement email authentication mechanisms like DMARC. Ignoring DMARC may result in non-compliance with industry regulations, leading to potential legal consequences and fines.

Loss of Trust Among Users:

- If your email domain is frequently used for phishing attacks, it can erode trust among your users and customers. Users may become skeptical of emails from your domain, affecting communication and potentially causing disruptions to legitimate business operations.

To mitigate these risks, it's important to **implement DMARC** and configure it appropriately. Regularly monitor DMARC reports, adjust policies, and take action based on the information received. Working towards DMARC enforcement helps ensure that only authorized senders can use your domain, reducing the likelihood of phishing and fraudulent activities.

What Are The Benefits Of Implementing DMARC Authentication?

Email Authentication:

- DMARC authenticates emails by allowing senders to publish policies for their domain. This helps ensure that only authorized senders can use the domain, reducing the risk of domain spoofing and impersonation.

Phishing Prevention:

- DMARC helps prevent phishing attacks by making it more difficult for attackers to impersonate trusted domains. It verifies the authenticity of the sender's domain, reducing the likelihood that recipients will fall victim to phishing scams.

Brand Protection:

- By preventing domain spoofing and brand impersonation, DMARC protects the reputation of your organization and helps build trust among recipients. It ensures that emails sent on behalf of your domain are legitimate and not malicious.

Enhanced Email Deliverability:

- Many email providers use DMARC policies to determine whether to deliver, mark as spam, or reject incoming emails. Implementing DMARC with a policy of enforcement can positively impact email deliverability by reducing the chances of legitimate emails being marked as spam.

Visibility and Reporting:

- DMARC provides reporting mechanisms that allow domain owners to gain insights into how their domain is being used for email communication. These reports include information about email authentication status, sources of email traffic, and potential abuse.

Policy Gradual Enforcement:

- DMARC allows for a phased implementation, enabling organizations to start with a monitoring-only (p=none) policy. This allows them to analyze reports and gradually move towards enforcement (p=quarantine or p=reject) once they are confident in the authentication status of their emails.

Compliance with Industry Standards:

- In certain industries, regulatory compliance requires the implementation of email authentication mechanisms. DMARC is recognized as an industry standard for email authentication and is often a requirement for compliance with regulations.

Reduced Risk of Business Email Compromise (BEC):

- DMARC helps protect against Business Email Compromise (BEC) attacks, where attackers attempt to impersonate trusted individuals within an organization to carry out financial fraud or unauthorized activities.

Notification of Authentication Failures:

- DMARC allows domain owners to receive notifications when authentication failures occur, giving them the opportunity to investigate and take corrective actions. This proactive approach helps organizations stay informed about potential abuse of their domain.

Global Email Security Standard:

- DMARC is a widely adopted and recognized email security standard. Implementing DMARC aligns your organization with best practices in email authentication and contributes to the overall improvement of global email security.

By **implementing DMARC**, organizations can significantly enhance their email security posture, protect their brand, and contribute to a safer email environment for both senders and recipients.

So Starting February 1, 2024, senders who send more than 5,000 messages per day to Gmail accounts or yahoo must meet the requirements in this section:

1. **SPF and DKIM Setup:**
   - Implement SPF and DKIM email authentication for your domain.

2. **DNS Records Validation:**
   - Ensure that sending domains or IPs possess valid forward and reverse DNS records (PTR records).

3. **TLS Connection:**
   - Use a TLS connection for transmitting email. Find steps to set up TLS in Google Workspace here (https://support.google.com/a/answer/2520500).

4. **Spam Rate Management:**
   - Maintain spam rates below 0.10% in Postmaster Tools and avoid exceeding a spam rate of 0.30% or higher.

5. **Message Formatting:**
   - Format messages according to the Internet Message Format standard (RFC 5322).

6. **DMARC Setup:**
   - Set up DMARC email authentication for your sending domain. Set the DMARC enforcement policy to none.

7. **Unsubscribe Support:**
   - Marketing and subscribed messages must facilitate one-click unsubscribe, with a clearly visible unsubscribe link in the message body.

8. **Email Service Provider Verification:**
   - If you use an email service provider, (aweber, mailchimp, etc.) verify that they authenticate your domain's email with SPF and DKIM. Always use your DOMAIN's email for marketing and autoresponders.

9. **Consistent Domain Usage:**
   - We recommend using the same domain for email authentication and hosting your public website.

Take Action Now:

Failure to comply with these requirements may lead to email delivery issues, spam classification, and susceptibility to **spoofing & phishing**. Act promptly to address non-compliance before the specified deadline.

How do you know if you are in compliance with Gmail mandate DMARC authentication already? Here's how.

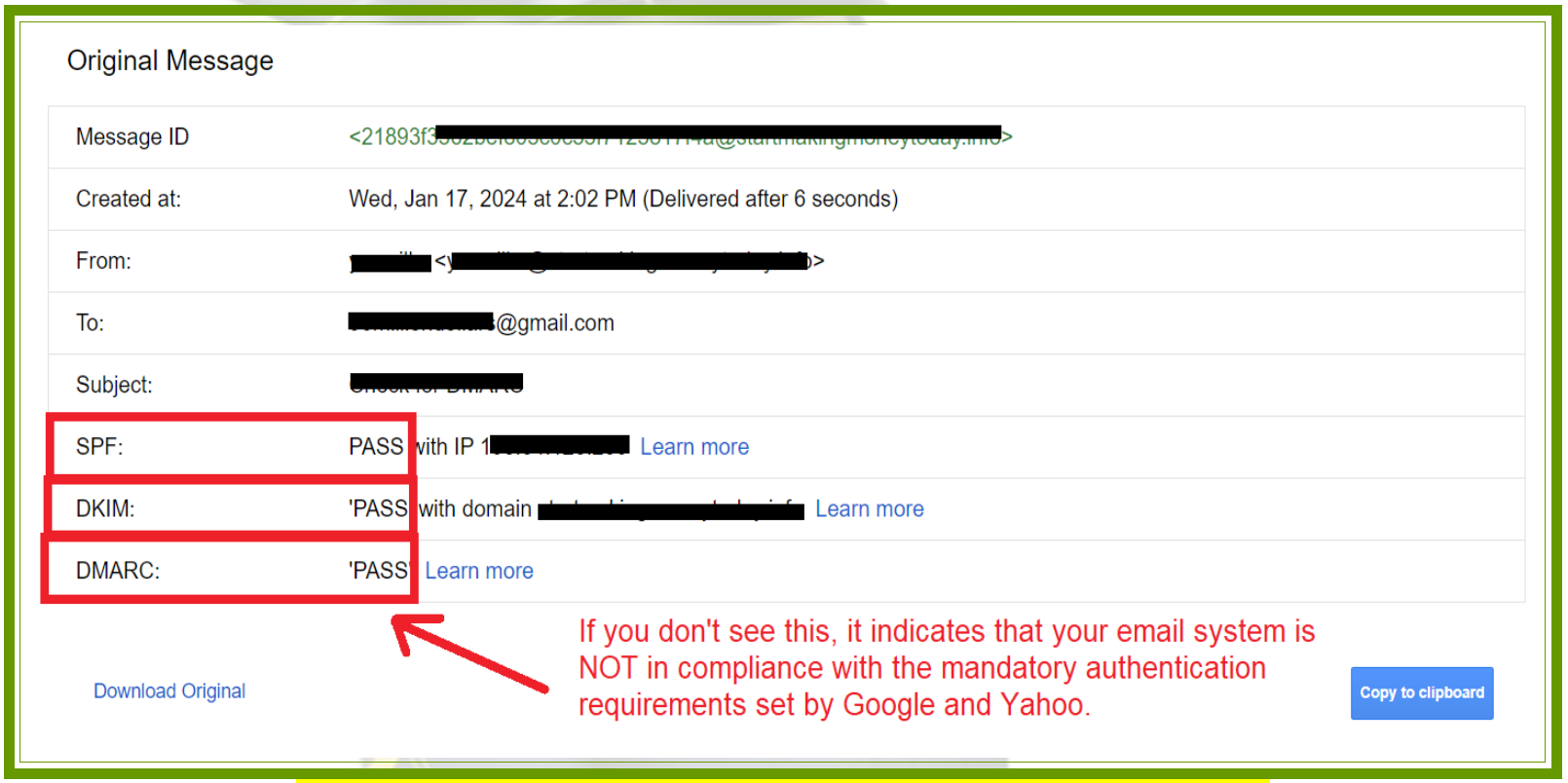
Send an e-mail from your "DOMAIN" web interface account to YOUR gmail account.
Example: If your business account is: "**support@networkmarketing.com**", send it from there, NOT from any other email account.

FROM: support@networkating.com
TO: your@gmail.com

Once you get the email from your business account to your gmail.com account, open it and click on the **3 dots** on the top right corner, and click on "**show original**"

Once you do that, it will open in a new window.
On that window you should be able to see the following (image below)

SPF: PASS
DKIM: PASS
DMARC: PASS



If you do not have a DOMAIN, you need to get one ASAP!

If you DO NOT see what the image above shows, then you need to make the changes immediately!

How Do You Make The Changes?

You can make the changes from your DNS/Cpanel and edit the DMARC, SPF & DKIM.

WARNING: If you don't have experience with editing information in your Cpanel or DNS, we don't recommend you even try to do it, as this could break something in your host or websites. **Avoid at all costs**.

If you are familiar with editing your Cpanel/DNS, and you know exactly what you need to do, g**o ahead and do it IMMEDIATELY before is too late**.

Otherwise, if you prefer to have someone more experienced do it for you, to protect yourself, prevent spam, **spoofing & phishing** with Gmail authentication, by **setting up DMARC email authentication, SPF & DKIM**, **let us know and contact us, and we will help you get it all done before it damages you even more**.

If you require assistance, contact us via text at: (209) 730-6530

Save Our Website: **CLICK HERE TO GO TO OUR WEBSITE**

¡Hablamos Español!
Visit our Spanish version BY CLICKING HERE.

Hope this information proves helpful.