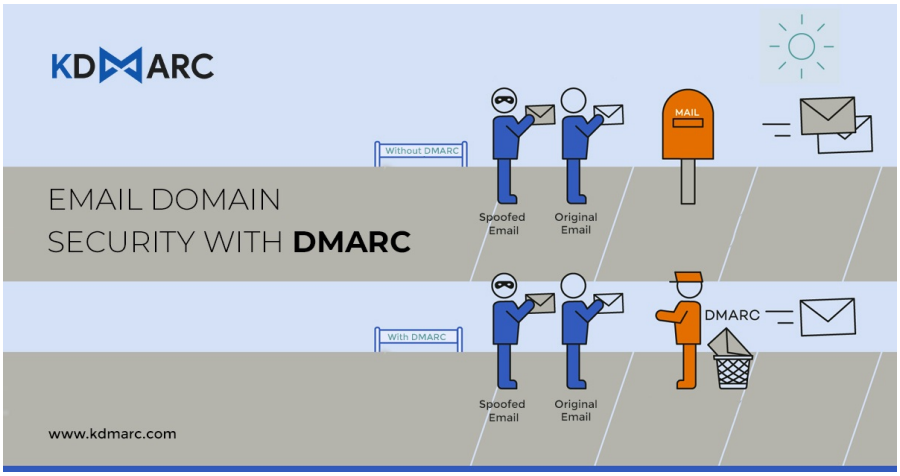
DMARC: A Prerequisite for Email Domain Security

DMARC: A Prerequisite For Email Domain Security

0 Comments (https://blog.kdmarc.com/blog/dmarc-a-prerequisite-for-email-domain-security/#respond) dmarc (https://blog.kdmarc.com/blog/dmarc/) **Dhwani Meharchandani (https://blog.kdmarc.com/blog/author/dhwani/)**
January 20, 2021



Domain-based Message Authentication Reporting and Conformance (DMARC) is an effective email validation system that protects your organization's email domain from being misused to carry out malicious activities like email spoofing and phishing scams. It monitors the two existing email authentication techniques: **Sender Policy Framework (SPF)** and **DomainKeys Identified Mail (DKIM)**.

It provides domain owners with insights into who is sending emails from their domain, giving them detailed information about their outbound email channel. This email authentication protocol offers the best way of ensuring that your customers or clients will only receive the emails sent by you. It assures your customers of the legitimacy of an email, resulting in an improved deliverability rate and domain reputation.

WHY IS DMARC IMPORTANT?

As per a **report (https://www.hacksplaining.com/prevention/email-spoofing)**, 95% of all emails sent over the internet end up in the spam box. And, the majority of these spam emails are sent using spoofed addresses. A cyber criminal can use your organization's domain name to send emails to your customers to trick them into giving up their credentials or other sensitive information.

If your email domain is impersonated, it can disrupt your relationship with your customers and impact your organization's reputation. It can also affect your domain's email deliverability and engagement rates. Once your domain reputation starts deteriorating, even the legitimate outbound emails may be redirected to spam or fail to deliver.

Securing your domain with DMARC can help in preventing impersonators from forging your domain name and sending fraudulent emails on your behalf. It gives you insights into your email channel and the sources trying to misuse your domain. Moreover, it helps in boosting your domain's engagement and deliverability rates.

WHAT DOES DMARC DO?

DMARC's primary function is to detect and stop email spoofing. For instance, a phishing scam impersonating the domain of a bank sends out emails to its customers stating that their accounts have been frozen and prompting them to click on a link to unfreeze them. Customers, assuming that the email is legitimate, click on the embedded link that leads them to a fraudulent website. When the customers log in, cyber criminals will get access to their credentials.

Email authentication techniques like SPF and DKIM were designed to protect your domains from such scams. However, cyber criminals have evolved their tactics and can easily bypass these security measures. To fully secure your email channel and domain, DMARC establishes a link between DKIM and SPF. Once you have implemented DMARC, ISPs send Forensic (RUF) and Aggregate (RUA) DMARC reports to the email address published in your DMARC record every day.

Here is some information about the two types of reports available:

AGGREGATE REPORTS (RUA)

Aggregate reports are sent to your email address every day for providing a detailed overview of your domain's email traffic. These reports include a list of all the IP addresses that have attempted to send emails using your domain name.

FORENSIC REPORTS (RUF)

Forensic reports send you real-time alerts in case emails sent from your domain fail to deliver. These reports always include original message headers and may include original messages.

HOW DOES DMARC WORK?

Flowchart Representation of How DMARC Works

DMARC enables you to determine what to do with the emails that fail the DMARC checks. You can define a policy in your domain's DMARC record. This policy instructs the email ISPs how to handle an email that fails the DMARC check. The email receiving server checks if an incoming email has valid DKIM and SPF records and whether these records align with the sending domain.

Once all these details have been checked, the ISP determines whether an email is DMARC failed or DMARC compliant. When an email's authentication status is verified, the email receiving server handles it according to the policy set by you.

Here are the three possible DMARC policies available:

NONE

The **none policy (p=none)** instructs the ISPs to send the reports to the email address published in the RUF or RUA tag of your domain's DMARC record. This is also known as a Monitoring only policy as it helps you gain deep insight into your email channel. This policy will not affect the email deliverability and will allow all emails to reach the recipient's inbox, no matter whether it fails or passes the DMARC authentication.

QUARANTINE

Apart from sending reports, the quarantine **policy (p=quarantine)** instructs the ISPs to redirect emails failing the DMARC authentication to the recipient's spam folder. Emails passing the DMARC authentication will be successfully delivered to the recipient's primary inbox. Even though this policy mitigates the impact of spoofing, the spoof emails will still be able to reach the receiver.

REJECT

Besides sending reports, the **reject policy (p=reject)** instructs the ISPs to not deliver emails failing the DMARC authentication at all. Emails passing the DMARC authentication will be successfully delivered to the recipient's primary inbox. Since this policy prevents all spoofed emails from landing in the recipient's inbox, it mitigates the impact of spoofing.

Notably, email receivers aren't obligated to follow the policy set by you. Sometimes, they can override DMARC policies with a local policy in case they have reasonable thoughts about the legitimacy of an email. So, an email that has failed the DMARC authentication can still land

into the recipient's primary inbox even if you have enforced the reject policy.

Secure your email domains with **KDMARC (https://kdmarc.com/?utm_source=DMARC%3A%20A%20Prerequisite%20for%20Email%20Domain%20Security&utm_medium=KDMARC%20Blog&utm_cam** to prevent advanced email-based attacks like BEC, spoofing and impersonation.

Get KDMARC Freemium (https://app.kdmarc.com/register?utm_source=DMARC%3A%20A%20Prerequisite%20For%20Email%20Domain%20Security&utm_medium=KDMARC%20Blog&utm_campaign=Blog)

Tags: DMARC (https://blog.kdmarc.com/blog/tag/dmarc/) DMARC Policies (https://blog.kdmarc.com/blog/tag/dmarc-policies/) DMARC record (https://blog.kdmarc.com/blog/tag/dmarc-record/) email dmarc explained (https://blog.kdmarc.com/blog/tag/email-dmarc-explained/) How does DMARC work? (https://blog.kdmarc.com/blog/tag/how-does-dmarc-work/) KDMARC (https://blog.kdmarc.com/blog/tag/kdmarc/) What is a DMARC report? (https://blog.kdmarc.com/blog/tag/what-is-a-dmarc-report/) What is dmarc (https://blog.kdmarc.com/blog/tag/what-is-dmarc/)

Previous Post
University Email Accounts Hijacking Drives Phishing and Malware Attacks
(https://blog.kdmarc.com/blog/university-email-accounts-hijacking-drives-phishing-and-malware-attacks/)

Next Post
7 Free Tools for Email Domain Security Checkup
(https://blog.kdmarc.com/blog/7-free-tools-for-email-domain-security-checkup/)

YOU MIGHT ALSO LIKE

(https://blog.kdmarc.com/blog/middle-east-organizations-need-to-be-alert-of-brand-exploitation/)
MIDDLE EAST ORGANIZATIONS NEED TO BE ALERT OF BRAND EXPLOITATION (HTTPS://BLOG.KDMARC.COM/BLOG/MIDDLE-EAST-ORGANIZATIONS-NEED-TO-BE-ALERT-OF-BRAND-EXPLOITATION/)

(https://blog.kdmarc.com/blog/email-borne-attacks-expected-to-hit-60-of-the-organizations-in-the-uae/)
EMAIL-BORNE ATTACKS EXPECTED TO HIT 60% OF THE ORGANIZATIONS IN THE UAE (HTTPS://BLOG.KDMARC.COM/BLOG/EMAIL-BORNE-ATTACKS-EXPECTED-TO-HIT-60-OF-THE-ORGANIZATIONS-IN-THE-UAE/)

(https://blog.kdmarc.com/blog/email-filters-are-helpless-when-these-phishing-messages-flow-in/)
EMAIL FILTERS ARE HELPLESS WHEN THESE PHISHING MESSAGES FLOW IN (HTTPS://BLOG.KDMARC.COM/BLOG/EMAIL-FILTERS-ARE-HELPLESS-WHEN-THESE-PHISHING-MESSAGES-FLOW-IN/)

CONTACT US

Kratikal Tech Pvt. Ltd.
A-130, Second Floor
Sector-63, Noida-201301
Phone: +91 9717792410
Email: sales@kratikal.com

POWERED BY

KRATIKAL
SECURE FOR SURE
(https://www.kratikal.com/)