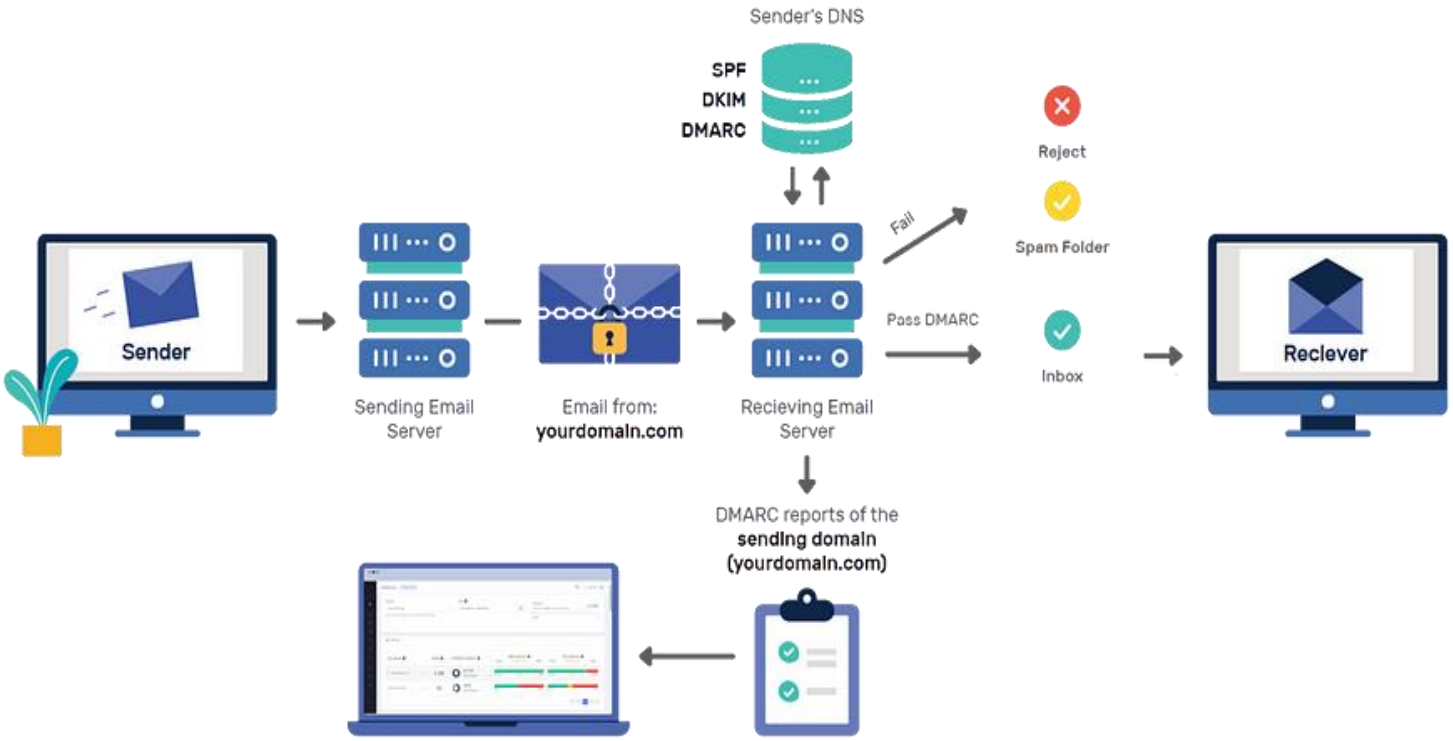
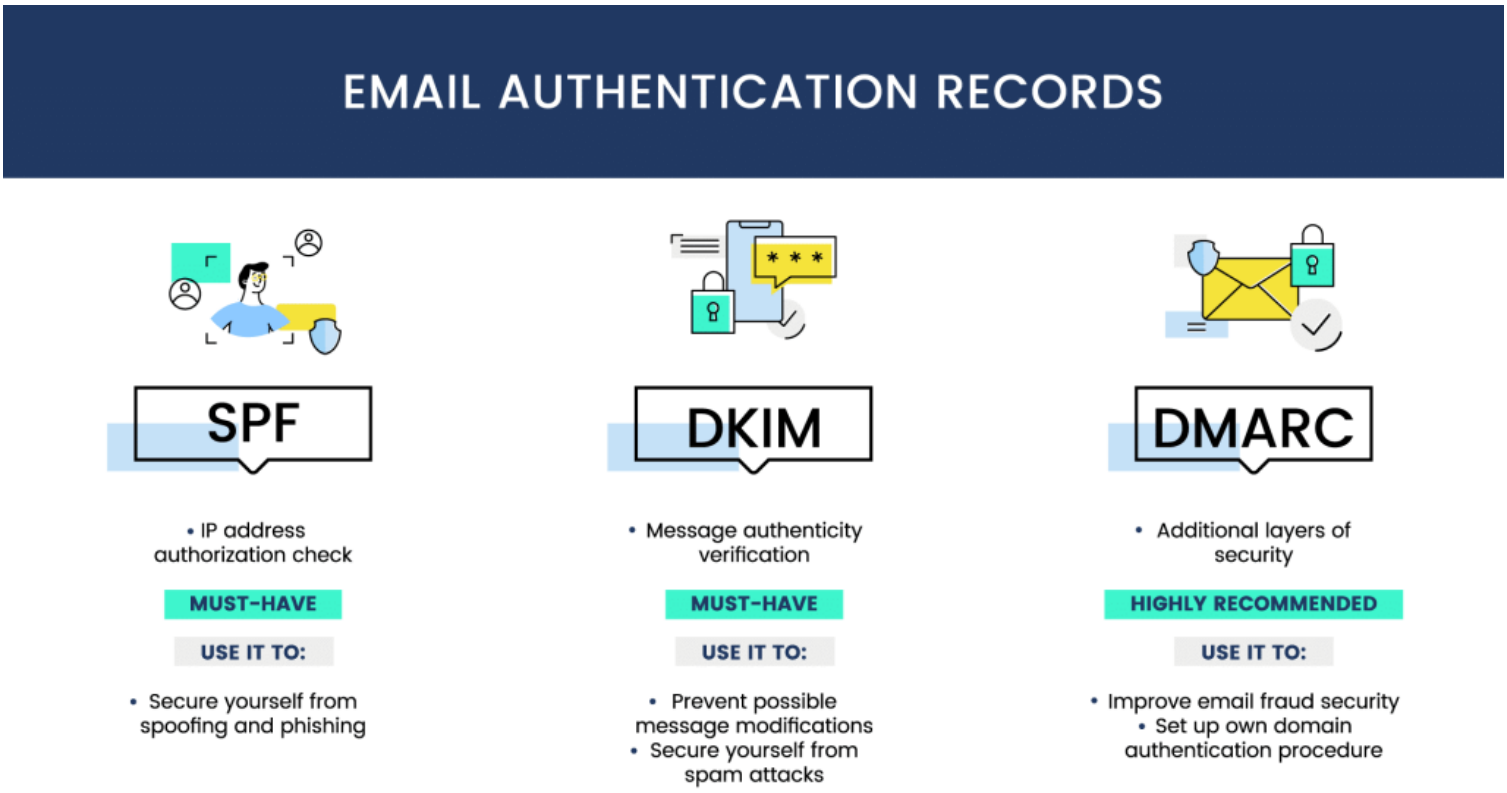
How SPF, DKIM, and DMARK work in your Email Flow



NELSON OJOVBO
https://www.linkedin.com/in/nelson-ojovbo/



Are simply a set of email authentication methods to prove to ISPs and mail services that senders are truly authorized to send email from a particular domain and, are a way of verifying your email-sending server is sending emails through your domain.

🚀 **Sender Policy Framework (SPF)**

- ❖ Defines a process for finding out whether a mail server is authorized to deliver email for a sending domain in DNS.

🚀 **DomainKeys Identified Mail (DKIM)**

- ❖ Defines a process for digitally signing and authenticating email messages as coming from an email server authorized to send email to the originating domain. ***DKIM signatures enable email providers to authenticate on behalf of the email domain owners***.

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

- ❖ Defines a process for discovering the appropriate response to receiving an email that fails to authenticate using **SPF (unauthorized email server) or DKIM (digital signature fails to authenticate).**

📁SPF

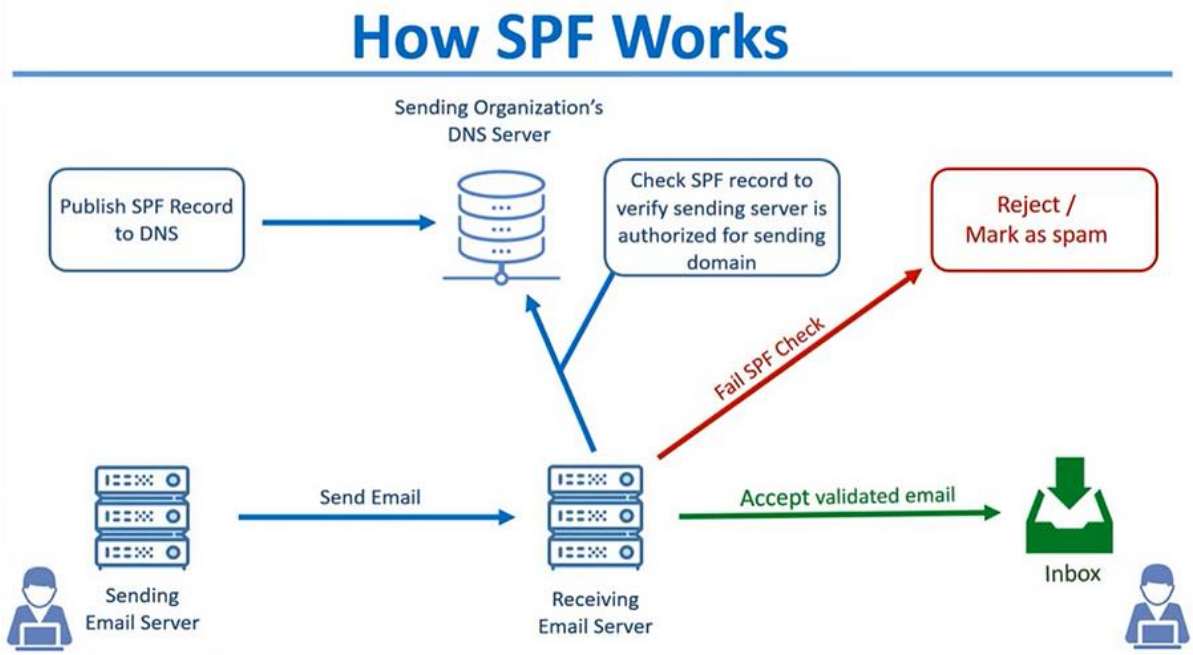
⚙️ SPF allows the owners of a domain to specify the mail servers authorized to send email on its behalf.

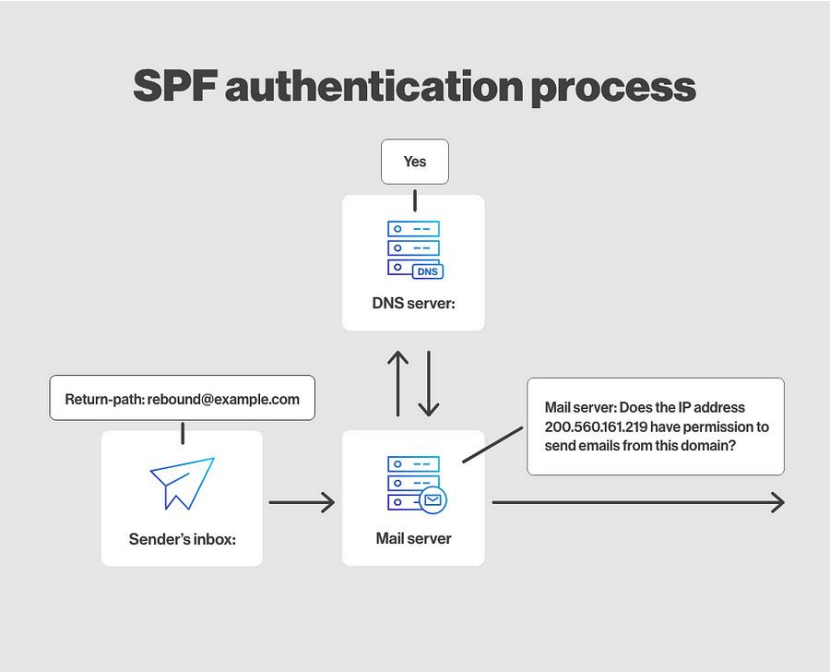
⚙️ SPF authentication is verified on the domain of the “**Return-path” address**.

⚙️ The SPF record is published in the DNS. The record is a list of all the IP addresses that are allowed to send email on behalf of the domain and it is listed as part of the domain’s overall DNS records.

Why use SPF

SPF authentication protects against identity theft by preventing the sending of fraudulent emails from unauthorized servers. This helps ensure that emails are sent by legitimate sources.





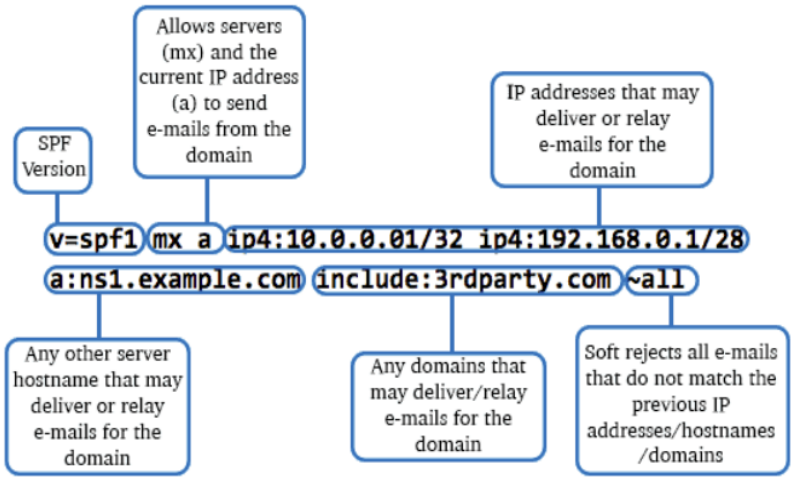
What does an SPF record look like?

An SPF record contains tags that give receiving email servers instructions on how to match incoming emails and handle failed authentications. There are two main components of an SPF record:

1. Mechanism
2. Qualifiers

This is how it may look:

```
v=spf1 a:mail.solarmora.com ip4:192.72.10.10 include:_spf.google.com ~all
```



SPF mechanisms are special elements or tags in an SPF record that show email servers what to match against the sender's address. Here are some of these elements:

- **v:** This is the first mechanism in every SPF record. It specifies the SPF version and in this case, the value is 1
- **a:** This specifies the authorized IP addresses in the A or AAAA records of the domain. If the domain has an A record that returns the sender's IP address, this mechanism passes
- **Ip4 or Ip6:** This specifies the Ip4 or Ip6 address respectively. The IP address range is given in the record and if the sender's address matches an address in the network range, this mechanism passes
- **mx:** This specifies the authorized email servers the sender uses to relay messages on behalf of the domain. The mx record of the domain is defined in the SPF record and a match is successful if the sender's IP is linked to the list of addresses in the record
- **include:** This specifies third-party IP addresses authorized to relay emails for the domain. This mechanism uses external mail servers' SPF records to match the sender's IP address. It returns a permanent error (PermError) if the third-party server has no SPF records
- **all:** This is the last mechanism in an SPF record and it defines how the incoming email server will handle any address that doesn't match other mechanisms. It uses qualifiers to determine what happens to the email after evaluating the addresses with other mechanisms

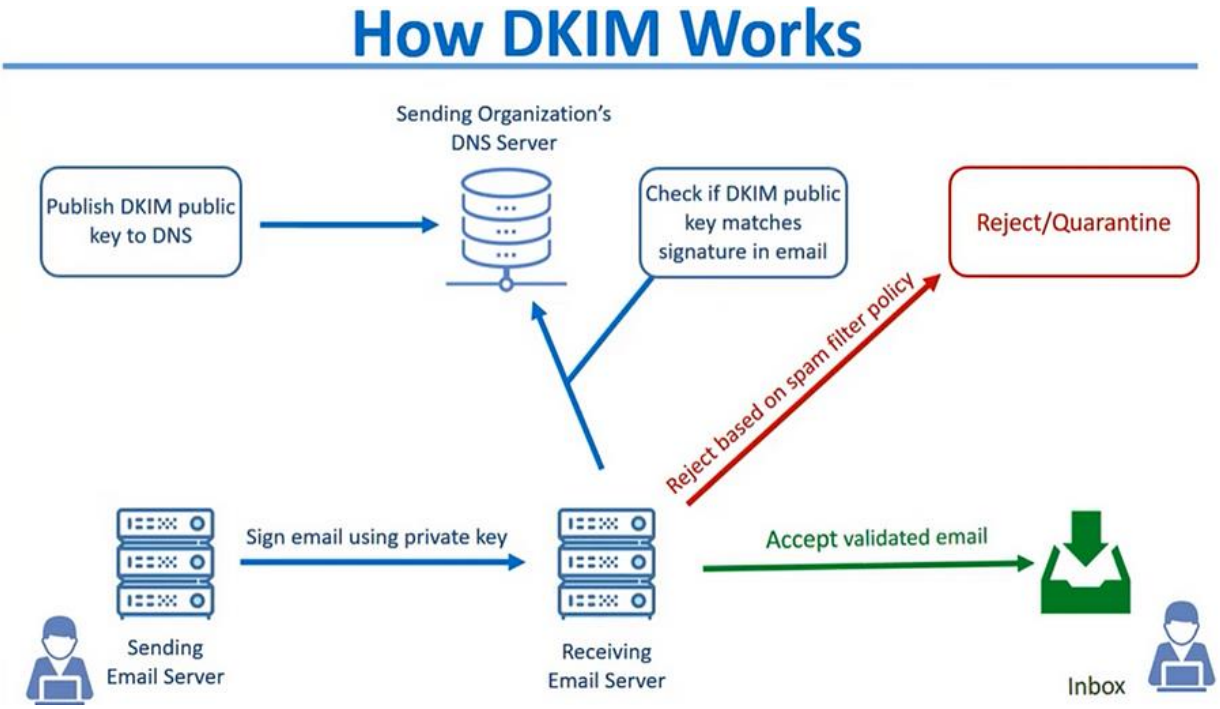
📁 What is DKIM?

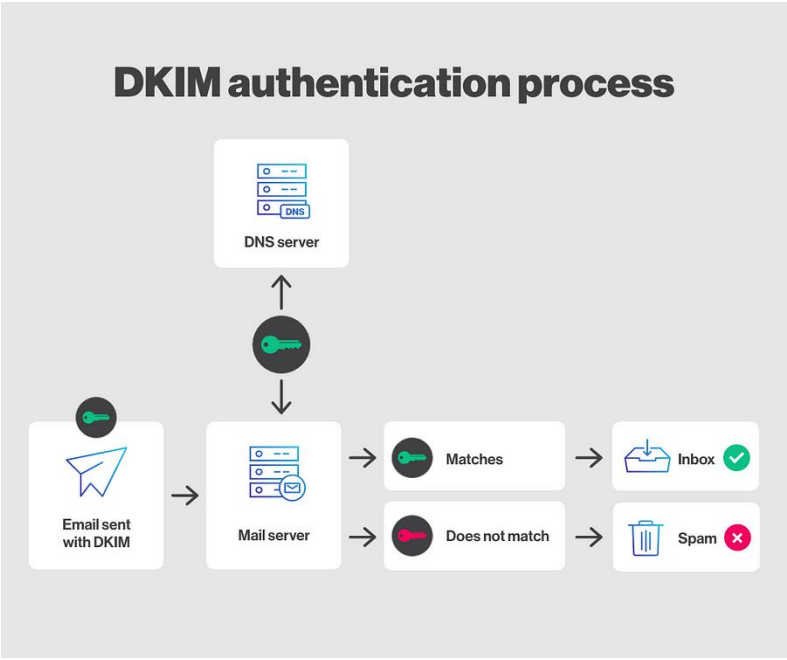
DMARC allows the domain owner to specify how unauthenticated messages should be treated. This approach detects spoofed or fake sender email addresses. It is also another way to link an email back to a domain.

⚙️ When using DKIM, a sender can attach DKIM signatures to an email (header that is added to the message and is secured with encryption), and once the recipient receives the email, they can verify who sent it.

How DKIM Works

DKIM Signs all outbound messages from a domain with a specific Key, called the **Private Key**. then The **Public Key** is published on a DNS server so that a receiving email server can compare and check if they match





📁 Why use DKIM

This signature (DKIM) is included in the headers of an email and is used to verify that the email was indeed sent by the claimed domain and has not been altered in transit. It also helps combat content forgery and strengthens recipient trust.

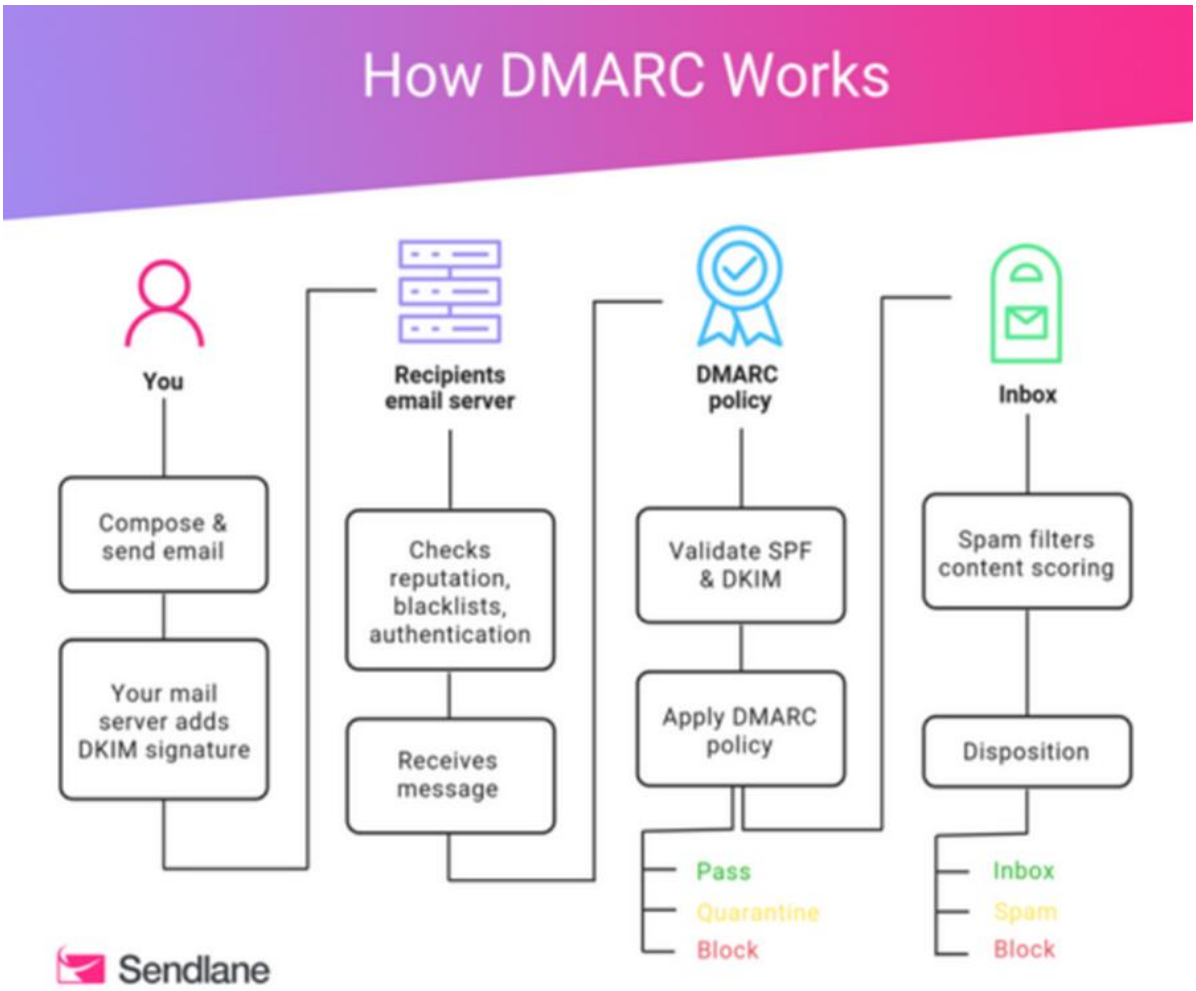
DMARC (Domain-based Message Authentication, Reporting, and Conformance)

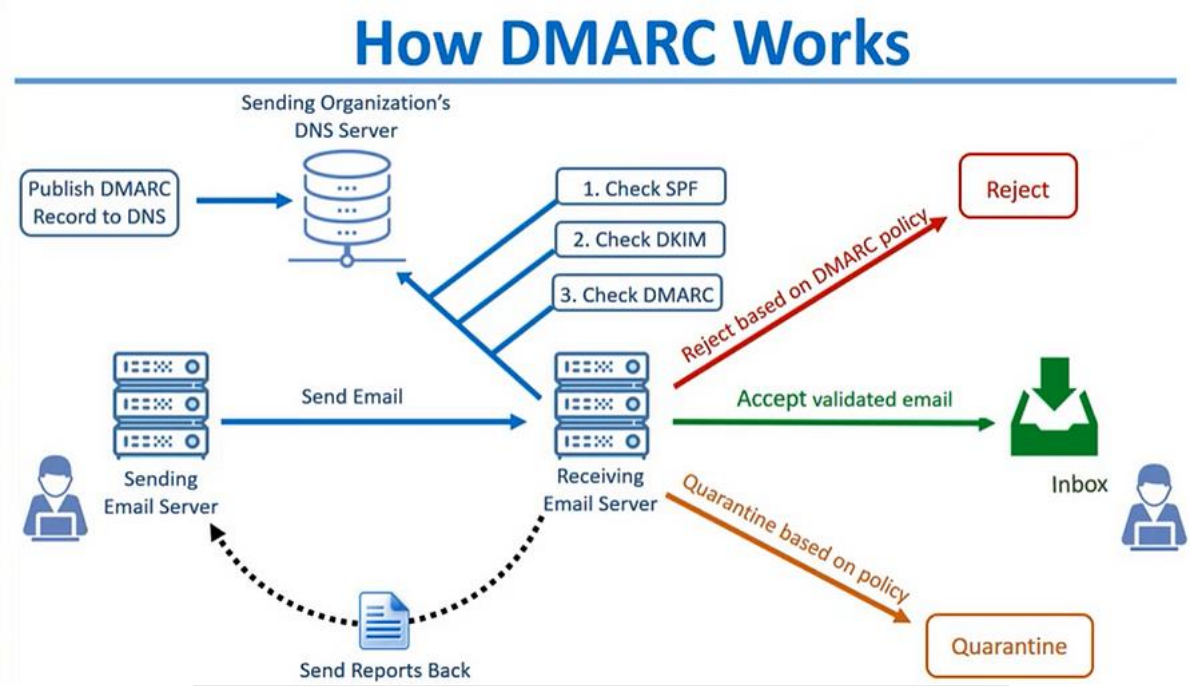
DMARC is an authentication method for ensuring that messages sent from your email address do come from you, and for specifying to others how emails that fail authentication tests should be handled.

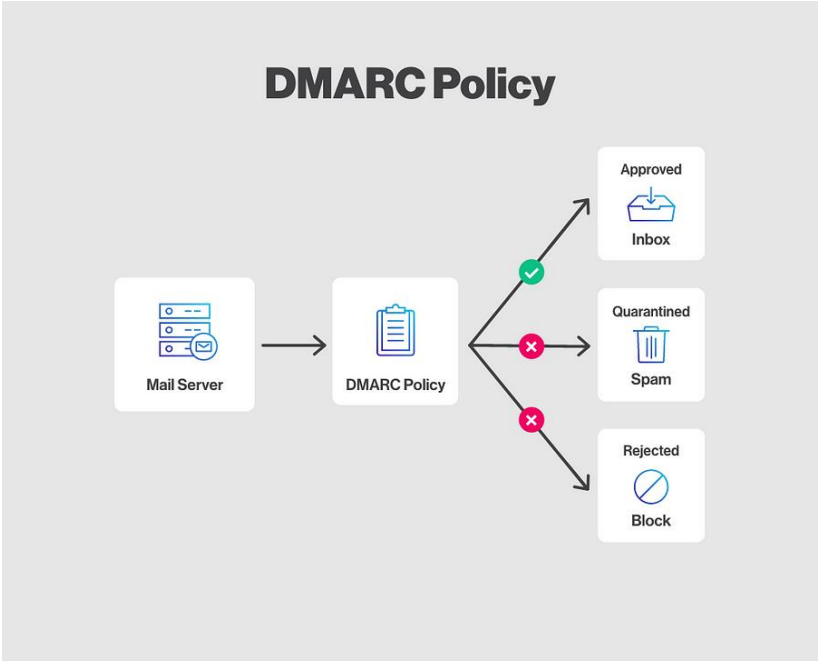
📁 For DMARC authentication to PASS:

A. The email must be correctly authenticated with SPF or a DKIM signature, and

B. The domain in the "**From**:" field (the visible header) must match the one of the SPF authentication or DKIM signature (also known as SPF or DKIM alignment).







📁 Why use DMARC

⚙️ The DMARC policy complements SPF and DKIM by providing an authentication policy for the domain.

⚙️ It helps define actions to be taken for emails that fail SPF and/or DKIM checks, such as quarantining or rejecting them.

⚙️ If someone tries to forge your email address, this will prevent forged emails from reaching their destination and damaging your reputation.

⚙️ Additionally, DMARC allows you to receive detailed reports on identity spoofing attempts if you include an email address in your record to receive them.

🚀 Differences Between SPF, DKIM, and DMARC 🚀

📁 SPF vs DKIM

● **SPF** allows email senders to define which IP addresses can send mail, while **DKIM** uses an encryption key and digital signature to verify an email.

● **SPF** doesn't use an encryption algorithm, while **DKIM** uses an encryption algorithm to create a pair of electronic keys.

● **SPF** is a protocol that adds information to the message envelope. Therefore, the forwarding server may remove sections of the message's envelope when you forward a message. **DKIM** works better when forwarding since the digital signature is kept with the email message as a part of the email header.

📁 SPF vs DMARC

- ❖ **SPF** works without **DMARC**. However, it will not be sufficient to rely just on SPF because it may have various flaws.
- ❖ **DMARC** validates the sender of an email using either DKIM or SPF records.
- ❖ **SPF** doesn't provide domain owners with a mechanism to send reports of failed deliveries.
- ❖ **DMARC** helps specify a reporting mechanism to assist receiving mail systems in determining what to do with messages sent from your domain that fails SPF or DKIM checks.

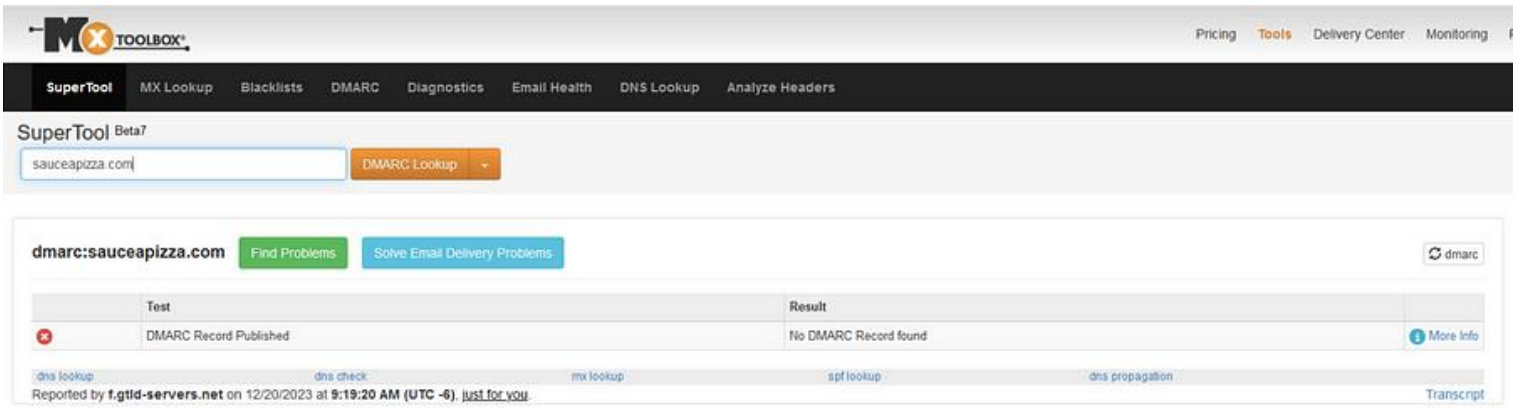
📁 DMARC vs DKIM

- ❖ DMARC works in conjunction with SPF and DKIM Records. So, if you want to implement a DMARC record, you have to set SPF and DKIM records first.
- ❖ DKIM does not require DMARC. However, using DKIM with DMARC helps to keep false negatives in DMARC.
- ❖ DMARC suggests what to do with mail that isn't legitimate, while DKIM tries to verify whether mail is legitimate or not.

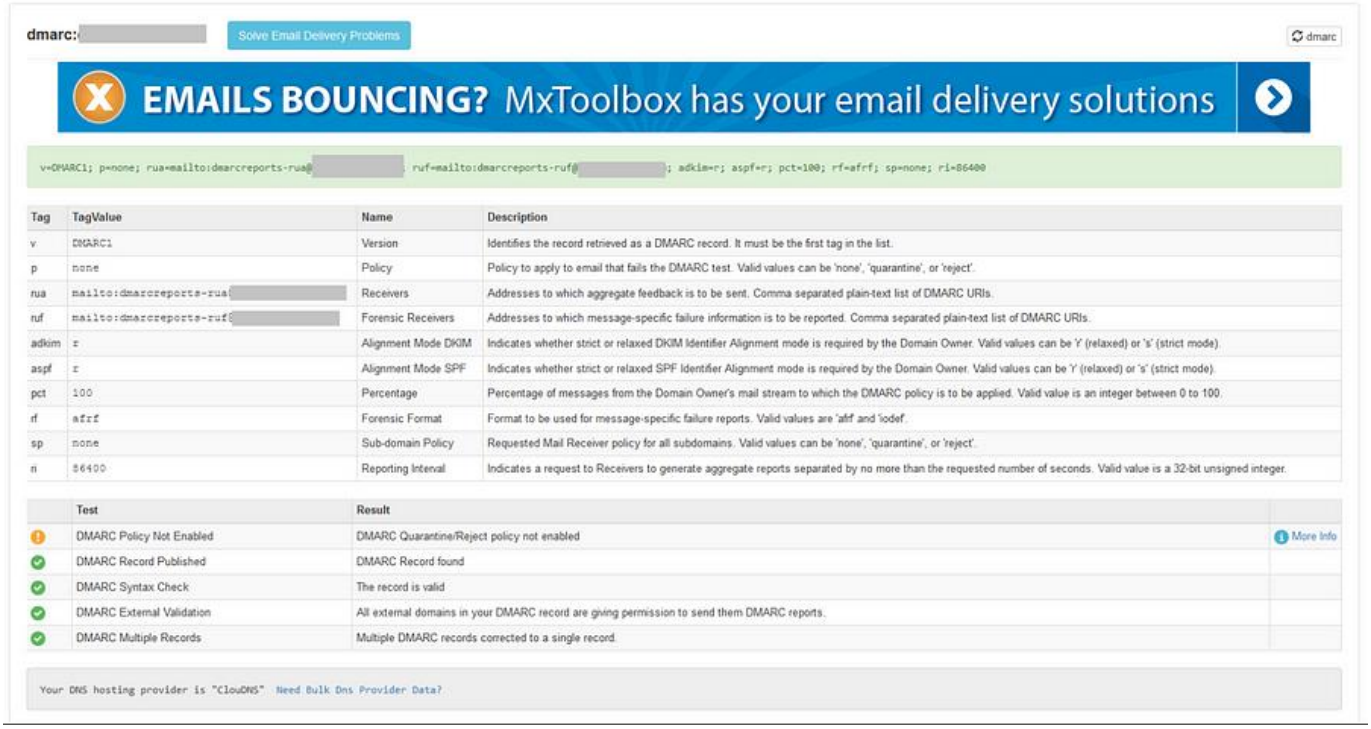
📁 To check if your Domain Name has DMARC authentication

You can check with online tools like **MXToolbox**. Simply enter your domain name (e.g., pizza.com) and launch the search by clicking on **DMARC Lookup.** The tool will show if a DMARC record is available in your domain.

Example of the result when there is no DMARC authentication found:



Example of the result when DMARC authentication is found:



Resources

- https://www.youtube.com/watch?v=c9fLp5uIxp8
- https://www.techtarget.com/searchsecurity/answer/Email-authentication-How-SPF-DKIM-and-DMARC-work-together
- https://snov.io/blog/how-to-set-up-spf-dkim-dmarc/
- https://www.cloudflare.com/learning/email-security/dmarc-dkim-spf/
- https://faq.cyberimpact.com/en/articles/1415/what-is-spf-dkim-and-dmarc-authentication