

DMARC

Domain-based Message Authentication, Reporting & Conformance

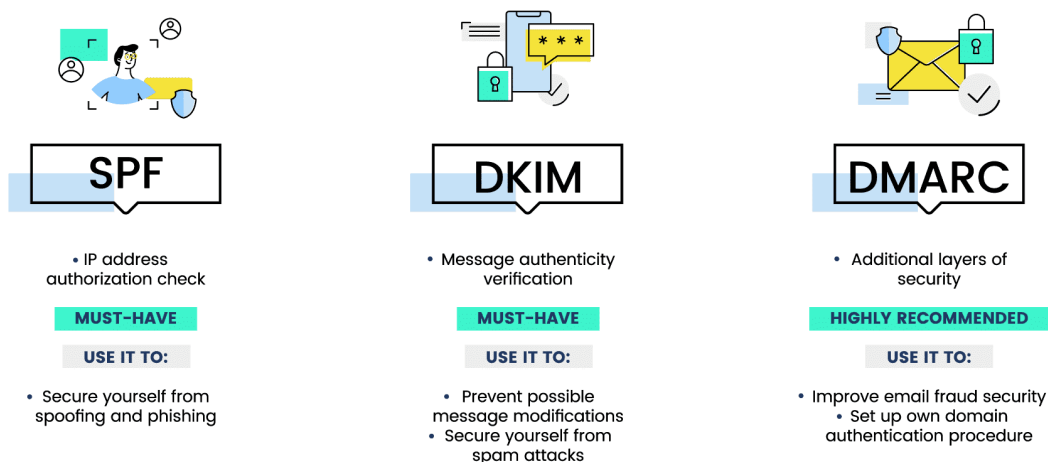
**DKIM, SPF,
DMARC**



DMARC POLICY

Domain-Based Message Authentication Reporting & Conformance (DMARC) is basically an email authenticator, policy and reporting protocol that operates by Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) to determine the authenticity of the email messages. It plays a crucial role to protect organization from business email cyber-attack.

EMAIL AUTHENTICATION RECORDS



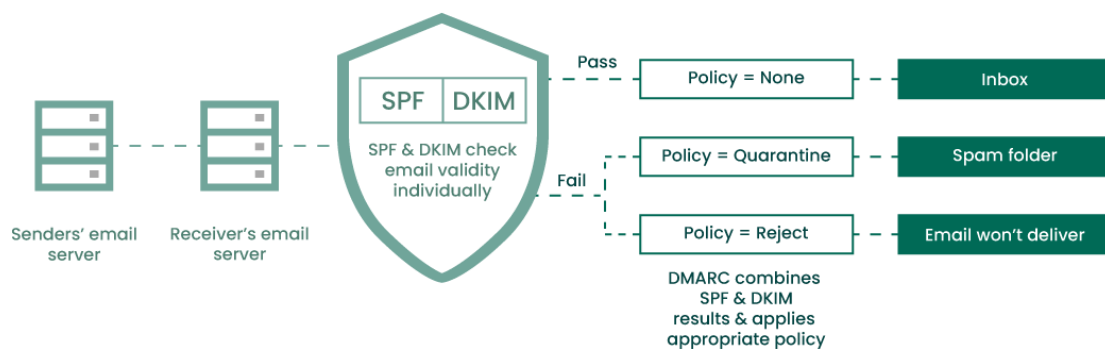
COMMON DMARC POLICY

1. **None:** This policy is also known as “Monitor” as it tells provider not to take any action against this email.
2. **Quarantine:** This policy tells provider to quarantine this email i.e., drop this unauthorized email into separate folder that can be spam box.
3. **Reject:** This policy tells provider to block this unauthorized email and do not allow to reach recipients mail box.

DMARC WORK

DMARC simply communicate with sender email server and check whether the authentication has been passed or not from SPF & DKIM? If the authentication passes, then the receiver receives the email in box. However, if the authentication has been failed then it removes the guesswork at receiver's end and put a limitation (quarantine) or eliminate those emails.

How DMARC Works



Let's assume I'm working in an organization, and our website don't have DMARC record which widely works on SPF & DKIM protocol, that means the domain is vulnerable to spoof an email. for example: we create an email mohan@example.com add phishing link then send it to my team member who is located at onshore for example: chris.mark@example.com and instruct to open the email and click on that link. Since the email looks genuine so Chris might think it's an official email from team and will try to access it, so once the link has been clicked then the attack will be success. Likewise, if the DMARC policy is enabled for the domain then it will simply follow the policy and take action according to the policy either it will quarantine or eliminate the email.

WHY COMPANIES SHOULD ADD DMARC POLICY TO THEIR DOMAIN


1. **Phishing Protection:** The DMARC policy prevents phishing attack by allowing domain owners to specify which servers are authorized to send email on behalf of their domain. This reduces the risk attackers to use company domain for fraudulent use.
2. **Brand Reputation:** The DMARC policy also helps to save the brand reputation by implementing this policy on their domain so that peoples can trust on incoming emails which is associated with the domain name but it's fake.
3. **Email Authentication:** It adds extra layer on the security of email communication with the help of SPF & DKIM Protocol.

DMARC addresses these issues, helping email senders and receivers work together to better secure emails, protecting users and brands from painfully costly abuse

HOW DO COMPANIES CAN IMPLEMENT A DMARC POLICY ON THEIR DOMAIN

You can use the DMARC Record Generator tool to create a customized DMARC record with a few simple steps:

1. Go to EasyDMARC free DMARC Record Generator tool.
2. Enter domain details.
3. Select the Policy type (choose from “none”, “quarantine”, and “reject”).
4. Enter details in report send to.
5. Select a Subdomain policy type (again, choose from “none”, “quarantine”, and “reject”).
6. Next, select SPF identifier alignment (can be chosen either “relaxed” or “strict”).
7. Choose DKIM identifier alignment (can be chosen either “relaxed” or “strict”).
8. Also, choose the Reporting interval (the requested interval in seconds between aggregate reports, the default is 86400)
9. Write down the Percentage applied for your DMARC policy (the percentage of messages from the domain owner mainstream to which the DMARC policy is applied, the default is 100).
10. Enter your Failure reporting address.
11. And lastly, pick out Failure reporting options (controls the type of reports that are sent out).
12. Once the tags are customized, click on the button that says “Generate DMARC Record” on the bottom.
13. Your DMARC record is created!



[Products](#) [Pricing](#) [Solutions](#) [Resources](#) [Company](#) [MSP Program](#)

DMARC Lookup

DMARC Generator

</> Get an embed

DMARC Record Generator

Create a valid DMARC record in a few clicks to use it in your DNS.

Domain

https://mohanreddy.com

Policy type

☒ None (monitoring) ☐ Quarantine ☐ Reject

Reports send to

mohan.reddy@reddy.com

Subdomain policy

none (monitoring) ▼

SPF identifier alignment

Relaxed ▼

DKIM identifier alignment

Strict ▼

Reporting interval

86400

Percentage applied to

100

Failure reporting send to

mohan.reddy@reddy.com

Failure reporting options

☒ 0 ☒ 1 ☒ d ☒ s

Generate

SCREENSHOT: DMARC RECORD GENERATOR

In order to access the DMARC Record Generator website you can enter the following link in the URL column of browser and hit enter.

<https://easydmarc.com/tools/dmarc-record-generator>

DMARC RECORD SYNTAX WORK

1. Mechanism (all | IPV4 | IPV6 | a | mx | ptr | exists | include).
2. Qualifiers (+ | - | ~ | ?).
3. Modifiers (redirect | exp).

- **all:** This mechanism always matches. It usually goes at the end of the SPF record.

"v=spf1 mx -all": Allow domain's MXes to send mail for the domain, prohibit all others.

- **ip4:<ip4-network>/<prefix-length>:**

"v=spf1 ip4:192.168.0.1/16 -all": Allow any IP address between 192.168.0.1 and 192.168.255.255.

- **ip6:<ip6-network>/<prefix-length>:**

"v=spf1 ip6:1080::8:800:200C:417A/96 -all": Allow any IPv6 address between 1080::8:800:0000:0000 and 1080::8:800:FFFF:FFFF.

- **a:**

"v=spf1 a -all"

- **mx:**

"v=spf1 mx mx:deferrals.domain.com -all"

- **ptr:<domain>:**

"v=spf1 ptr:otherdomain.com -all": Any server whose hostname ends in otherdomain.com is designated.

- **exists:<domain>:**

"v=spf1 exists:example.com -all": If example.com does not resolve, the result is fail. If it does resolve, this mechanism results in a match.

- **include:<domain>:**

"v=spf1 include:example.com -all"

- **redirect=<domain>:**

"v=spf1 redirect=example.com"

- **exp=<domain>:** If an SMTP receiver rejects a message, it can include an explanation

- '+': Pass.
- '-': Fail.
- '~': SoftFail.
- '?': Neutral.

HOW TO CHECK IF THE SPF RECORD FOR DOMAIN

Using web tool, user can check for the domain whether the SPF policy is existing or not for your domain. Enter *Kitterman>SPF Record>Testing Tool* on google and hit enter.

SPF Record Testing Tools

Home About Site

Overview

These tools are meant to help you deploy SPF records for your domain. They use an actual RFC 7208 compliant library (pyspf) for tests and will dynamically test for processing limit errors (no other testers I'm aware of do this). This site uses a caching DNS resolver, so for tests that use live DNS, results will be cached for the Time To Live of the DNS record. For most basic uses, these tests should be reasonably self explanatory. Advanced users may need, and probably want, some additional information on how these tools work. It can be found [here](#).

Does my domain already have an SPF record? What is it? Is it valid?

Retrieves SPF records for the specified domain name and determines if the record is valid.

Domain name

NOTE: The domain is everything to the right of the '@' in the e-mail address.

Is this SPF record valid - syntactically correct?

Tests the supplied SPF record to see if it is valid. This test does NOT look up the record for the supplied domain. It only tests the validity of the supplied record. This test is for checking the syntax of records before you publish them. The domain is used only for mechanisms such as a bare 'a' mechanism that have an implied domain. It will also be used for the '%d' macro if present.

Domain:

SPF Record:

Contact :
[E-mail](#)

Links :
[Sender Policy Framework](#)
[DNS provides the support TXT \(SPF\)](#)

Content Copyright 2005 - 2018 Kitterman Technical Services, Inc.
Design by Minimalistic Design

SCREENSHOT: KITTERMANTOOL

Enter the domain name in the highlighted area, for example: *byjus.com* and click on *Get SPF Record (If any)*. And you will see the results. Screenshot provided below.

```
SPF record lookup and validation for: byjus.com
SPF records are published in DNS as TXT records.

The TXT records found for your domain are:
workplace-domain-verification=WSRmc05KgxAyhvYI1NGSV4iWApO5
google-site-verification=2Tog4hINC3Q4Vgj5bVbwF5ytlQqkiaoFC3BIMB-A
ZOOM_verify_1LxSh88km0jrtbCqVvXQe8
google-site-verification=xumWA_2E5QYNGetcQWV1QDiA9U_hBbPHPCaVhe_WWY
MS=DCEA471DD7327F0778C5794D33BF6AED475FA693
google-site-verification=IN7i40BYU09dEvAPBSVGh1XoJhMRIFFPeEdnFMHIY
google-site-verification=GEVYC0H62bLjKItaYQjuwidMoAbhtotD7YSA0g-Uk8
v=spf1 include:_spf.google.com include:sendgrid.net include:1278314a1.spf2.netcorecloud.net -all
google-site-verification=PNRfKjMRHCvVwNZdVHyYD0pCHuqP2VX8sjTmrDyQ
google-site-verification=8d050zjwVipAPmNYKt7X84cJP04AT89fXC1BkFtO
google-site-verification=0v1WR38Wg8asZL_kNBKYSLZO_9oSqx6NO1tunQ1_YdU

Checking to see if there is a valid SPF record.

DNS: Truncated UDP Reply, SPF records should fit in a UDP packet, retrying TCP
Found v=spf1 record for byjus.com:
v=spf1 include:_spf.google.com include:sendgrid.net include:1278314a1.spf2.netcorecloud.net -all
evaluating...
SPF record passed validation test with pySPF (Python SPF library)!

Return to SPF checking tool (clears form)

Use the back button on your browser to return to the SPF checking tool without clearing the form.
```

WEBTOOLS THAT HELPS YOU TO TEST YOUR SECURITY LAYER ON EMAIL

*Whatever details we mention in our documents it is only for educational purpose.
Kindly take proper permissions before testing any website.*

 Select Language ▼



Free online fake mailer with attachments, encryption,
HTML editor and advanced settings...

From Name:

From E-mail:

To:

Subject:

Attachment: No file selected.
[Attach another file](#)

Content-Type: ☒ text/plain ☐ text/html ☐ Editor

Text:

Captcha: ☒ I am human  [Privacy - Terms](#)

SCREENSHOT: EMKEI'S WEB TOOL

REFERENCES

http://www.open-spf.org/SPF_Record_Syntax/

<https://www.geeksforgeeks.org/what-is-dmarc/>

<https://dmarc.org/>

www.google.com