Domain Alignment & Dmarc Monitoring

Stop Hackers & cybercriminals Sending Emails From Your Domain

We implement domain alignment using SPF, DKIM and monitoring with DMARC to prevent cybercriminals from sending fraudulent and spam emails from your domain.

- Prevent Data Leakage
- Protect Against Financial Loss
- Prevent Customer Loss
- Secure Your Email Accounts
- Protect against spoofing and spamming
- Protect your reputation
- Keep your domain off blacklists

What is DMARC in simple terms?

Domain-based Message Authentication, Reporting, and Conformance, or DMARC, is a technical standard that helps protect email senders and recipients from spam, spoofing, and phishing.

DMARC has three basic purposes:

- To verify that the sender's email message is protected by both DKIM and SPF protocols.
- To inform the receiving mail server what it should do if neither of those email security protocols passes, and
- To provide a way for the receiver server to report to the sender about the email message or messages that fail or pass the DMARC evaluation.

SPF, DKIM, DMARC explained

DID YOU KNOW?

468,000

Global emails were attacked in March 2020 alone

Cyberattacks using email as an entry point have become more creatively sophisticated and technical over the years. Even during this pandemic, cyber-criminals have taken advantage of the uncertainty.

Understanding SPF, DKIM, & DMARC

SPF, DKIM, and DMARC are the **three main email security protocols** that complement one another.

They are methods to authenticate a mail server and help prove to Internet Service Providers (ISPs), mail services, and other mail servers that senders are truly authorized to send an email.

What's the Importance of SPF, DKIM, DMARC?

- Enhances your email security posture.
- Combat phishing & spoofing as you're verifying the IP address of the sender.
- Keeps your domain off the global blacklists.
- Improves domain reputation.
- Improves the overall deliverability of your emails.

SPF: Sender Policy Framework

Sender Policy Framework (SPF) works by strictly determining the number of allowed IP addresses that can send emails from your domain.

The idea behind the use of SPF is that if the recipient knows who sent the email, they are more likely to open it.

SPF has three major elements

- The policy framework as the name implies
- The authentication method
- The specialized headers in the email itself that conveys the data

DKIM: DomainKeys Identified Mail

DomainKeys Identified Mail (DKIM) authentication ensures that the content of the email is trusted and has not been compromised or tampered with during the delivery.

If SPF is like the return address of a postcard or letter, DKIM is likened to sending that postcard or letter through special or recorded delivery that further builds trust between the receiver and the sender server.

DMARC: Domain-based Message Authentication, Reporting, & Conformance

Also referred to as "email signing." It ties the first two email security protocols (the SPF and DKIM) together with a more consistent set of policies.

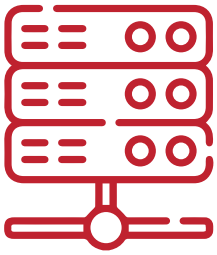
DMARC HAS THREE BASIC PURPOSES

To verify that the sender's email message is protected by both DKIM and SPF protocols.

To inform the receiving mail server what it should do if neither of those email security protocols passes.

To provide a way for the receiving server to report to the sender about the email message or messages that fail or pass the DMARC evaluation.

How do they work?



SPF - By adding an SPF record to your DNS records/ DNS txt record, it will list all of the approved servers that a mail is allowed to come from. here is an example

```
v=spfl a ip4:12.34.56.78/28 include:marketingemailserver.com
-all
```

In that example, such an SPF authentication record allows email sent from 12.34.56.78/28 and marketingemailserver.com.
If the email comes from other addresses, then it will be

DKIM - At the most basic level, DKIM works by adding a digital signature to the email message header. DKIM also uses an encryption algorithm that creates electronic keys - a private key and a public key.

DMARC - This policy relies on the established standards of SPF and DKIM for email authentication. Generally, DMARC validation works by deciding whether to reject, accept, or flag the email message. To deploy this authentication policy, you need to publish a DMARC record (text entry within the DNS record).

Key Takeaway

The SPF/DKIM/DMARC journey may not be an easy one. But working on these authentication mechanisms can work wonders in your email deliverability.
How about you? Have you already achieved the gold standard of email authentication by setting up the SPF, DKIM, and DMARC?

Apply
Highest Standards

Acquire industry standard email authentication and dramatically reduce the risk of fraudulent emails.

Alert
Your Employees

Get constant alerts and alert your employees about active phishing attacks while immediately finding the sources and catching the hackers.

Boost
Your Reputation

Show your customers, partners, and employees that you value their security and data privacy.

Protect
Your Data

Your business heavily relies on this data. Without proper protection, you will pay a lot of money to the hacker, who will constantly hold you at ransom.

Reach
The Inbox

Decrease the risk of being marked as spam, as strongly authenticated email is far more trustworthy to email providers (Gmail, Outlook, etc.).

Know
Your Senders

See who sends emails from your domain (customer support services, marketing campaigns, etc.).

Investigate Email Issues

Identify email problems and implement the necessary fixes for compliance.

What is Email Investigate and how can it help?

When adding a DMARC record into your DNS, it takes some time for the first report to arrive. Instead of waiting, you can get your first aggregate report instantly and check if your particular sending source is configured properly.

This helps to speed up your DMARC policy enforcement journey and check your email sending source's compliance. Email Investigate helps you detect and troubleshoot any potential issues with delivery. It also gives you a configuration overview with email authentication from any of your email sending services.

How Email Investigate works?

Email Investigate provides a unique inbox address to which you can send an email from each sending source. It analyzes the results and provides you with detailed information about SPF, DKIM, and DMARC records. It also reveals the DMARC policy that will be applied to your email and retrieves the configuration guide for source authentication setup.

DMARC Failure (Forensic) Reports

EasyDMARC renders DMARC Failure Reports' data into human-readable and easy-to-understand reports. Quickly discover the domain users when an authentication failure occurs. Gain full visibility into your outgoing email ecosystem and identify fraudulent emails sent from your domain.