DMARC REPORT

Email Authentication Essentials

A Practical Guide to SPF, DKIM, and DMARC Implementation

www.dmarcreport.com

Table of Content

Achieving (almost) Bulletproof Email Security & Deliverability....4

Lesson 1: Understanding Phishing & Other Email-Borne Cyber Threats 5

- Understanding Business Email Compromise (BEC) 5
- The Tactics Behind Email Spoofing 6
- Malware, Ransomware, and Trojans Explained 6
- What Happens in Email Bombing? 7
- Managing Email Threats with Authentication Protocols 7

Lesson 2: What is DMARC? 9

- DMARC: An Introduction 9
- How DMARC Works 9
- DMARC as an Email Security Tool 10
- Limitations of DMARC 11
- Creating a DMARC Record 11
- Adding DMARC to Your Domain 12

Lesson 3: What is SPF? 13

- Introduction to SPF 13
- SPF DNS Record Syntax Explained 13
- What are SPF Tags? 15
- Are There Any Downsides to Using SPF? 15
- Creating an SPF record 16
- Adding SPF Records for Your Domain 16

Lesson 4: What is DKIM? 17

Introduction to DKIM 17
What are DKIM Keys? 19
How Does DKIM Work? 19
What is a DKIM selector? 20
Adding DKIM to DNS Records 20
Are There Any Downsides to DKIM? 21
DKIM Key Size Limitations 22
DKIM Key Rotation- Importance and Best Practices 22
Recommended Smart Habits 23

Lesson 5: Defining a DMARC Policy 23

Understanding the Difference Between Aggregate and Forensic Reports 23
SPF & DKIM Alignment Defined 25
Reading a DMARC record 26
The 3 DMARC Policies 27

BIMI- the Newer Layer of Email Authentication 28

Final Checklist: Getting Started with Email Authentication 28

Conclusion 29

Achieving (Almost) Bulletproof Email Security & Deliverability

Emails are a primary mode of communication in all professional or academic settings. Therefore, protecting our email systems from unauthorized access is of utmost importance to ensure the well-being of our organizations, employees, associates, clients, and customers. Effective email protection strategies and technologies are the need of the hour, and three frameworks widely adopted in this process include SPF, DKIM, and DMARC.

This book discusses the fundamentals of Domain-based Message Authentication, Reporting, and Conformance (DMARC) and guides users through its functions, advantages, disadvantages, and implementation. Similarly, the chapters dedicated to SPF, DKIM, and DMARC policy look at the functioning and mechanisms of these email security solutions. The eBook doesn't merely inform why these technologies are recommended but also provides insights on whether these technologies would be suitable to meet the growing cybersecurity demands of your organization.

Since these email protections are often grouped under a single umbrella term, the book helps distinguish between DMARC, SPF, and DKIM by discussing their origins, specifications, and distinct features. *Understanding the advantages of one over the other, or both together, helps readers make informed decisions about their email security choices.* By the end of this eBook, readers will be in a better position to create DMARC, SPF, or DKIM records for their respective organizations.

As of February 2024, DMARC adoption reached 2.3 million organizations globally, reflecting a strong shift towards safer email ecosystems, with certain nations taking the lead.

Lesson 1: Understanding Phishing & Other Email-Borne Cyber Threats

Generative AI has transformed email-borne cyber threats by enabling attackers to craft highly convincing phishing emails that mimic official communication styles with flawless grammar and personalization. This technology allows cybercriminals to generate scam emails at scale, dramatically increasing their reach and success rates.

As a result, malicious emails have become harder to detect than ever before, posing a serious challenge for traditional email security systems.

Here are some of these threats, along with methods to mitigate them, ensuring an organization's data confidentiality, integrity, and availability.

Understanding Business Email Compromise (BEC)

Phishing is a cyber threat in which fake emails from malicious actors pretending to be genuine mislead you into divulging confidential and crucial information. It has many advanced forms. Business Email Compromise (BEC) is an advanced phishing method in which the malicious actor impersonates or compromises a business executive's email account to manipulate their subordinate into initiating a financial transaction or revealing sensitive information.

The Tactics Behind Email Spoofing

Spoofing is a tactic where a malicious actor uses an email address or other credentials resembling a genuine entity to deceive the recipient into believing it is from a trusted source. They use spoofing to extract money or induce targets to download malware or share sensitive information. Unlike BEC, the threat actor does not particularly compromise the email account of the organization's business executive to send malicious messages. Instead, it could be anyone that the target trusts as genuine.

New Gmail Spoofing Scam Impersonates Law Enforcement

Cybersecurity expert Nick Johnson (Ethereum Name Service) recently uncovered a highly sophisticated phishing campaign that spoofs Gmail's own domain to mimic official law enforcement subpoenas. Attackers fabricated emails appearing to come from "no-reply@google.com," embedded within genuine Gmail security threads, directing recipients to a hosted Google Sites page that harvested user credentials. The scam was so credible that even tech-savvy users were being targeted.

Malware, Ransomware, and Trojans Explained

Malware, ransomware, and trojans are a few common forms of threats that may reach you through phishing emails. Here is a brief idea of such threats.

- Malware is software designed to damage, disrupt, and gain unauthorized access to an organization's network system. Malicious actors often send executable or downloadable files containing malware through email. The threat actor can control the network remotely by gaining access to it.

- Ransomware is different from malware; it restricts the target from accessing data in their information systems by encrypting it. It places a ransom demand for the target, satisfying which will provide access to the restricted data by decrypting it. The ransom is usually required to be paid in cryptocurrency.
- Trojans are malware that disguise themselves as a legitimate program and take control of your information network system. These viruses pretend to be operational programs and perform destructive actions before you realize their presence.

What Happens in Email Bombing?

Email bombing is a kind of DDoS attack where the victim receives an uncontrollable deluge of email messages that quickly fills the inbox, overloads the email server, and renders it useless. At times, the victim may overlook actual business email communications by getting lost in the flood of fraudulent email messages.

Managing Email Threats with Authentication Protocols

Emails are a weak link in an organization, opening a path for malicious actors to unleash their cyberattacks. Here are the measures one can take to handle email threats.

- End-to-end encryption is one way to ensure that no third-party entity accesses your email contents.
- Educating employees to identify suspicious email communications, such as BEC scams, can help businesses protect themselves from cyberattacks.
- Installing anti-malware solutions and regularly updating them can prevent malware from infiltrating the network systems.

- Restricting administrator privileges can help reduce privilege escalation attacks and discourage third-party interference.
- Robust password maintenance is another deterrent to email threats.
- Using high-level email authentication standards can secure emails from the source and prevent phishing or spoofing attacks. The email authentication protocols include the following (More details are covered in the upcoming chapters).
- SPF (Sender Policy Framework): SPF specifies servers and domains authorized to send emails on your domain's behalf.
- DKIM (DomainKeys Identified Mail): DKIM adds a digital signature to each of your outgoing messages to help the recipient verify that the message originated from the right source.
- DMARC (Domain-based Message Authentication, Reporting, and Conformance): DMARC is a free and open technical specification that authenticates emails by aligning SPF and DKIM mechanisms. It instructs receiving servers on how to handle messages that do not pass SPF or DKIM verification.

With more people using emails for correspondence, malicious actors have greater scope to launch cyber-attacks through email. Hence, organizations need to be aware of the latest mitigation tools like email authentication protocols. Investing in such solutions and regularly updating them can deter most email threats an organization may otherwise face.

Lesson 2: What is DMARC?

DMARC is an email authentication policy and reporting protocol. It helps organizations protect their email domains from being spoofed.

Through this chapter, you will learn how DMARC works and why it is essential for email security.

DMARC: An Introduction

DMARC (Domain-based Message Authentication, Reporting, and Conformance) is a technical specification for email authentication, developed in 2012 by a group of email administrators, security professionals, and industry leaders.

It is a security protocol used to identify and authenticate email senders. DMARC enables email senders to establish a policy that dictates how receiving email servers should handle emails sent by them. It helps the recipients know that your emails are genuine.

How DMARC Works?

DMARC allows organizations to specify the action they want taken if a fraudulent email is detected in their name, such as rejecting the email or quarantining it. DMARC also enables organizations to collect data on all emails sent to their domain, helping them identify any potentially fraudulent emails.

DMARC is another authentication protocol, similar to Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM), employed by businesses for email security. DMARC enables organizations to set up rules concerning recipients' actions on sent emails. The most basic rule is called the SPF Box Rule.

This rule, when enabled, will identify senders of emails that are not associated with the domain name. You can set up additional controls to help classify the type of email being sent, allowing people to avoid accidentally sending emails to the wrong address or filtering spam.

DMARC as an Email Security Tool

> *Gmail & Yahoo announced on October 3, 2023 that any domain sending 5,000+ messages/day must enforce a DMARC policy starting from February 1, 2024.*
>
> *Microsoft followed suit in early 2025, and as of May 5, 2025, Outlook.com, Hotmail.com, and Live.com now reject emails from non-compliant bulk senders*

Malicious actors and adversaries continue to find new ways to send fraudulent emails from trusted domains, thereby damaging the brand reputation. In this situation, email authentication techniques such as SPF, DKIM, and DMARC can help protect your domain from being used by spammers to send fraudulent emails.

Apart from protecting your domain from being misused by spammers, email authentication methods like DMARC also help prevent C-level fraud, such as Business Email Compromise (BEC) and whaling attacks.

One helpful functionality that DMARC provides, apart from spam email protection, is the addition of a reporting feature. With reporting, businesses can get detailed insights into who uses their domain to send emails.

Limitations of DMARC

DMARC is a valuable tool that can help protect your email from being spoofed; however, it has some limitations. One such factor is that DMARC only applies to email messages sent from your domain. If someone else sends an email message on your behalf, DMARC will not protect it. Besides, DMARC does not work with email messages sent through third-party services, such as Gmail or Yahoo! Mail.

Creating a DMARC Record

A DMARC record is a TXT record added to your domain name that instructs the receiving email server on what to do if email authentication fails. It urges the recipient email server to reject/quarantine or allow the email and send a report back to the email address provided in the DMARC record.

A sample DMARC record looks like this:

v=DMARC1; p=none; rua=dmarc@domainname.com

The DMARC record is made of 3 tags, namely v, p, and rua, where,

v – version of DMARC

p – action to be taken (1: None, 2: Quarantine, 3: Reject)

rua – return email address

According to the DMARC guidelines, 11 tags can be added; however, these three tags are considered essential. The other tags include pct, ruf, fo, aspf, adkim, rf, ri, and sp.

Several online tools are available to help you create and validate DMARC records for your domain.

Adding DMARC to Your Domain

To add DMARC records for your domain, follow the steps below:

- Visit the control panel of your DNS hosting provider.
- Choose the 'Add New DNS Record' option.
- Add "_dmarc" to the Name section.
- You can set TTL to "Auto".
- In the Content section, add the DMARC record that you created earlier.
- Click 'Save'.
- Validate the record.

Thus, your DMARC record is created.

Authentication protocols like SPF, DKIM, and DMARC will undoubtedly add an extra layer of authentication and protection for your emails. Though none of the existing authentication protocols provides businesses with a 100% guarantee to ensure that the emails reach their customer's inboxes, email authentication helps organizations maintain their trust and reliability to a significant extent.

Hence, anyone serious about email security must have DMARC set up for email authentication, as it can help protect your domain from being spoofed.

Lesson 3: What is SPF?

Hence, anyone serious about email security must have DMARC set up for email authentication, as it can help protect your domain from being spoofed.

In most cases, it is used to prevent spammers from sending emails with forged sender addresses from a domain by publishing an SPF record in the domain's DNS zone.

Introduction to SPF

The Sender Policy Framework (SPF) is another widely used method of email authentication that prevents spammers from using a domain for spam emailing.

The framework publishes an SPF record to the DNS, i.e., a list of the IP addresses authorized to use your domain name for email. It also points out the unauthorized senders who cannot use your domain name.

SPF DNS Record Syntax Explained

A typical SPF record in the DNS looks like the following:

v=spf1 ip4:192.0.2.0 ip4:192.0.2.1 include:example.com -all

The SPF DNS method employs a list of 8 mechanisms that differentiate authorized email senders from unauthorized ones.

- all: This mechanism is at the end of the SPF record and matches all the senders.
- ip4: This mechanism allows IP addresses of the IPv4 network range of a pre-specified list to send emails using a given domain name.

- ip6: This mechanism is similar to ip4 but works on the IPv6 network range.
- a: When this mechanism is used, the IP address should strictly match the SPF DNS record unless a prefix length is provided. When the **prefix length** is provided, the system searches for all IP addresses that match that prefix length.
- mx: In the case of this mechanism, the entire list of records is tested in the order of specified priority.
- ptr: The hostnames are validated using PTR queries. The invalid hostnames are rejected, while the valid ones are matched.
- exists: This mechanism utilizes an A query based on which the existing IP addresses are validated and approved.
- include: This mechanism searches the domain for a match. If a match is not found, it forwards the list for further processing.

Each of the mechanisms can use any one of the four qualifiers:

- + (Pass)

The Pass qualifiers list the domain-authorized email sender.

- – (Fail)

The Fail qualifier lists the unauthorized senders.

- ~ (SoftFail)

The SoftFail qualifier provides a list of in-transition, unauthorized senders.

- ? (Neutral)

The Neutral qualifier is used to mark the questionable senders.

While the DNS processing is ongoing, a temporary error may be represented by the qualifier' TempError.' In contrast, a syntax or evaluation error is notified by 'PermError.' In the cases where the domain has not created the record yet, the qualifier 'None' is observed.

What are SPF Tags?

The eight SPF mechanisms, which perform different types of functions according to the SPF DNS record, are also known as SPF Tags. Apart from these eight, the tag "v" is utilized to represent the protocol version.

Are There Any Downsides to Using SPF?

Using SPF can sometimes be disadvantageous as well. Below are a few drawbacks of using SPF.

- **Email Forwarding**: When an email sent from an authorized IP address is forwarded, the IP address of the person forwarding the email won't be recorded.
- **End-User Discretion**: Attackers might build a domain similar to yours. Since end-users do not verify the Return-Path/mailfrom domain, they may fall victim to phishing attacks from such fake domains.
- **Third-Party Vendors**: Domain owners depend on third parties that use their domain names. Therefore, there is a constant need to continuously update the SPF record list, which can be a significant inconvenience.
- **Limited DNS Lookup**: A single SPF record allows checking only a maximum of 10 DNS lookups.

Creating an SPF record

> *Did you know?*
> *Around 70% of domains globally have misconfigured SPF records, leading to deliverability issues or security gaps. Even worse, over 15% of domains publish invalid SPF records altogether, making their anti-spoofing efforts useless.*

Make sure to follow the instructions below while creating an SPF record.

- Keep a record of the authorized IP addresses.
- Create SPF records for all your domains, including those that do not send emails. The practice helps you avoid instances of spoofing in case an attacker tries to use domains that are not typically used for sending emails.
- Create your SPF record with the help of the 8 SPF mechanisms.
- Publish the SPF record with the help of your DNS server admin.
- Perform a test run to verify that the SPF mechanisms are functioning correctly.

Adding SPF Records for Your Domain

If you are new to SPF, you can utilize the pre-configured SPF record to use the framework. If you want to add your list of SPF records, you can do so by following the steps given below:

- Log in to your Account Control Center.
- Go to 'Domains' and then 'Manage Your Domain Names.'
- Go to the Domain Name to which you want to add your SPF record.

- *Go to 'Manage Custom DNS Records.'*
- Next, you will see the option 'Add DNS Records.' Click on it.
- It will take you to the section that will allow you to choose the 'Type of Record' you want to add. Click on the 'TXT' option and then 'Proceed.'
- You will then reach a page with two text boxes, one for Hostname and another for Text Record.
- In the Hostname section, you can write the name of the subdomain for which you are creating the record, or leave the box empty if you want the record to be made for the entire domain. Write your SPF record in the 'Text Record' text box, and click on the 'Create Record' option.

  ***Note that the process may vary slightly for different hosting providers.*

Since the SPF record is a simple TXT record, it is easy to create. However, you have to be thorough about the syntax and the correct use and implications of its mechanisms, qualifiers, etc., to avoid errors and make the record work for you in the best possible way.

Lesson 4: What is DKIM?

DomainKeys Identified Mail (DKIM) is a way of communicating with other email servers that your messages are legitimate and haven't been tampered with during transit. It works by adding a cryptographic signature to your messages, demonstrating to the other party that the messages haven't been altered and that the sender is who they claim to be.

Introduction to DKIM

DKIM stands for DomainKeys Identified Mail and is a protocol for email authentication that enables recipients to verify whether an email was sent and authorized by the domain owner.

In other words, DKIM will enable organizations to take ownership of emails sent through their domains by providing a digital signature that mailbox providers can easily verify. DKIM is used to distinguish between phishing emails and genuine ones, using the DKIM signature as the primary means of verification. The **DKIM signature** is typically added as a message header and secured with cryptographic encryption.

The DKIM signature is typically invisible to end-users or email recipients and primarily functions at the server level. The receiving server identifies whether an email is signed with the DKIM signature of the organization whose domain name is used. Once verification is complete, the email, including all its constituent messages and attachments, is forwarded to the end user's mailbox.

> As of 2024, only about 32% of global domains have properly configured DKIM records – despite DKIM being critical for ensuring email integrity and preventing tampering in transit.

DomainKeys Identified Mail (DKIM) began in 2004 as a merger of two existing technologies – Enhanced DomainKeys from Yahoo and Identified Internet Mail from Cisco. This new technology eventually became a widely adopted email authentication technique. *DKIM is a testament to the integrity of a message's content and verifies that its contents have not been changed in transmission*. Additionally, it reduces the likelihood of emails not being delivered – a problem that has cost companies many loyal customers.

What are DKIM Keys?

DKIM operates by using the public-key cryptography approach to detect forgery in emails and verify whether an email message was sent from a legitimate mail server. The DKIM keys help spot spam and malware-embedded emails.

DKIM involves generating a pair of **private and public encryption** keys for each server. While the private key is allotted to the sender's server, the public key is placed on the domain owner's DNS zone file to form a special TXT record.

The private key helps the sender's server generate the required DKIM headers for outgoing client emails. The public key, on the other hand, verifies the authenticity of the sender.

How Does DKIM Work?

DKIM adds digital signatures to the headers of email messages, which are then validated against public cryptographic keys in the organizational Domain Name System (DNS) records.

The following steps are involved in the process:

- Any outbound mail server sending an email generates a unique DKIM signature, which is attached as a message header.
- Inbound mail servers receiving these incoming emails scan the sender's public DKIM keys in the DNS.
- The inbound server decrypts the signature and compares it with a newly generated one using this public key.
- If both values match, the message is considered authentic and unaltered in transmission.

What is a DKIM selector?

A DKIM selector is a small piece of text that helps email providers find the right DKIM public key in your DNS records. It's added to your email's header and works like a label that points to the correct key. This is useful when you have multiple DKIM keys—for example, if different tools or services send emails on your behalf. The selector makes sure the receiving server knows exactly which key to check for verifying the email's authenticity.

Adding DKIM to DNS Records

Having understood the role of DKIM in ensuring email delivery and authenticity, let us now look at the process of adding DKIM to your DNS records.

- The first step is to create a list of all domains that have your authorization to represent you and send emails to end-users on your behalf. This list could include sending services and domains, such as invoice generators and marketing campaign platforms.
- *These domains should then be contacted to procure the DKIM configuration and a copy of the public key.*
- The next step is to generate key pairs either internally (if your organization uses its server) or using third-party tools that facilitate DKIM record creation. However, third-party tools should be used only after checking your organization's security policy.

- After generating your DKIM record, you must publish your public key to your DNS record. **DNS providers** often support text (TXT) records of up to 255 characters; however, you will need to contact your provider if you wish to increase the record size.
- The final step is to save the private key to your mail transfer agent or **SMTP server**.

Are There Any Downsides to DKIM?

While DKIM has its advantages and enhances the efficiency of email communication, it has its downsides. Some of these are:

- **Replay Attack:** A replay attack enables adversaries to insert extra fields into a DKIM-signed message, thereby bypassing authentication, as the signature would still match. DKIM was primarily created to verify the reputation of sender domains, and in that sense, it remains useful. But what happens if DKIM authenticates an email from a reputed domain that perhaps was altered during transmission by adversaries to include additional header fields? Replay attacks are a common problem with DKIM because it doesn't sign all parts of an email message and only authorizes selected parts. All the adversaries need to do is add a few more header fields, and the DKIM signature will still match. This makes end-users of such forwarded messages vulnerable.

In April 2025, attackers used a DKIM replay attack to target Gmail users. They exploited Google's own no-reply@accounts.google.com address by replaying a legitimate DKIM-signed email to bypass security checks. The email contained links to a phishing page on sites.google.com, stealing user credentials. Since the DKIM signature was valid, it easily landed in inboxes. This attack showed how even DKIM-signed emails can be misused for sophisticated phishing.

- **Allowlisting:** Yet another limitation of DKIM is the risk associated with allowlisting. For efficiency purposes, companies often allowlist trusted domains based on their DKIM signature. Allowlisting a domain is the opposite of blocklisting it, implying that emails from that domain are authenticated without any scrutiny or analysis. However, such practices often make organizations vulnerable to phishing attacks.

DKIM Key Size Limitations

DKIM keys help prove your emails are coming from you and haven't been tampered with. For better security, 2048-bit keys are the recommended standard. But since DNS records have size limits, the key needs to be properly split into smaller chunks when publishing it. If not done right, email authentication can fail.

To avoid that, use a DNS provider that supports long TXT records and always test the setup after adding the key. It's also best to avoid 1024-bit keys—they're outdated and often rejected by major email providers

DKIM Key Rotation- Importance and Best Practices

DKIM key rotation simply refers to replacing your old keys with new ones from time to time. If a key is used for too long, the chances of it getting stolen and abused increases, especially if you use third-party tools to send emails. This practice keeps your email setup safer and trustworthy in the eyes of mailbox providers.

Recommended Smart Habits

- Use 2048-bit keys for better security
- Rotate your DKIM keys once every 3-4 months
- Remove old keys from the DNS once you have updated the new ones
- Test your emails after rotation to make sure signing and verification are working correctly.
- Keep a record of all the selectors and keys in use, especially if multiple services send emails for your domain

Lesson 5: Defining a DMARC Policy

This chapter focuses on defining an effective DMARC policy by explaining the difference between aggregate and forensic DMARC reports and SPF/DKIM alignment. It also sheds light on reading a DMARC record and the three DMARC policies.

Understanding the Difference Between Aggregate and Forensic Reports

DMARC Aggregate Reports: DMARC aggregate reports are obtained with details on the source and authenticity of emails issued on behalf of a domain that reveal information on the following points:

- If the emails authenticate against DKIM (DomainKeys Identified Mail) and SPF (Sender Policy Framework).
- The transmitting domain for DKIM/SPF.
- The originator of a message.
- Messages that were sent on a given day.
- The DMARC result.

> Most people don't realize that DMARC aggregate reports are XML files—making them super hard to read manually. That's why DMARC monitoring tools exist: they translate those complex XML records into human-readable dashboards, showing which IPs are sending emails on your behalf, where authentication fails, and who might be spoofing your domain.

DMARC Aggregate reports are sent in XML file format and do not include details about the emails themselves. You may analyze the content from aggregate reports to recognize all valid email sources, as well as the sender's capabilities for sending out emails and authorizing them appropriately.

DMARC Forensic Reports: Forensic reports are received every time an email from your domain fails both SPF & DKIM authentications. A forensic report is used to conduct a thorough investigation of email spoofing your domain since it contains message-level data, including:

- Email addresses of the sender and recipient
- Subject lines for emails
- The message ID and message time
- Information about IP (Internet Protocol), ISP (Internet Service Provider), and domain
- Results from SPF, DKIM, and DMARC

Data collected in forensic reports reveals trouble associated with a particular source, mail stream, or transmitting IP address.

But there's a size limit—if a DMARC report is over 32KB, it might get broken into parts or not sent at all. This usually happens if your domain sends a lot of emails or if many different sources are using it.

To stay within the limit:

- Use a subdomain dedicated just for DMARC reports.
- Monitor and reduce the number of unauthorized or unknown sources using your domain.
- Use a DMARC reporting tool or service that can collect, store, and organize these reports, even if they arrive in pieces.

In summary, aggregate reports help identify and authenticate genuine emails, while forensic reports facilitate the analysis of falsified emails and the detection of malicious attack traits.

SPF & DKIM Alignment Defined

SPF and DKIM alignment mean the matching of domains. A DMARC requires validating the authenticity of the sender's address as the message's legitimate sender, which is accomplished by authenticating the sender's DKIM and SPF.

- **DKIM Alignment**: The DomainKeys Identified Mail alignment checks if the root domain of the email used to construct the signature (specified in "d =" argument) is aligned with, i.e., matches the domain in the "From" header.
- **SPF Alignment**: The Sender Policy Framework Alignment checks the alignment, i.e., the matching of the domains specified in the two headers of the email, namely the "From" and "MailFrom / Return Path."

You can use the "aspf" and "adkim" parameters for SPF and DKIM alignment, respectively, in a DMARC record to stress the severity of the alignment, i.e., relaxed or strict alignment for flexible or absolute matching of the domains. By default, the option is set to "relaxed."

Configuring SPF and DKIM alignments for authentication adds an extra degree of security to your outbound emails, and pairing SPF and DKIM for authentication is a powerful strategy for preventing malicious emails from reaching the inbox.

Reading a DMARC record

A DMARC record notifies email recipients if a domain has been configured for DMARC and includes the domain owner's policy. A DMARC record is enclosed in the tag and encloses subtags that provide information, such as:

- The tag encloses the name of your domain.
- The tag contains information about relaxed (r) or strict (s) DKIM alignment.
- The tag contains information about relaxed (r) or strict (s) SPF alignment.
- The tag indicates the requested policy (none, quarantine, or reject) when an email fails DMARC authentication.
- The tag is for subdomain policy used to indicate a separate DMARC record for the subdomain.
- The tag is used to specify the percentage of emails to be checked for authentication in an email stream, but it is optional.

The 3 DMARC Policies

There are 3 DMARC policies for handling emails that fail authentication, which are:

- **Monitor:** Monitor, also known as none policy, is the most basic DMARC policy, specified by "p=none." The monitor enables monitoring and sends all emails (including failed authentication) to maintain regular traffic flow. The monitor generates data on your domain usage and helps you understand how DMARC functions by revealing the emails handled by a specific email provider and the ones that failed verification.

- **Quarantine:** The quarantine policy is specified by "p=quarantine," which sends unqualified emails (those that fail authentication) to the recipient's trash or spam folder. The quarantine policy is advised as a second level in **DMARC implementation**. The quarantine policy prevents your domain from being used for malicious purposes and helps you control misclassification. As a result, genuine emails and data can be analyzed that were banned and spammed due to configuration errors.

- **Reject**: The Reject policy prevents unqualified emails (those with failed authentication) from reaching their intended recipient. The reject policy, specified by "p=reject," is the most effective DMARC policy against cybercrime. Still, it requires a more sophisticated stage to ensure that authentic emails are not rejected. The reject policy requires proper allow listing permissions for third-party senders such as CRM systems or Email Service Providers.

BIMI-the Newer Layer of Email Authentication

BIMI stands for Brand Indicators for Message Identification. It's a newer standard that builds on existing email authentication protocols— SPF, DKIM, and DMARC. Once these are properly set, BIMI allows you to display your brand's logo next to your emails in recipients' inboxes.

While BIMI doesn't directly prevent phishing, it adds visual trust, helping your emails stand out in cluttered inboxes and look more legitimate. It also shows that your domain follows strong email security practices.

Final Checklist: Getting Started with Email Authentication

- Understand the threats: Learn how phishing, spoofing, and BEC attacks work
- Set up SPF: Create and publish an SPF record listing authorized IPs
- Implement DKIM: Generate DKIM keys and add them to your DNS
- Choose a DKIM selector: Label your keys for better tracking
- Rotate DKIM keys regularly: Update them every 3–4 months for security
- Use 2048-bit DKIM keys: Avoid 1024 or shorter bit keys as they are easier to break
- Set up a DMARC policy: Start with p=none, then move to 'quarantine' or 'reject'
- Ensure SPF and DKIM alignment: Use relaxed or strict settings as needed
- Monitor aggregate reports: Analyze email activity using 'rua' reports
- Handle 32KB report size limit: Use subdomains and reporting tools
- Review forensic reports: Investigate failed authentications and spoof attempts
- Add BIMI (optional but recommended): Display your brand logo next to your emails

Conclusion

The growing risk of cyberattacks necessitates increased awareness and comprehensive employee training programs. The book DMARC Fundamentals can become a valuable resource to meet the needs that organizations worldwide face today. About two-thirds of the Fortune 500 companies are estimated not to have a DMARC record on their corporate domain.

DMARC is regarded as the standard for email authentication. Not incorporating it increases the risks of unauthorized third parties using your organization's name and goodwill to infect end-user devices and steal their details.

This book aims to raise awareness and urges CISOs, CIOs, and other company leaders to encourage the adoption of effective DMARC policies to ensure email authentication by preventing adversaries from intercepting emails during transmission. DMARC, SPF, and DKIM are certainly not 100% effective in evading phishing and other email fraud on their own, but these technologies serve as an initial authentication measure. Without the initial authentication and verification of domains, preventing email scams is far more complicated.

The book DMARC Fundamentals works in the direction of igniting minds on the significance of creating DMARC records for their organizations to ensure that only verified senders can use their domain name to reach customers and end-users.

Free Tools

- DMARC Lookup Tool
- SPF Lookup Tool
- MTA-STS Lookup Tool
- BIMI Lookup Tool
- TLS-RPT Lookup Tool

DMARC REPORT

Contact Us


www.dmarcreport.com


support@dmarcreport.com


(+1) 855-700-1386

Reach Us on Social Media