What is DMARC:
Email Security with DMARC, SPF, and DKIM

Nowadays, it is normal for us to walk in the store and see security cameras. We know that shops have alarms and anti-shoplifting systems. But how come so many of us still do not realize the importance of the same kind of security measures when it comes to our cyber safety? Every email marketing campaign aims to engage customers with the brand. Today to become a brand that people trust, one must create a safe environment for both the company and the audience. That is why, today, it is necessary to talk about the most effective protection protocol – DMARC.

What is DMARC?

DMARC stands for Domain-based Message Authentication, Reporting & Conformance. It is an email authentication, policy, and reporting protocol. In simpler terms, DMARC prevents unauthorized use of the email domain, protects email recipients from phishing, spoofing, and other email scams that may use one's brand to get read. It is like a door frame detector for the email: monitors what is coming in and out.

DMARC is built on two email authentication standards adopted earlier: SPF and DKIM. While being efficient, these standards have significant flaws that scammers and phishers can take advantage of: they do not look at the email address used in the "From" field of an email message.

SPF only validates the domain used in the "Return-Path" field. Scammers can use an email address on an SPF-validated domain in "Return-Path" while putting an impersonated email in the "From" field. If a recipient ignores it, they will not know the email came from a scammer or phisher.

DKIM validates only the domain used in the DKIM signature. Malicious senders can sign the messages with DKIM on behalf of the domain that does not correlate with the email address in the "From" field of the message.

DMARC closes these gaps and ensures that a legitimate email is properly authenticated against established DKIM and SPF standards.

What is DMARC Used for?

Three key values of DMARC are domain alignment, policy, and reporting. Together they create a strong authentication for securing both the brand and the recipients.

DMARC's alignment prevents spoofing of the "Header From" address by:

- Matching the "Header From" domain name with the "Return-Path" domain name during an SPF check;

- Matching the "Header From" domain name with the "d=" tag's domain name in the DKIM signature.

DMARC's policy provides three action options email receivers can take for an incoming email if it fails the DMARC check: none, quarantine, or reject.

The meaning of DMARC policies:

none: do nothing with the email. It is a monitoring mode that senders can use to collect data about the authentication of all the emails coming from the domain.

quarantine: accept the email but treat it very carefully. A quarantined email will be considered suspicious and sent to the Junk or Spam folder.

reject: the email is rejected and is never delivered to the recipient.

It is important to note that a DMARC policy is a request, not an obligation. Although the DMARC policy instructs email receivers to handle the emails according to its requirements, email receivers are not obligated to take the DMARC policy into account. They sometimes

apply their local policies. When an email receiver reasonably finds an email to be legitimate, for example, when the email is forwarded, they will apply their local policy or downgrade the “Reject” policy to “Quarantine”. It means that an email failing the DMARC checks can still reach the recipient, even though the “Reject” DMARC policy is enforced.

DMARC provides an option of setting different DMARC policies for the primary domain and subdomains using the corresponding tags in the DMARC record: p= and sp=. The p= tag contains the policy for the primary domain, and the sp= tag contains the policy for the sub-domains. If the sp= tag is not included, the policy used in the p= tag is applied to the messages sent from the sub-domains.

DMARC’s reporting gives visibility into what messages are authenticated, what messages are not, and why. There are two available types of DMARC reports: the Aggregate Reports (RUA) and Forensic reports (RUF).

Aggregate DMARC reports (RUA):

- sent daily;
- contain the information about all emails sent from the domain, regardless of whether the message passed the DMARC check or not;
- provide information on how each message is authenticated;
- show all IP addresses that have attempted to send an email using the owner's domain name.

Forensic DMARC reports (RUF):

- sent in real-time;
- only sent for the messages that failed the DMARC check;
- include original message headers;
- may include the original message;
- include information about SPF and DKIM authentication problems.

How Does DMARC Work?

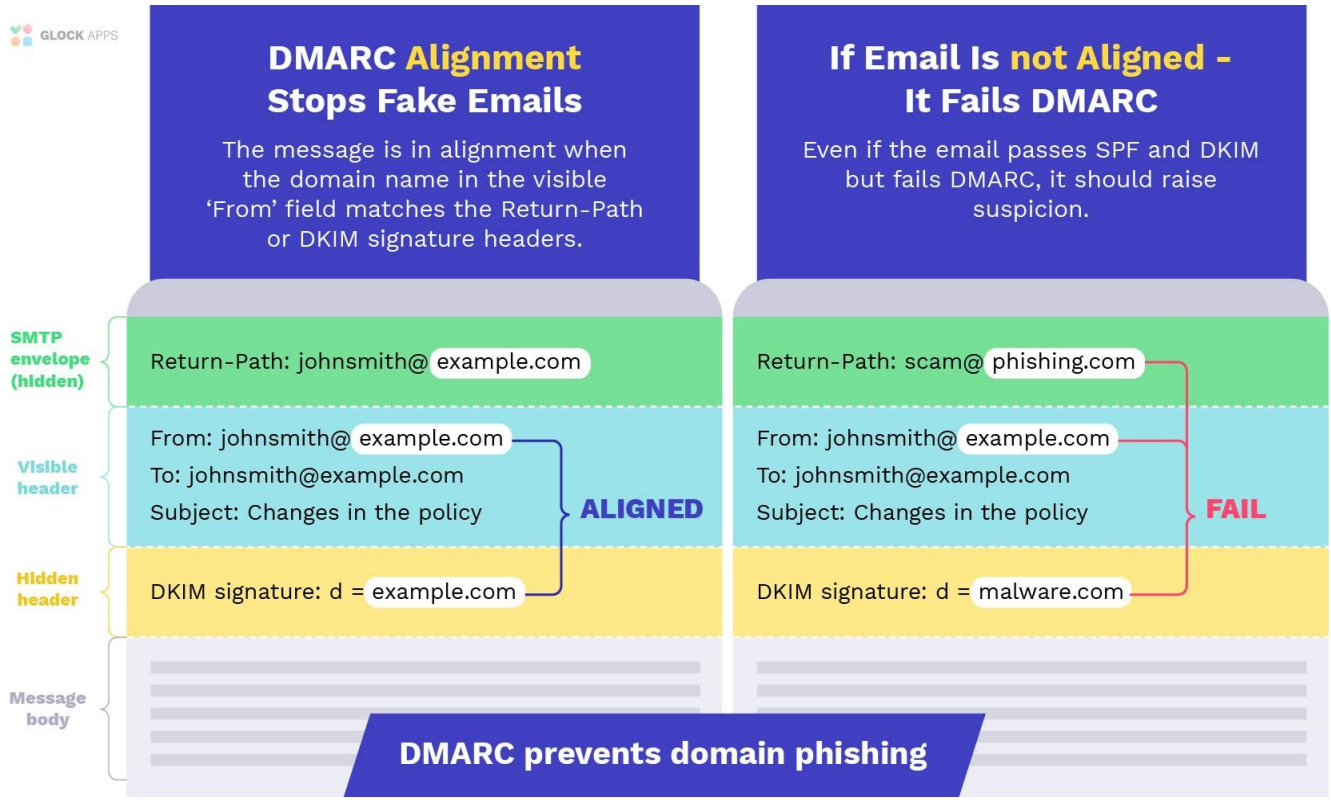
These are the steps an email undergoes when DMARC is installed:

1. The mail server completes the SPF and DKIM alignment.

   To pass DMARC, a message must pass SPF authentication and SPF alignment and/or DKIM authentication and DKIM alignment. A message will fail DMARC if it fails both (1) SPF or SPF alignment and (2) DKIM or DKIM alignment.

2. The server applies the DMARC policy that defines what to do with the email.

3. The email receiver sends a report back to the email sender.



What is a DMARC Record?

A DMARC record is the implementation of DMARC in the form of a TXT record. It contains the domain owner's DMARC policy settings and the email addresses to send the aggregate and forensic reports to. Including the email addresses is not an obligation, but a recommendation - it allows the domain owner to control email traffic coming from the domain and know whether or not their messages are authenticated.

How to Create a DMARC Record?

The beauty of DMARC is in the simplicity of deployment. All one needs to do is create a TXT record and add it to the domain's DNS.

DMARC record is published under _dmarc.yourdomain.com, where "yourdomain.com" is replaced with the actual domain (or subdomain) of its owner.

There are many tags that can be included in the DMARC record. Some of them are required, and some are optional.

Required tags:

v: This is the version tag that identifies the record retrieved as a DMARC record. Its value must be DMARC1 and must be listed the first in the DMARC record.

p: This is the tag that indicates the requested policy email receivers should apply when an email fails DMARC authentication and alignment checks. The policy is applied to the primary domain and all of its sub-domains unless the sp= tag is used with a different policy value.

Optional tags:

rua=: This is a tag that lets mailbox providers know where aggregate reports should be sent.

fo: This is a tag that lets mailbox providers know that the owner wants samples of emails that failed either SPF and/or DKIM. There are four options available:

0: Generate a DMARC failure report if all underlying authentication mechanisms (SPF and DKIM) fail to produce an aligned “pass” result. (default).

1: Generate a DMARC failure report if any underlying authentication mechanism (SPF or DKIM) produced something other than an aligned “pass” result. (recommended)

d: Generate a DKIM failure report if the message had a signature that failed evaluation, regardless of its alignment.

s: Generate an SPF failure report if the message failed SPF evaluation, regardless of its alignment.

sp: This tag is used to indicate a requested policy for all subdomains where an email is failing the DMARC authentication and alignment checks. The policy options are the same as the "p" tag listed above.

adkim: Indicates strict or relaxed DKIM identifier alignment. The default is relaxed.

aspf: Indicates strict or relaxed SPF identifier alignment. The default is relaxed.

pct: The percentage of messages to which the DMARC policy is to be applied. This tag provides a way to gradually implement and test the impact of the policy.

Values are integers ranging from 1 - 100. The default value is 100.

ruf=mailto:address@company.com: This tag lets mailbox providers know where the owner wants the forensic (message-level) reports to be sent. However, due to potential privacy and performance concerns, most mailbox providers do not send them.

rf: Format for message failure reports. The default is the Authentication Failure Reporting Format, or "afrf." Afrf is the only value supported at this time.

ri: The number of seconds elapsed between sending aggregate reports to the sender. The default value is 86400 seconds which is equivalent to one day.

The easiest way to create a DMARC record is through an online tool.

With GlockApps DMARC Analytics it takes a minute.

To publish a DMARC record to DNS, one must:

1. Log in to the DNS management console.

2. Navigate to the domain where the DMARC record will be published.

Most DNS management consoles will ask for:

Hostname: this should be _dmarc. NOTE: the leading “underbar” character is required!

Resource type: this is TXT, as DMARC records are published in the DNS as TXT resources.

Value: this is the DMARC record itself.

Example:

v=DMARC1; p=none; rua=mailto:example@ar.glockapps.com; ruf=mailto:example@fr.glockapps.com; fo=1;

3. Save the settings.

What are the Benefits of DMARC?

1. DMARC eliminates email spoofing.

Once set to the enforcement, DMARC ensures that only authorized senders can use the domain to send messages and guarantees that there is a match between what is used in the “From” message field and the “Return-Path” or DKIM signature field.

2. DMARC increases email deliverability.

If the message is DMARC aligned, it is always prioritized with regards to email placement. Email receiving systems have more trust in email messages that have strong authentication in place.

3. DMARC protects domain reputation.

Without DMARC, spammers can use someone else's domain to send unwanted messages, which will hurt the domain's reputation among mailbox providers. With the DMARC set up, scammers cannot deliver phishing messages on behalf of the domain – thus, the domain reputation is not affected.

4. DMARC gives visibility and control.

DMARC provides information about how the domain is being used across the Internet. DMARC reports show any source that sent emails using a specific domain, regardless of the source's location. If anyone starts abusing the domain, the owner will instantly see it in the DMARC report. If any of the domain owner's legal sources start sending unauthenticated emails, DMARC reports will show it and the domain owner will make the corrections.

5. DMARC enables brand recognition.

DMARC provides access to the BIMI (Brand Indicators for Message Identification) standard.

BIMI provides email senders yet another way to stand out in their recipient's Inbox by displaying their logo next to the message. This option gives an email instant brand recognition and credibility. Although it is a fairly new email standard, its adoption has already begun.

BIMI can be deployed if the strong email authentication is in place, and the "p=quarantine" or "p=reject" DMARC policy is applied to unauthenticated messages.

Misconceptions about DMARC

While DMARC is powerful, there are also some misunderstandings about it:

1. DMARC is a quick deliverability fix.

By adding a DMARC record with the "Quarantine" or "Reject" policy, the domain owner shows the mailbox provider that they are working on improving the security of the email streams. Therefore, email receivers are more likely to let emails land in the Inbox of the recipient. However, it is not just a quick email deliverability fix. Deploying and enforcing the DMARC policy is working for the perspective.

2. DMARC enforcement is a good start.

Using the DMARC enforcement (100% Reject policy) is indeed effective when blocking a detected phishing attack. If no attack takes place, DMARC enforcement will block legitimate messages that fail the DMARC check. It is recommended to start with a p=none policy, monitor the results, improve SPF and DKIM authentication if any breaches are detected, and then enforce the policy to p=quarantine.

It is strongly recommended to set the p=reject policy when the DMARC compliance rate is near 100%. Depending on the organization's email channels and setup, it can take from one to six months to achieve almost 100% compliance.

3. DMARC protects inbound emails.

DMARC is not designed to protect the inbound email streams. However, when the messages are sent to colleagues within the organization, DMARC will influence whether or not these messages are delivered and where.

Takeaway

DMARC enforcement should be applied to all of the domains, even to those, which do not send emails. It protects the brand, subscribers, customers, and partners from email impersonation and phishing attacks. Additionally, the domain owner will augment email security, sender reputation, and deliverability.

To implement strong domain protection we recommend starting the DMARC Analytics trial at GlockApps as the first step towards DMARC enforcement.