SocketLabs
the science of hitting the inbox

Understanding DMARC:

Your Guide to Powerful Email Authentication

An Email **Best Practices** Whitepaper

CONTENTS

Introduction

As marketing and transactional email becomes a more prominent part of modern business, the security of email has become a topic of much conversation. While the basic principles of SMTP have yet to change by any significant measure, modern technology has changed the rate at which we are able to configure, send, receive, and consume email. With this increase in traffic and overall usage of email comes an equal increase in malicious entities looking to take advantage of users through phishing, spoofing, and forgery tactics.

An increase in compromising email tactics demands an increase in security, which has been duly noted by the larger players in the email industry. This increase in security takes the form of many different measures including intelligent spam filters, advanced encryption, authentication protocols like SPF and DKIM, and the primary topic of this guide, DMARC (Domain-based Message Authentication, Reporting & Conformance).

DMARC is a protocol that is designed to prevent spammers from sending malicious email on behalf of your domain without your permission through a practice known as spoofing.

Modern Threats to Email Security: Phishing and Spoofing

Before you understand the ins and outs of how spammers conduct phishing and spoofing techniques, you need to first understand what a "message header" is. The majority of people do not know that emails contain a hidden section known as the "message header" which provides technical details about the email. The header can include information on who created the message, the software used to compose it, and the email servers it passed through on its way to the recipient.

```
Received: from s1-b4b4.socketlabs.email-od.com (s1-b4b4.socketlabs.email-od.com. [142.0.180.180])
        by mx.google.com with ESMTPS id w49si4926449qta.277.2019.08.05.09.24.36
        for <socketlabs@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-SHA bits=128/128);
        Mon, 05 Aug 2019 09:24:36 -0700 (PDT)
Received-SPF: pass (google.com: domain of 33d0.10.socketlabs=gmail.com@bounces.socketlabs.com designates 142.0.180.180 as permitted sender) client-ip=142.0.180.180;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@socketlabs.com header.s=dkim header.b=fCxNUcNB;
       dkim=pass header.i=@email-od.com header.s=dkim header.b=TU8oUiK3;
       spf=pass (google.com: domain of 33d0.10.socketlabs=gmail.com@bounces.socketlabs.com designates 142.0.180.180 as permitted sender)
smtp.mailfrom="33d0.10.socketlabs=gmail.com@bounces.socketlabs.com";
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=socketlabs.com
DKIM-Signature: v=1; a=rsa-sha256; d=socketlabs.com;s=dkim;
c=relaxed/relaxed; q=dns/txt; t=1565022276; x=1567614276; h=content-type:subject:date:reply-to:to:from:mime-version:message-id:list-unsubscribe:feedback-id:x-thread-info;
bh=U+lTRiZx1UmIOWavVvFxJCtf+nsoY3DUtPueCsGAkfE=;
b=fCxNUcNBi9EunxpnBkizn25ZXaN9KthvumNgHz9IImIo3Hn/GUQCQW5IP37W7E/N+zh1vX15lyQi4dlzOwz3G2Qc6Hdt5I7nXdGDv3hkNHhGziu42ENxDxRwvE6R1/eo5fcbYKL1pp/q8opq0/gnYPrW5CJdk9MJzuXWwx/iHIA=
```

There are two pieces of a message header; the "mail from", or the return path address, and the "envelope from" address. The return path address is typically hidden from recipients, and is used to tell the recipient server where to send a reply to if the message fails. The "envelope from" address is the visible portion of an email header that shows who the email is from. Information in the header that identifies who is sending the message can be forged by spammers in an act known as spoofing.

A **phishing attack** is when a malicious entity attempts to obtain sensitive information for financial or personal gain by disguising itself as a trustworthy company. The primary attack method for phishing is through **email spoofing**, the practice of sending messages with a falsified from address. Most users will not read emails from senders they do not recognize, and phishers take advantage of that trust by posing as a recognized sender.

What is DMARC?

DMARC, is a technology that aims to prevent spoofing by allowing domain owners to control what receiving mail servers do when messages do not pass certain authentication checks. By verifying the authenticity of messages coming from your domain, **DMARC is the first technology to give email domain owners the ability to protect their domain from unauthorized use.** With DMARC in place, senders and recipients alike can establish a healthier relationship as spammers and malicious actors find it harder to carry out deceptive email attacks by posing as a trusted contact.

Setting up a DMARC policy also lets domain owners/organizations get full reports on the email they are sending with information on:

- ✔ What percent of messages are being properly authenticated
- ✔ Which email aren't being authenticated
- ✔ Where the emails are coming from
- ✔ Who's receiving the emails, etc.

Answers to all of these questions can be provided by a DMARC report. This valuable information can help organizations and IT administrators make more informed decisions about their email strategy moving forward.

How DMARC Works

DMARC is not an authentication protocol, per se, but rather a security policy for domain owners built on top of existing SPF and DKIM authentication technologies. The primary function of DMARC is to align the functions of SPF and DKIM and to determine what action is taken on unauthenticated email. DMARC contemporaneously works to standardize and incentivize the use of SPF & DKIM authentication as the practice of implementing such authentication continues to become more relevant.

SPF (Sender Policy Framework) is a form of email authentication that specifically protects and authenticates the return path address used in the message delivery process, preventing "from address" forgery. It does this by ensuring that the sent email originated from a server that has permission to send emails on behalf of the sender.

DKIM (Domain Keys Identified Mail) is an email authentication mechanism that allows the recipient mail server to check if a message has been altered during transit. This is done by the recipient server, checking and verifying an encrypted signature left on the message by the sending server to ensure the message arrived in the same form that it was sent.

Socketlabs has created Free Email Tools to help developers and email administrators generate DKIM private and public keys.

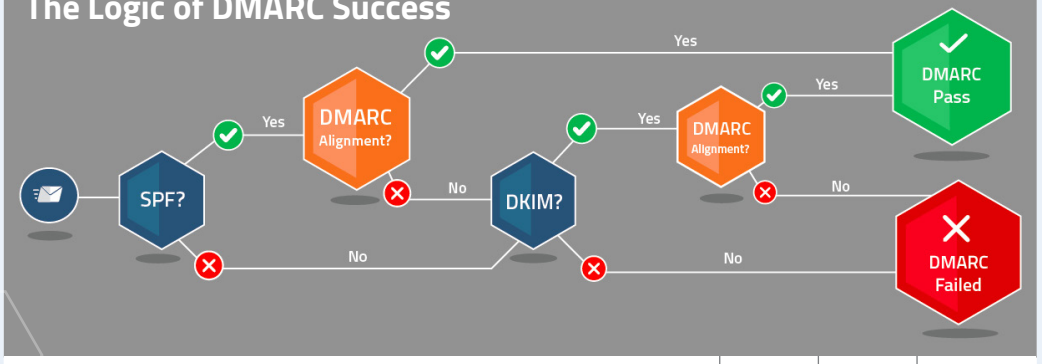
How DMARC Works
(continued)

(continued from previous page)

DMARC requires that a message must pass SPF and/or DKIM with alignment. A message will fail DMARC only if it fails both DKIM and SPF with alignment. More specifically, to pass DMARC an email must 1) pass either SPF or DKIM authentication (as explained above) and then 2) the authentication method that "passes" must also be in alignment.

For example, a message can have a valid DKIM signature, but if the DKIM signing domain is unrelated to the domain of the "from address", there is no alignment and DMARC will be considered as a failure assuming there is no validated and aligned SPF. For SPF alignment, the "from address" field in the email's message header must match the domain name in the "envelope from" used during SMTP communication.

The Logic of DMARC Success



	DKIM	SPF	DMARC
Provides confirmation that the email has not been altered during transit	X		
Provides confirmation that header was not spoofed		X	
Provides confirmation that message header was not spoofed (SPF) and/or was not altered in transit (DKIM)			X
Provides a comprehensive report on all emails being sent on behalf of their domain/organization			X

While SPF and DKIM may not be the answer to all deliverability and security issues, the proper implementation of DMARC at a technical level is a step in the right direction, as it requires one or both of these authentication technologies to be set up correctly.

When configured effectively, DMARC provides instructions to mailbox providers for how to handle messages that do not pass authentication and alignment of SPF and/or DKIM. Through DMARC, the email can be handled in three possible ways. Messages failing DMARC may be:

1. **Quarantined** - meaning unauthenticated email can be placed in an isolated location for further review
2. **Rejected** - meaning unauthenticated email is completely blocked before anyone sees it, or
3. **None** - meaning no action is taken upon failure and the message is delivered, regardless.

The action taken on an unauthorized email by your system (reject, quarantine, or none) is a function of which policy your email administrator chooses to configure.

How DMARC Impacts Deliverability

DMARC is not the be-all/end-all solution of email deliverability issues, and it is not for everyone. DMARC is only a concern for domains that are trying to eventually move to a "reject policy", and for organizations who care about their domain's branding being used without permission.

Implementing DMARC does not immediately help improve inbox placement rates. In fact, it could limit inbox placement because email authentication protocols can be rather sensitive in determining what gets through versus what doesn't. Having a DMARC "reject" policy can amplify such sensitivities, limiting the amount to email coming through that do not pass SPF or DKIM.

However, in the longer term, **a DMARC policy provides protection from malicious entities who are trying to leech your reputation.** By setting up and enforcing strict DMARC policies, you can help mailbox providers "authenticate" the emails you send which will indirectly help improve inbox placement over time by strengthening a sender's reputation.

Who is Using DMARC?

As you might expect, mailbox providers like Yahoo and AOL have DMARC policies for their users and other industry leaders are following. But aside from just the email giants, other industries like finance, healthcare, and insurance have also started to develop and implement DMARC policies of their own. This comes as an added layer of security for companies who have very sensitive data that needs added protection.

The Evolution of DMARC Within the Industry

In what was considered a controversial move, Yahoo was the first major mailbox provider to move to a full reject policy. This caused messages with Yahoo.com in the "envelope from" address and a different return path address, to fail delivery. At the time, because Yahoo had been the victim of a database leak, they had decided the sea of broken mailing lists left in the wake of their decision was worth the level of security that the policy provided their customers.

The controversial part of this decision was whether users of free mailbox services like Yahoo or AOL could use the address provided to send mailings through third party mail systems. By implementing their DMARC policy, Yahoo changed what had been a common email practice for years. Yahoo was followed shortly by AOL, who provided a little more warning in their choice of moving to a "reject policy".

Who is Using DMARC?
(continued)

Aside from the early adaptors, Office365 now has a "reject" policy, but tested the waters in the beginning with a quarantine policy. Verizon is also currently using a "quarantine" policy, and has not made any statements yet if they plan on moving to a "reject" policy. Comcast.net has a "none" policy set, and have expressed that they will not be moving to be a full "reject" policy. Sending on behalf of clients that use an email address from a provider like Gmail carries some risk. Gmail currently has a "p=none" policy, but has announced that they will be instituting a "reject" policy sometime soon.

Mailbox Provider DMARC Policy

	Reject Policy (reject)	Quarantine Policy (quarantine)	No Policy (none)
YAHOO	X		
AOL	X		
Gmail			X
Office 365	X		
Verizon		X	
Comcast			X

Other Industries and DMARC

Outside of the email industry leaders, others have taken DMARC to practice. There are a couple of business types you would expect to use a "reject" DMARC policy as a standard practice, such as banks, credit card companies, insurance, and health care providers, etc. While most of these businesses are moving towards DMARC policies, progress has been rather slow.

Financial institutions have DMARC records across the spectrum. Bank of America, American Express, Wells Fargo, and Chase are all using a "reject" policy, while other institutions, like Capital One, TD Bank, and Citizens Bank are collecting data are using a "none" policy.

Paypal, is the originator and one of the writers of the DMARC RFC. Naturally, they also have a "reject" policy. LinkedIn and Facebook are both using "reject". **Britain's Government Digital Service (GDS)** has stated that all agencies running on the sub-domain service.gov.uk are required to publish a DMARC "reject" policy as of October 1st, 2016.

Insurance agencies similarly differ in their decisions to use DMARC security policies. AETNA and HealthCare.gov are both "reject," and United Health One is using "none." And then there are a few organizations who are not even collecting data on how their domains are being used. PNC Bank, Blue Cross Blue Shield, State Farm, and Nationwide are just a few we found that have not published any sort of DMARC policy for their domains.

Implementing a DMARC Policy for Your Domain

Below is an example of a DMARC record that you would want to configure in your domain's DNS records. There are a variety of tags used in your DMARC record, but only the "version" tag (v=) and the "policy" tag (p=) are required for DMARC to be configured correctly. Currently, there is only one version of DMARC. The version tag was created for the future of DMARC.
"v=DMARC1; p=reject; pct=100; rua=mailto:postmaster@example.com"

Understanding DMARC Tags

Tag Name	Purpose	Sample
V=	Protocol version	v=DMARC1
P=	Policy for organizational domain	p=reject (or quarantine or none)
Pct=	Percentage of messages subjected to filtering	pct=100
Ruf=	Reporting URI for forensic reports	ruf=mailto:postmaster@example.com
Rua=	Reporting URI for aggregate reports	rua=mailto:postmaster@example.com
Sp=	Policy for subdomains of the OD	sp=reject
Adkim=	Alignment mode for DKIM	adkim=s
Aspf=	Alignment mode for SPF	aspf=r

The process of implementing DMARC does not need to be implemented all at once, rather it can be done in stages. Your first step is going to be setting up a mailbox to receive your aggregate DMARC reports.

DMARC.org suggests that a domain owner set the DMARC policy tag (p=) to "none" as a means to begin collecting data. Doing so is known as setting DMARC to "monitor mode." There are many tools available to a domain owner to view the collected data. The three most popular tools for DMARC belong to Dmarcian, Agari, and 250ok. SocketLabs currently has a "none" policy, and has been using Dmarcian's tools to monitor and adjust our domain's DMARC compliance before we move to a "reject" policy.

Once the data collected for your domain confirms that your legitimate traffic is passing authentication checks, you can change your policy to request that failing messages be quarantined. By setting your DMARC policy to "quarantine," you are instructing mail servers to put messages using your domain that fail DMARC checks into a location on the receiving email infrastructure and to send a report back to the RUA or RUF address specified in your policy. How exactly a message is quarantined is specified by the recipient system. Typical examples of quarantine are delivering the failed messages to spam folders or holding messages in a database for further investigation by an email administrator.

Implementing a DMARC Policy for Your Domain (continued)

Once you are confident that legitimate messages are not failing DMARC and being quarantined, you can change your policy to "reject."

Within the DMARC policy you can also control the granularity of messages that are subject to the policy. The "pct" flag denotes the percentage of messages that should be evaluated. The balance (those not being evaluated) are subjected to the next less-restrictive policy. For example, if you were to set your DMARC policy to "reject" and have "pct" set to "50," half of your messages would be rejected, and the other half would be quarantined. If you set the DMARC policy to "quarantine" and have the "pct" set to "50", half of your messages would be quarantined, and the other half would just process through without issue. The "pct" flag does not apply to monitor mode because "none" is the least restrictive of the modes available.

Socketlabs has created **Free Email Tools** to help developers and email administrators generate a valid DMARC policy for your domain.

The Future of DMARC

DMARC is a strong step in a positive direction for limiting nefarious email manipulation. Ensuring SPF and/or DKIM authentication will help enhance the safety of your email and improve the overall success of your ability to send, receive, and consume email.

While DMARC is a relatively new policy, its adoption is gaining momentum. As more major mailbox providers and industries implement DMARC policies, it will become an accepted norm across the email industry. Rather than avoiding it, organizations are best advised to embrace DMARC and use it as a tool to improve email security.

DMARC Authentication at SocketLabs®

At SocketLabs, we provide authentication with SPF and DKIM using our own domain in the authentication process. While this authentication uses our own domain as the default setting, it can easily be reconfigured to use your domain.

Since DMARC allows for domain owners to control what messages should be delivered, it is very important for clients who are sending messages on behalf of others to understand its impact. Our clients' customers who implement DMARC on their own domain (with either "quarantine" or "reject" policies) can send their mail through the SocketLabs' account. They can achieve this through the SocketLabs platform configuration tools using the authentication feature Custom Bounce Domain and the DKIM integration methods Custom DKIM or Advanced DKIM.

With a valid DMARC record in place for their domain, clients can begin to solicit DMARC data directly from supporting mailbox providers and publish reports regarding DMARC. As of May 1st, 2017, most, if not all, major mailbox providers all support DMARC, and publish reports regarding DMARC.

While the overall topic of DMARC can be a little overwhelming, especially in configuring it, SocketLabs' live support team can help you through every step of the journey.

About SocketLabs

SocketLabs is a B2B technology firm that provides flexible SaaS and on-premises solutions for solving a variety of complex email delivery challenges for both transactional and marketing messages. We are a pioneer in the Email Service Provider (ESP) market with a decade-long track record of excellence. Our unique, proprietary mail transfer agent (MTA) technology is trusted by clients around the globe who invigorate their SaaS platforms, mobile apps, and custom applications by "plugging in" to an unmatched email experience. Our founders have been creating cutting-edge email solutions for over 20 years and have built a customer support organization that considers "responsiveness and satisfaction" as our key performance objectives.

Email us!

support@socketlabs.com

Call us!

USA:
800.650.1639
International:
484.418.1285

Chat with us!

www.socketlabs.com/chat