E-BOOK

GETTING STARTED WITH DMARC

www.proofpoint.com

TABLE OF CONTENTS

INTRODUCTION

Email is great for business: it's inexpensive, scalable, and, most importantly, effective at driving leads and revenue. Unfortunately, the very things that make email so popular—ease of use, convenience, transparency—also make it a vector of choice for cybercriminals.

Email fraud costs companies around the world billions, and can destroy brand reputation and consumer trust in a matter of minutes. Email fraud is implicated in a quarter of all data breaches, causing the average 10,000-employee company an expense of $3.7 million a year. Highly-targeted, low volume business email compromise (BEC) scams are arguably the most dangerous, costing organizations around the globe $3.1 billion since January 2015, according the the FBI.

The DMARC standard, unveiled by a group of leading email organizations in February 2012, is the most powerful and proactive weapon to date in the fight against phishing and spoofing.

It has reshaped the email fraud landscape, disrupting long standing phishing strategies and forcing cybercriminals to abandon preferred targets. DMARC has the potential to nullify an entire class of fraud within the next few years.

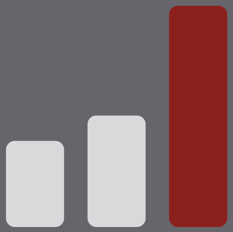
In this guide, we'll cover what DMARC is, how it works, its key benefits, and what it means to your organization.

$4.5B

Phishing costs brands around the globe $4.5 billion each year

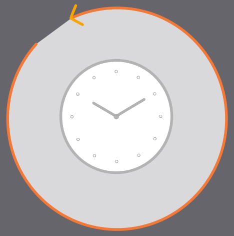
5/6

5 out of 6 big companies are targeted with phishing attacks



40%

Spear phishing rose 40% in 2014



1 MIN

RSA identifies a phishing attack every minute

WHAT IS DMARC?

Unveiled in 2012 by an industry consortium, DMARC—Domain-based Message Authentication Reporting & Conformance—is an open email authentication protocol that enables domain-level protection of the email channel.

Building on existing standards SPF and DKIM, DMARC is the first and only widely deployed technology that can make the "header from" domain (what users see in their email clients) trustworthy.

Domain-based

Message

Authentication

Reporting &

Conformance

Open email authentication standard

Launched in 2012

Founded by over 20 companies

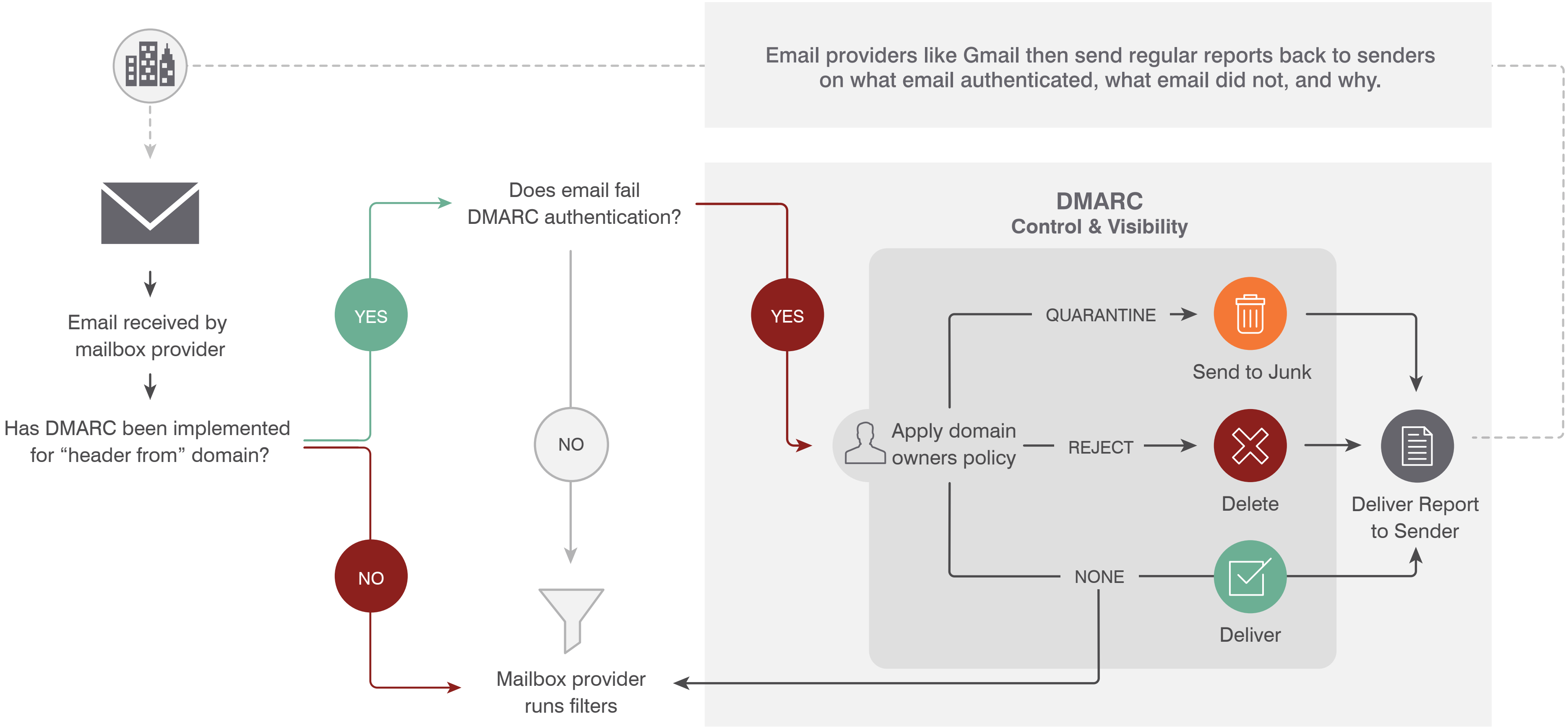
DMARC ALLOWS EMAIL SENDERS TO:

Reclaim control by authenticating legitimate email messages for their email-sending domains.

Instruct mailbox providers on how to treat messages that fail authentication, via an explicit policy setting. These messages can either be sent to a junk folder or rejected outright, protecting consumers from exposure to attacks.

Gain insights into the email threat landscape to help you identify threats against your customers and better protect your brand against phishing and spoofing.

HOW DMARC WORKS


Email providers like Gmail then send regular reports back to senders on what email authenticated, what email did not, and why.
Email received by mailbox provider
Has DMARC been implemented for “header from” domain?
YES
NO
Does email fail DMARC authentication?
NO
YES
Mailbox provider runs filters
DMARC
Control & Visibility
Apply domain owners policy
QUARANTINE
Send to Junk
REJECT
Delete
NONE
Deliver
Deliver Report to Sender

DMARC POLICY SETTINGS:

✓ **None:** The entire email authentication ecosystem is monitored to map out legitimate traffic.

Quarantine: Messages that fail DMARC move to the spam folder.

✕ **Reject:** Messages that fail DMARC do not get delivered at all.

WHY DMARC?

DMARC EMPOWERS SENDERS TO...

- Gain visibility into who is sending on your behalf, what email is authenticating, what email is not, and why.
- Instruct email receivers on how to handle mail that does not pass authentication.
- Block phishing attacks spoofing owned domains before they reach employee and consumer inboxes.

DMARC EMPOWERS RECEIVERS TO...

- Distinguish between legitimate senders and malicious senders.
- Foster consumer loyalty and employee protection.
- Improve and protect the reputation of the email channel.

> "SIMPLY PUT, THE DMARC STANDARD WORKS. IN A BLENDED APPROACH TO FIGHT EMAIL FRAUD, DMARC REPRESENTS THE CORNERSTONE OF TECHNICAL CONTROLS...TO REBUILD TRUST AND RETAKE THE EMAIL CHANNEL FOR LEGITIMATE BRANDS AND CONSUMERS."
>
> Edward Tucker, Head of Cyber Security, HM Revenue & Customs

> "WITH STRICTER DMARC POLICIES, USERS ARE SAFER, AND THE BAD GUYS WILL BE IN A TOUGH SPOT. MORE IMPORTANTLY, VERIFIED SENDERS WILL UNLOCK A MASSIVE WAVE OF INNOVATION AND ADVANCEMENT FOR ALL OUR INBOXES."
>
> Jeff Bonforte, SVP of Communications Products, Yahoo

THE BENEFITS OF DMARC

PROTECTS EMPLOYEES, BUSINESS PARTNERS, AND CONSUMERS.	DMARC eliminates an entire class of fraudulent email before it reaches your employees, partners, and customers.
GIVES IMMEDIATE INSIGHT INTO THE EMAIL THREAT LANDSCAPE.	You can't control what you can't see! Implementing DMARC gives you instant visibility into the threats targeting your company. It effectively shines a light on domain phishing and spoofing attacks putting your customers and brand reputation at risk.
INCREASES EMAIL DELIVERABILITY AND ENGAGEMENT.	Approximately one in five phishing attacks results in reduced deliverability and one in three results in reduced email engagement. DMARC increases both deliverability and engagement of legitimate email programs.
REDUCES CUSTOMER SERVICE COSTS.	By blocking phishing attacks, DMARC dramatically reduces customer service costs. Scandinavian retailer Blocket saw a 70 percent drop in customer service tickets after implementing DMARC.
REDUCES PHISHING REMEDIATION COSTS.	Phishing costs brands $4.5 billion every year. DMARC reduces the spend on fraud, reimbursement, and phishing remediation costs.

DMARC BY THE NUMBERS

70%
of global consumer mailboxes are currently DMARC-enabled.

24%
year-over-year DMARC adoption across 1,000 top global brands.

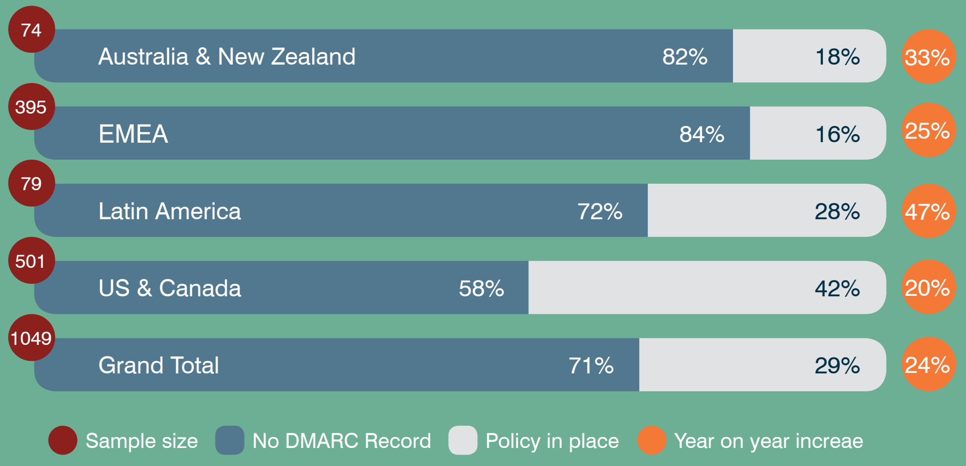
122%
year-over-year increase in users that sent 100 or more DMARC reports.

145%
year-over-year increase in the number of domains with a reject policy.

2016 DMARC ADOPTION BY INDUSTRY

Vertical	Sample Size	DMARC Adoption
Social Media	59	59%
Technology	61	51%
Logistics	22	41%
Payment Services	87	32%
Travel	110	31%
Banking	275	27%
Retail/Gaming/ eCommerce	267	25%
Public Sector	16	25%
ISP/Telco	77	21%
Healthcare	75	16%
Total	1,049	29%

2016 DMARC SENDER ADOPTION GROWTH WORLDWIDE



Source: Proofpoint

EMAIL AUTHENTICATION AT A GLANCE

DMARC is built on the backbone of two other extremely important email authentication standards, SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail). To fully understand DMARC, you must also understand the benefits—and the failings—of SPF and DKIM.

	SPF (Sender Policy Framework) www.openspf.org	**DKIM** (DomainKeys Identified Mail) www.dkim.org	**DMARC** (Domain-based Message Authentication Reporting & Conformance) www.dmarc.org
Benefits	SPF allows brands to specify who can send email on behalf of their domain. Brands list the IP addresses of authorized senders in a DNS record. If the IP address sending email on behalf of the brand isn't listed in that SPF record, the message fails SPF authentication.	DKIM allows an organization to take responsibility for transmitting a message in a way that can be verified by the email provider. This verification is made possible through cryptographic authentication within the digital signature of the email.	DMARC ensures that legitimate email is properly authenticating against established DKIM and SPF standards, and that fraudulent activity appearing to come from domains under a brand's control is blocked before ever reaching the customer's inbox.
Example DNS Record	v=spf1 ip4:204.200.197.197 -all	v=DKIM1; p=MIGfMA0GCSqGSIb3DQEBAQUAA4G NADCBiQKBgQDfl0chtL4siFYCrSPxw43fqc4z Oo3N	v=DMARC1; p=reject; fo=1; rua=mailto:dmarc_agg@auth.yourdomain.com;ruf=mailto:dmarc_afrf@auth.yourdomain.com
Failings	• Keeping SPF records updated as brands change service providers and add mail streams is difficult. • Just because a message fails SPF, doesn't mean it will always be blocked from the inbox. • SPF breaks when a message is forwarded. • SPF does nothing to protect brands against cybercriminals who spoof the Display Name or "header from" address in their message.	• DKIM is more difficult to implement, thus fewer senders adopt it. • This spotty adoption means that the absence of a DKIM signature does not necessarily indicate the email is fraudulent. • DKIM alone is not a universally reliable way of authenticating the identity of a sender. • The DKIM domain is not visible to the non-technical end user, and does nothing to prevent the spoofing of the visible "header from" domain.	• While essential, DMARC is not a complete solution. • DMARC only protects your brand from 30 percent of email attacks (direct domain threats). • DMARC does not protect against brand spoofing (including Display Name spoofing and look alike domains).

DMARC CHAMPIONS—BRANDS

These DMARC champions have paved the way for the standard. These early adopters are at the forefront of the fight against email fraud and are proactively defending their customers against cybercriminals.

> "MORE AND MORE COMPANIES HAVE BEEN ADOPTING DMARC AND EMAIL AUTHENTICATION OVER THE PAST FEW YEARS, WITH MORE VENDORS AND SERVICE PROVIDERS ADDING THE NECESSARY SUPPORT TO THEIR OFFERINGS IN ORDER TO MAKE THAT ADOPTION SIMPLER."
>
> Steven Jones, DMARC.org

DMARC
Skrill
VISA
HM Revenue & Customs
IHG
InterContinental Hotels Group
RBS
The Royal Bank of Scotland
PCH
Publishers Clearing House
USAA®
FedEx
DELTA
blocket

> "AFTER WE IMPLEMENTED A DMARC REJECT POLICY, WE SAW PHISHING CUSTOMER SERVICE TICKETS DROP BY MORE THAN 70% WHICH MEANT THAT SERVICE STAFF WERE ABLE TO FOCUS ON ASSISTING CUSTOMERS WITH REVENUE GENERATING INQUIRIES."
>
> Thomas Bäcker, Head of Customer Security, Blocket

DMARC CHAMPIONS—MAILBOX PROVIDERS

Some of the world's largest mailbox providers are supporting DMARC. Today, it is estimated that 70% of the world's consumer inboxes are protected by DMARC.

> "WE'RE RAPIDLY MOVING TOWARD A WORLD WHERE ALL EMAIL IS AUTHENTICATED. IMPLEMENTING A DMARC POLICY ENSURES THAT A SENDER'S REPUTATION DOESN'T DROP DUE TO THE ACTIONS OF SPAMMERS. IF YOUR DOMAIN DOESN'T PROTECT ITSELF WITH DMARC, YOU WILL BE INCREASINGLY LIKELY TO SEE YOUR MESSAGES SENT DIRECTLY TO A SPAM FOLDER OR EVEN REJECTED."
>
> John Rae-Grant, Product Manager, Google

DMARC
YAHOO!
Microsoft
Aol.
COMCAST
Outlook.com
at&t
BT

> "OVERNIGHT, THE BAD GUYS WHO HAVE USED EMAIL SPOOFING TO FORGE EMAILS AND LAUNCH PHISHING ATTEMPTS PRETENDING TO COME FROM A YAHOO! MAIL ACCOUNT WERE NEARLY STOPPED IN THEIR TRACKS."
>
> Jeff Bonforte, SVP of Communications Products, Yahoo

DMARC TAG GLOSSARY

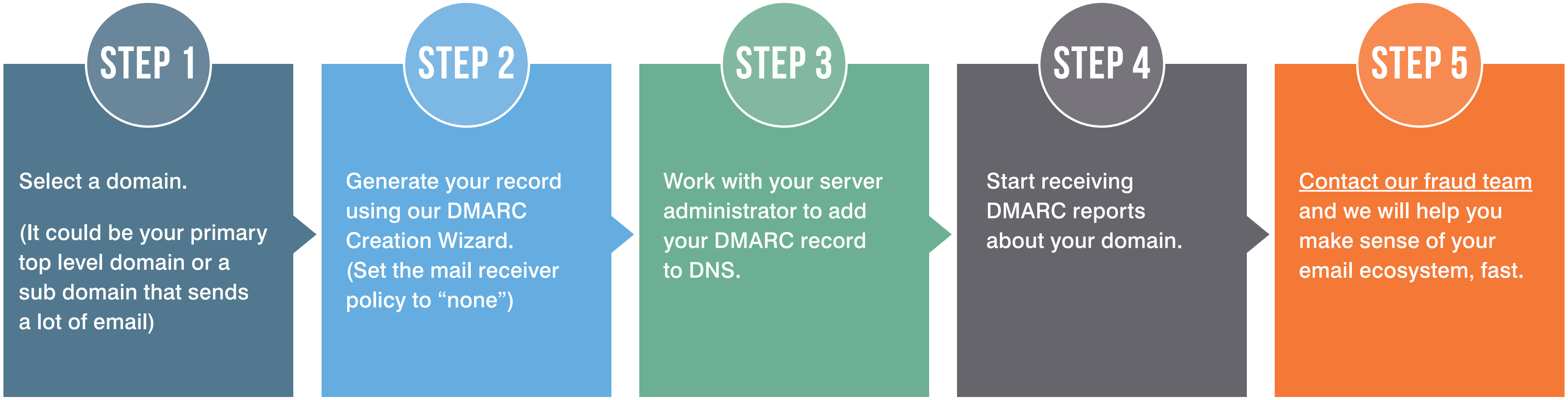
DMARC tags are the language of the DMARC standard. They tell the email receiver to check for DMARC and instruct them on what to do with messages that fail authentication. For more information on all DMARC tags, click here.

Tag Name	Required?	Purpose	Sample
v	Yes	Protocol version	v=DMARC1
p	Yes	Policy for domain	p=quarantine
pct	Optional	% of messages subjected to filtering	pct=20
rua	Optional	Reporting URI of aggregate reports	rua=mailto:aggrep@example.com
sp	Optional	Policy for subdomains of the domain	sp=reject
aspf	Optional	Alignment mode for SPF (strict or relaxed)	aspf=r
ruf	Optional	Reporting URI of forensic reports	ruf=mailto:aggrep@example.com
adkim	Optional	Alignment for DKIM (strict or relaxed)	adkim=r
ri	Optional	The number of seconds elapsed between sending aggregate reports to sender.	ri=86400
fo	Optional	Provides options for generation of failure reports.	“fo=1”

TIME TO START YOUR DMARC JOURNEY!

At Proofpoint, we help some of the world's largest brands successfully complete their DMARC journey. And while every organization will confront challenges when implementing DMARC, these standard steps will help guide all parties toward full deployment over time.

It starts with a very simple first step: create a DMARC record in DNS and shine a light onto your entire email ecosystem.



STEP 1

Select a domain.

(It could be your primary top level domain or a sub domain that sends a lot of email)

STEP 2

Generate your record using our DMARC Creation Wizard. (Set the mail receiver policy to "none")

STEP 3

Work with your server administrator to add your DMARC record to DNS.

STEP 4

Start receiving DMARC reports about your domain.

STEP 5

Contact our fraud team and we will help you make sense of your email ecosystem, fast.

Congratulations! You have taken your first steps to fighting email fraud.

Contact us to protect your employees, business partners, and customers from today's advanced email threats

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.

proofpoint.™

www.proofpoint.com