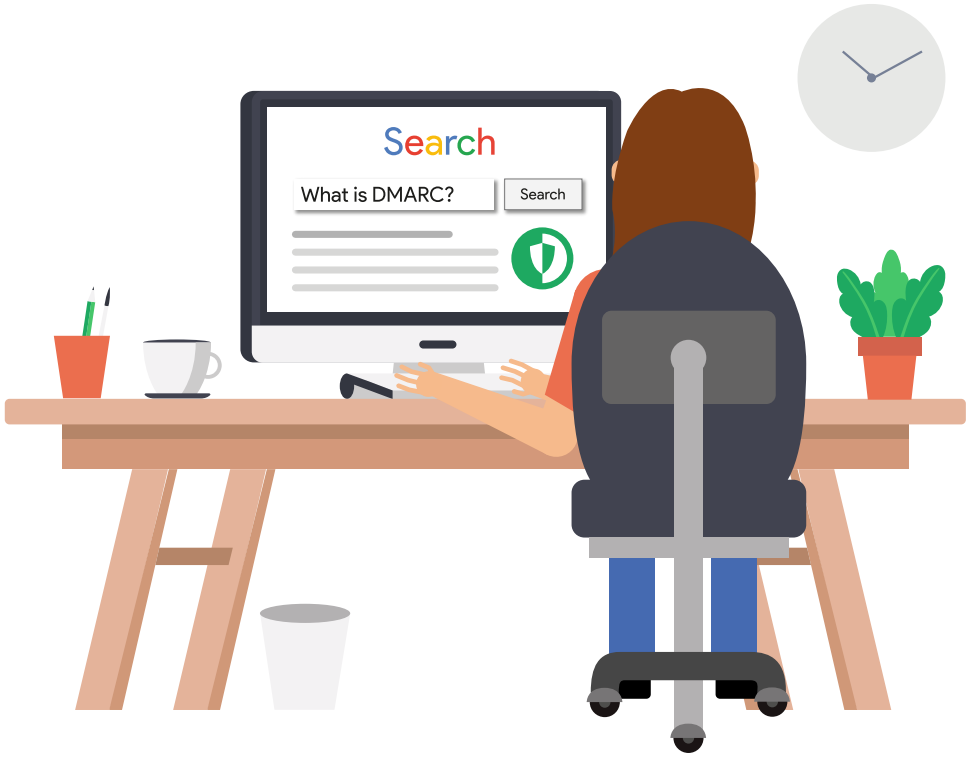
# DMARC: What is it and why should it be your next priority?

The email authentication protocol that reliably reduces phishing attacks and improves deliverability.



# Contents

# 1. A brief history of email

1971
First email sent

1981
ASCII encoding launched

1982
SMTP established

1988
Microsoft and Compuserve offer email via dial-up

1991
First email sent from space

1992
Email attachments introduced

1998
The term “spam” coined

2003
Mobile email boom started with Blackberry Quark

2004
DKIM introduced

2005
SPF introduced

2008
“SMTP mail is inherently insecure” - RFC5321

2012
DMARC born

2017
269 billion[1] emails sent everyday

2018
DMARC adoption rises by 51%[2]

## 2. Email: The easy way in?

According to Verizon's 2019 Data Breach Investigations[3] email continues to be the most common vector of phishing attacks, making it a **top cybersecurity concern** for organizations.

### Spam

More than 50% of emails are spam and criminals regularly use spam emails as a vehicle for malware.

### Advance-fee scams

These are targeted at vulnerable individuals, with scammers attempting to elicit money or bank details in exchange for the promise of rewards or for charity (for example, the Nigerian 419 scams[4]).

### Spear phishing

This is an evolution of the traditional phishing email, where scammers directly target individuals or organizations with content that is relevant to them. These scammers research the individual or organization in question - a task made simple by professional networking sites such as LinkedIn - to make the email appear legitimate.

Whale phishing is a version of spear phishing whereby a scammer sends a phishing email to a senior executive (the 'big fish'). Social engineering is key to successful phishing scams with 93% of data breaches linked to social engineering incidents[5].

# 3. Is your email security defending against one threat and wide open to another?

Email security technologies come in many forms but ultimately all forms are intended to keep the volume of spam emails to a minimum and to detect unwanted content (from malware to suspicious links) to prevent them reaching the user's mailbox.

More often than not these technologies look for the most common traits of a malicious email such as a blacklisted IP address, or a dodgy domain and block it to protect the recipient.

This is due to an unanticipated flaw in the global email infrastructure which exposes every organization.

## *But what if the email comes from a legitimate domain?*

All email security measures, other than DMARC, are likely to be virtually ineffective when an email comes from a legitimate domain.

This is due to an unanticipated flaw in the global email infrastructure which exposes every organization to the risk of being phished as the result of the Simple Mail Transfer Protocol (SMTP), originally designed without considering security. This has left standards for sending email today still open to data and financial theft because an email can easily be sent under someone else's domain name.

## Email impersonation: Your evil twin

Anyone with even the most limited knowledge of coding can learn the basic steps required to impersonate someone's email identity. All it takes is a quick Google search. The result is an email that looks legitimate and does not have the typical indicators of a phishing attack, such as a suspicious email address. An email server will allow such an email into a user's inbox if the appropriate security measures are not in place, where it will be difficult for the user to identify that the email is a phishing attack.

## Sophistication levels of phishing attacks

1 Obviously suspicious
*hsbc@yourbank.com*

2 Looks genuine
*customercare@hsbo.com*

3 Spoofing
*info@hsbc.com*

Looking at the illustration above, it is not surprising that many users are deceived by phishing emails. Although there will not have been any wrongdoing by the organizations which are impersonated in these cases, and a spammer does not need to access their systems in order to impersonate them, many governments and regulators consider that organizations have a responsibility to safeguard their customers against phishing attacks. As such, organizations which have not taken appropriate measures to safeguard their customers may be liable for a data breach.

## Email impersonation bypasses the following security measures:

Strong passwords

Biometrics

Two-factor authentication

Security protection dongle

In the last decade, a series of email security protocols have been introduced by industry leaders to provide email authenticity and to block phishing emails, as well as to increase the deliverability of genuine emails.

## Potential spoofing scenarios

A phishing email usually contains instructions of the following nature

| *Internal* | *External* | *Outcome* |
|---|---|---|
| Please pay this invoice | Your debit details have expired... | Financial loss |
| Can you send over that contract? | I need to confirm your personal details | Data loss |
| See the attached HR presentation | Follow this link to reset your password... | Cyber attack |


Time to
meet
DMARC

# 4. DMARC

In 2011, several of the major global email providers came together in an attempt to put an end to phishing.

Although there were already two email security protocols in place at that time Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM), neither protocol effectively prevented phishing.

***SPF***

This protocol verifies emails which are sent from a valid IP address.

***DKIM***

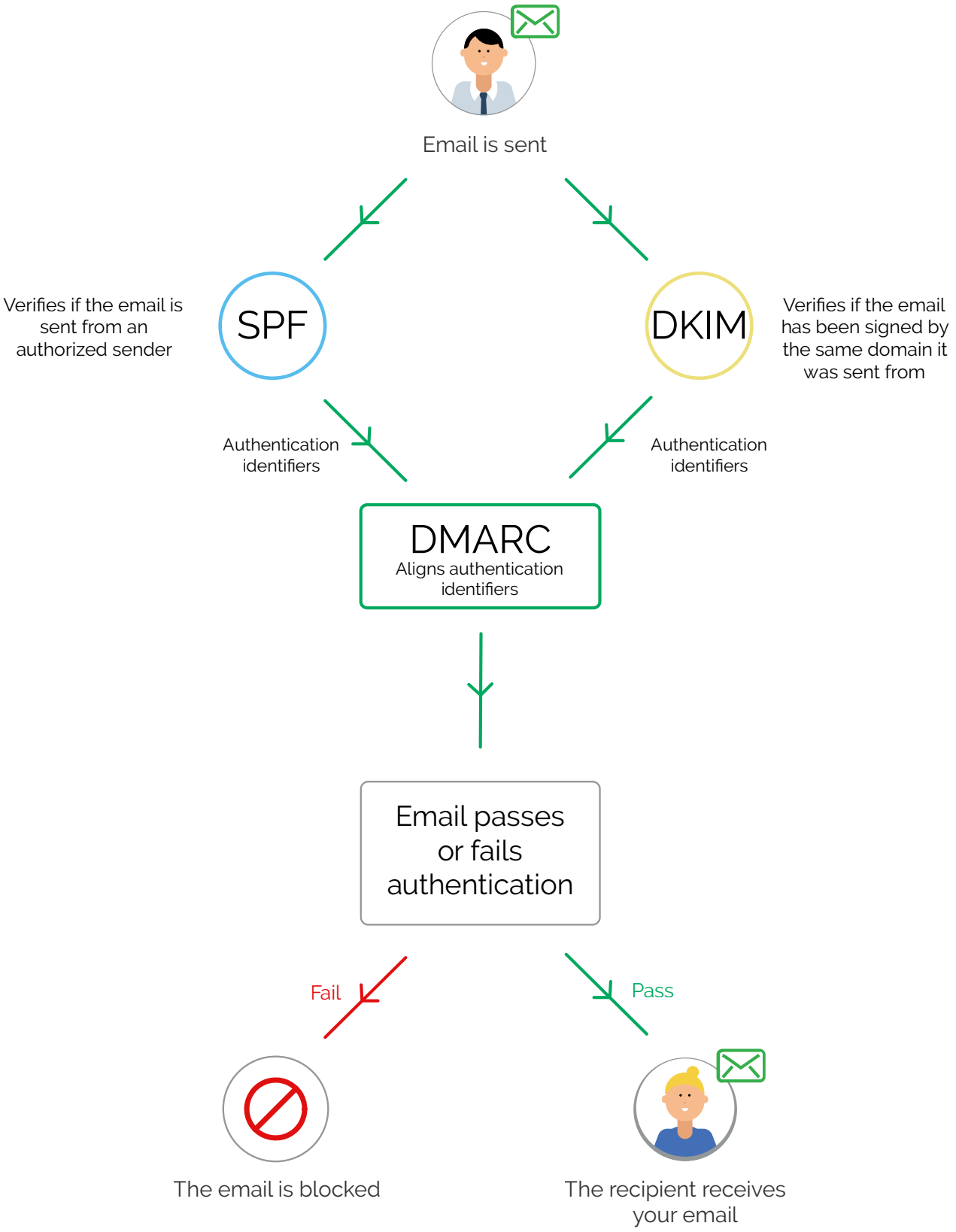
This protocol verifies that the received emails have been digitally signed by the domain they were sent from or on behalf of.

While these protocols had been accepted by the major global email providers, a secondary layer was required to actually block the emails being identified by the protocols as fraudulent or spoof.

## *DMARC*

In 2012, the **Domain-based Messaging, Authentication and Reporting Conformance** (DMARC) was ratified so that domain owners could take back control of their email identity by telling receiving inboxes to reject spoof emails. The authentication of an email's origin via DMARC also greatly improves deliverability.

# 5. How DMARC works



## Actions speak louder than words: Turning security policies into live defenses

The delivery of emails is handled by DMARC by choosing one of the following three policies, which can be set by the domain owner:

- ***p=none*** - this policy allows all emails to reach the receiver, regardless of whether they have been authorized.
- ***p=quarantine*** - this policy determines that emails which fail DMARC validation will be sent to the receiver's junk/spam folder.
- ***p=reject*** - this policy determines that all unauthorized emails are completely blocked.

Regardless of which policy the domain is set to, reports will be sent to the user to help identify the email sources with appropriate authentication, and those without (these are unauthorized).

## Which organizations are already using DMARC?

**Senders**

DMARC has already been implemented by a number of large brands and organizations, most of which are already in protection mode, including:

- Adobe
- Amazon
- AOL
- CNN
- Dropbox
- Facebook
- Google
- Instagram
- Microsoft
- PayPal
- Pinterest
- Pret-a-Manger
- Telefonica
- Transferwise
- Twitter
- Verizon
- Yahoo
- YouTube

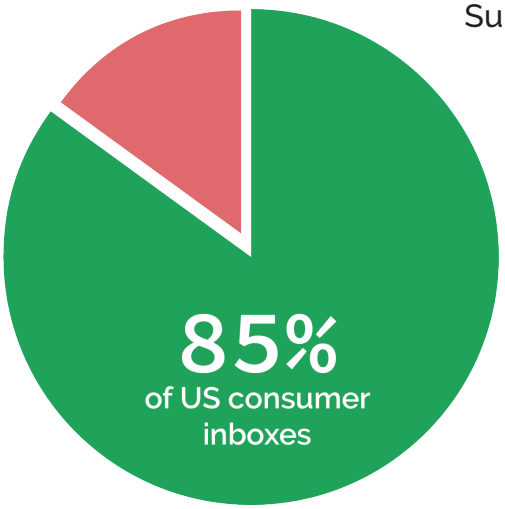
## Recipients

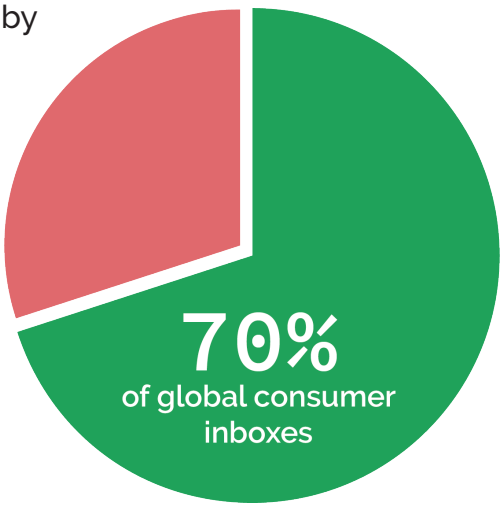
DMARC has been widely adopted by most email receivers (including Google, Yahoo, and Microsoft), which means that most consumer inboxes are already protected. DMARC already protects 85% of consumer US inboxes and approximately 70% of consumer inboxes worldwide from phishing emails, provided that the organization that is being impersonated in a phishing email has a published DMARC record.

*It is important to note that an organization which has implemented DMARC will not be notified of phishing emails which impersonate that organization if the inbox of the recipient of the relevant email has not enabled DMARC.*

- Since **2015**, Gartner has included the provision of DMARC as a qualifying feature for its Magic Quadrant for Secure Email Gateways 'leader' position.
- In **2016**, the UK Government mandated DMARC as a must-have minimum for a new standards framework for all ".gov.uk" domains by March 2019. This ensured that emails in transit are authenticated.
- In **2017**, the U.S. Government mandated DMARC for its Department of Homeland Security domains.
- **2018**, The NCSC (Part of GCHQ) issue guidance to make it a top 5 priority for the board - "Organisations that deploy these measures properly can ensure that their email addresses are not used by criminals".[6]

Supported by



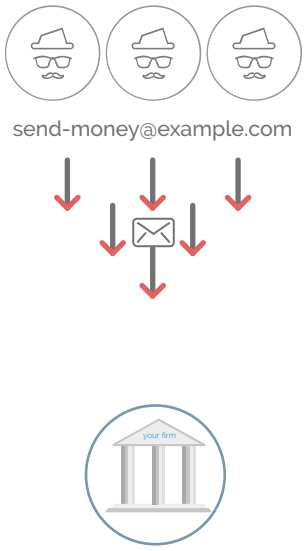
# 6. How to communicate the need for DMARC

You can check your organization's current DMARC set-up at ***www.ondmarc.com***, where you'll get clear information on the status of your DMARC, SPF and DKIM. It'll also let you know whether your inbox and DNS are compatible with DMARC.

## Complete visibility of your email landscape

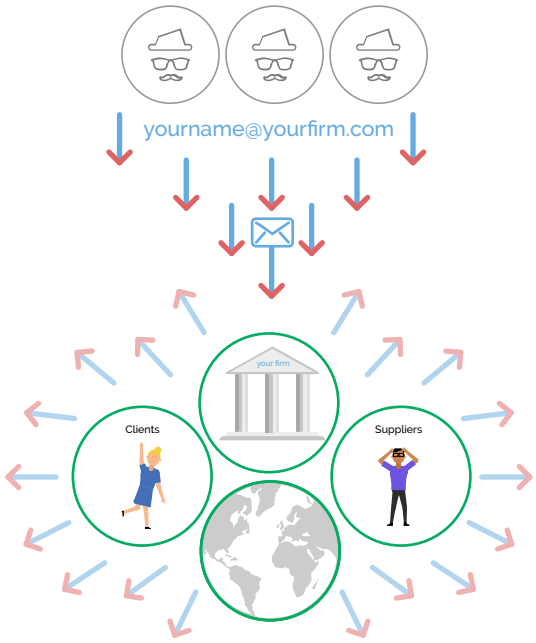
DMARC provides reports to users showing most, if not all, emails that come from a user's domain, not just those that cross the organization's network boundary. This contrasts with traditional cybersecurity solutions, such as MessageLabs and Mimecast, which only pick up phishing emails that cross the network boundary. Without DMARC, organizations are therefore not getting a complete picture of the number and scale of attacks against them.

Hackers send email phishing attacks to your firm




Various cyber security solutions filter inbound email

Hackers can impersonate your email address and send phishing attacks inside and outside your firm




OnDMARC stops impersonation of your email address gobally.

## Protect your reputation

Organization's domains subject to email spoofing may suffer considerable reputational damage. Phishing scams may well attract negative press, with liability often attributed to the organization which has been impersonated.

## Ensure financial security

Paying fake invoices or completing wire transfers impersonating the CEO are common mistakes incurred as a result of email spoofing. In fact, the financial cost has consistently increased according to The UK Government's 2018 Cybersecurity Breaches Survey[7].

## Comply with GDPR

General Data Protection Regulation (GDPR) came into force May 2018, requiring you to have Data Processing Agreements (DPAs) with every cloud service provider that handles EU consumer data on your behalf. With DMARC, if a cloud service provider does send email using your company's domain name in the 'From' field then DMARC will reveal them to you.

## Improve email deliverability

Email providers, such as Gmail, Yahoo and Hotmail, are becoming more protective of their users' inboxes.  An email provider may well refuse to deliver an email to a user's inbox if it does not have a SPF and/or DKIM signature.

With DMARC, emails are reliably authenticated, thereby improving the deliverability of legitimate emails to a user's inbox.

## Nurture trust

Organizations that fail to take the necessary precautions to prevent email spoofing are likely to be considered less trustworthy. Customers may not trust emails which purport to come from such organizations and may be deterred from using email to communicate with them, which can impact on those organizations' ability to communicate effectively with their customers.

## Identify and remove shadow IT

It's not easy to find all "shadow IT" cloud services. For example, If someone in Marketing set up an account with a Salesforce add-on years ago that no one in IT knows about and it sends emails to customers, then you would need to check DPA's (Data Processing Agreements) are in place. Implementing the email protocol DMARC uncovers all the email services sending email from your domain, whether you officially know about them, or not.

The costs of data theft as a result of spam emails continue to escalate, but adopting **DMARC** could save an organization thousands, if not millions, of dollars.

## Answering common objections

- **Why should we prioritize adopting DMARC?**

  DMARC is fundamental to cybersecurity. The UK's National Cyber Security Centre declared that, ***"Widespread adoption of the DMARC protocol is essential to defend against targeted cyber threats."*** [8] An organization which spends money on sophisticated and expensive security measures but fails to deploy DMARC is analogous to a homeowner installing a high-tech burglar alarm but leaving the front door unlocked.

- **Why should we pay for something that is an open standard?**

  You can deploy DMARC at no cost by configuring your own reports, interpreting the results and then adjusting your SPF and DKIM configurations accordingly. However, DMARC XML reports are very lengthy and require staff resourcing to interpret the data and make adjustments accordingly. DMARC providers, such as ***OnDMARC***, provide support in interpreting these reports and guidance on the appropriate DMARC configuration to get to the stage of being able to implement p=quarantine or p=reject policies more quickly.

- **We haven't deployed SPF and/or DKIM yet - don't we have to do that first?**

  You don't need to have deployed SPF and/or DKIM to get up and running with DMARC. In fact, the insight from your DMARC reports will help you to correctly deploy and configure SPF and DKIM.

- **DMARC seems to be really complex to deploy based on our experience with other cybersecurity providers.**

  Deploying DMARC should be a logical and iterative process, however it does rely on a certain level of expertise about email security. A good DMARC provider, such as ***OnDMARC***, will massively simplify this process and help you to reach full protection mode.

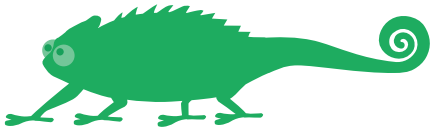
- **I'm concerned that implementing DMARC is going to affect our current email deliverability.**

  DMARC will improve your email deliverability significantly, providing that it is correctly configured. An easy-to-use DMARC provider, such as ***OnDMARC***, will help you reach full protection mode far more quickly, minimizing day-to-day email operational issues and helping your organization achieve a far higher level of email deliverability.

- **We already have Mimecast/Messagelabs - doesn't that do this job?**

  Most of the email security solutions currently available do not give organizations total protection against email impersonation. This is because they focus on preventing security breaches which result in spam emails being sent from within an organization's network boundary. They do not prevent attacks which originate outside the organization's network and which will not cross the network boundary. The DMARC protocol is the only way to close this loophole by ring fencing an organization's domain and preventing spammers from impersonating it.

The potential costs of data theft and loss of services continue to escalate, but simple measures, such as ***DMARC***, could save single organizations, thousands, if not millions of dollars.



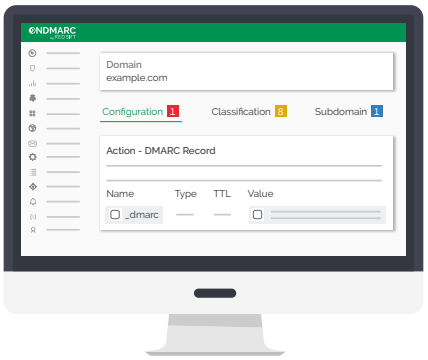
# 7. What's next?

We hope that you found this guide useful to start building your own understanding of DMARC and its security benefits in a way that's clear and easy to communicate to others in the business.

We recommend you check out Part 2 of the DMARC Digest series Finding your perfect DMARC provider for a clear and concise checklist of everything you need to know to identify a trusted and proven DMARC provider for your organization.

## Want to see DMARC in action?

An easy-to-use DMARC provider, such as ***OnDMARC*** will help you reach full protection mode far more quickly. Test the waters to see how simple it is to navigate your email landscape and take the first steps to secure your domain from impersonation by signing up to our free trial at: https://login.ondmarc.com/signup.




Stay safe,

*Team OnDMARC*

**References**

1. http://www.radicati.com/wp/wp-content/uploads/2017/01/Email-Statistics-Report-2017-2021-Executive-Summary.pdf
2. https://techcrunch.com/2018/11/01/half-fortune-500-dmarc-email-security/
3. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
4. http://www.newsweek.com/origins-nigerias-notorious-419-scams-456701
5. https://enterprise.verizon.com/resources/reports/dbir/
6. https://www.ncsc.gov.uk/guidance/board-toolkit-five-questions-your-boards-agenda
7. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf
8. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf


## Start your DMARC conversation today!

www.ondmarc.redsift.com

ONDMARC

The Red Sift Open Cloud is a data analysis platform that is purpose-built for the challenges of cybersecurity. By harnessing the power of AI we can securely collate, compute & visualize data from thousands of individual signals to help organizations to optimize their cybersecurity.

Our first product on the Red Sift platform is OnDMARC, a SaaS product that helps to implement and maintain DMARC. This email authentication protocol effectively blocks phishing attacks and increases the deliverability of genuine emails.


www.ondmarc.redsift.com
contact@redsift.com
@redsift