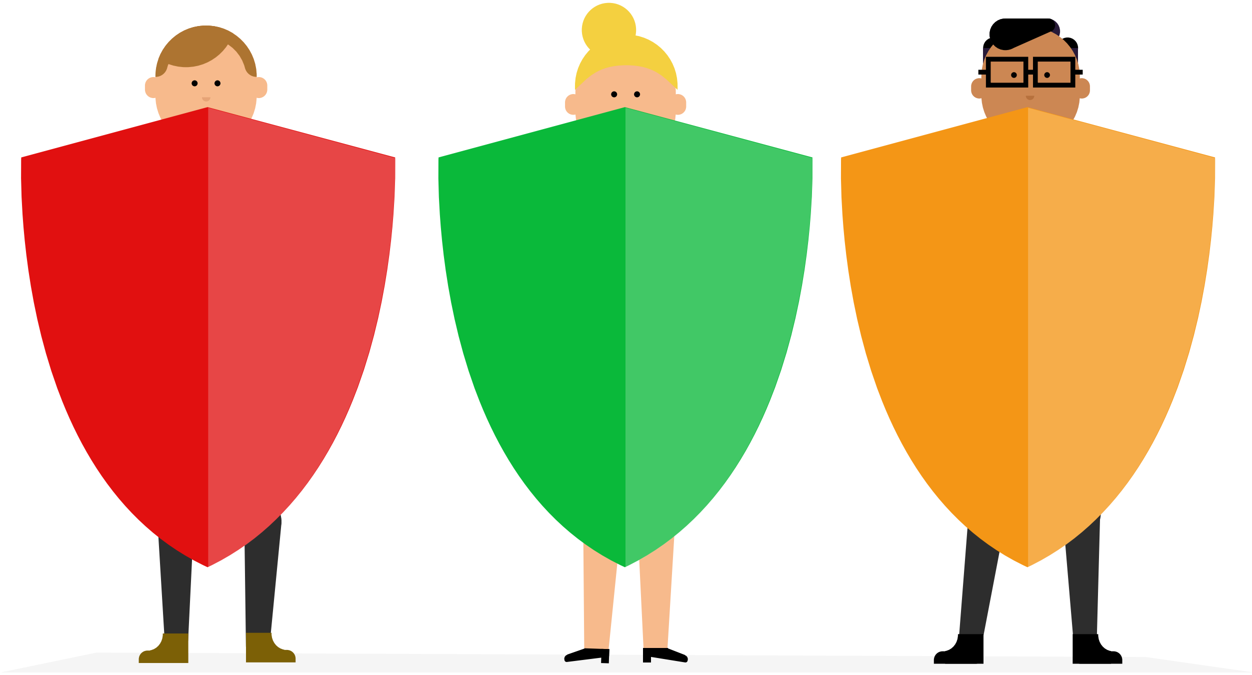
A Buyer's Guide to DMARC

Meet the cybersecurity protocol that reduces phishing attacks and improves email deliverability



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]

Email: The easy way in?

According to Verizon's 2018 Data Breach Investigations[3] email continues to be the most common vector of phishing attacks, making it a **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].

Is your email security defending 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 from 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 a result of the Simple Mail Transfer Protocol (SMTP), originally being 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

It is not surprising that many users are deceived by phishing emails. Although there will not have been any wrongdoing by the organizations, and a spammer does not need to access their systems to carry out an attack. Many governments and regulators consider organizations to 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

Dongle

In the last decade, a series of email 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

DMARC

In 2012, 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

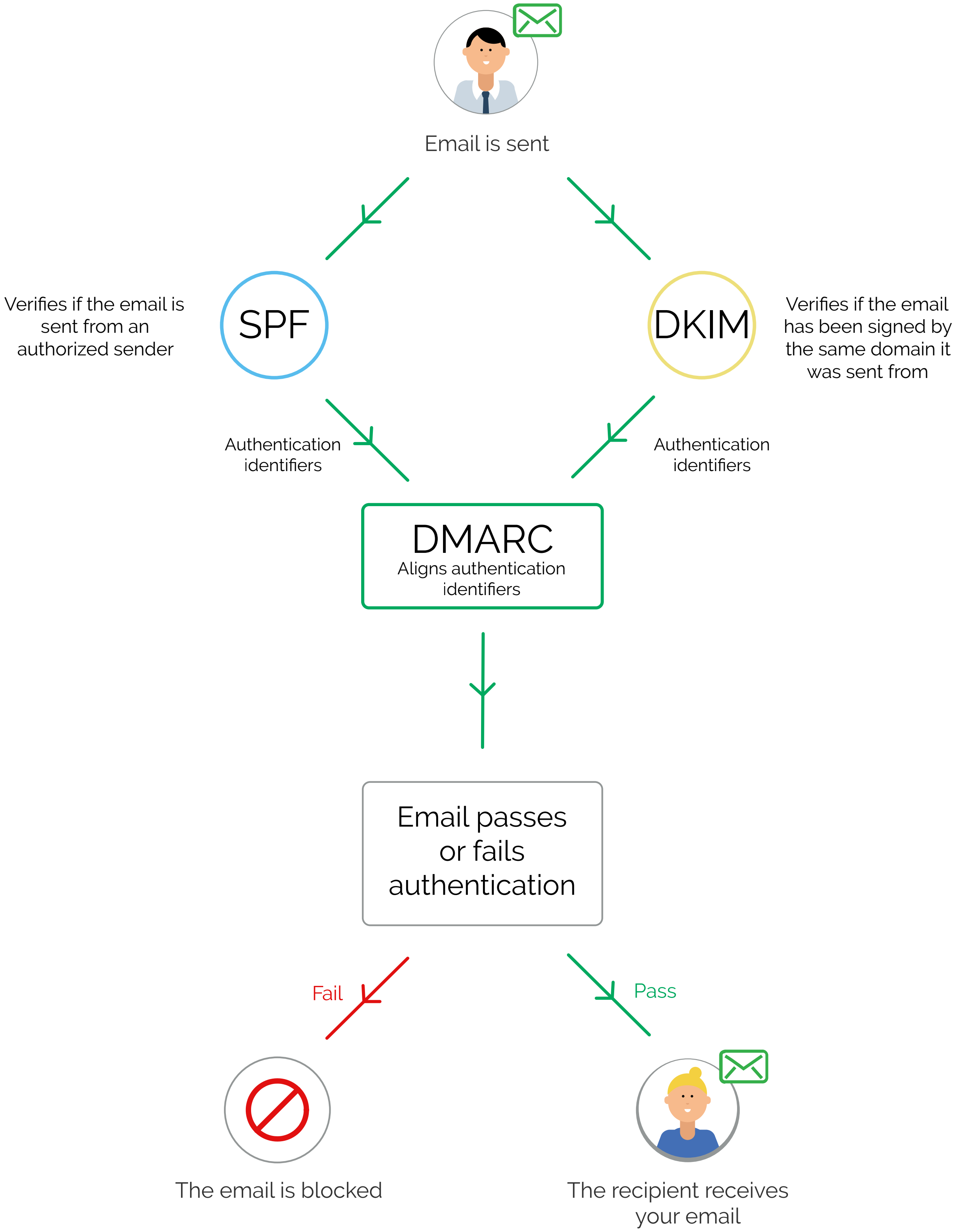
This protocol verifies that the received emails have been digitally signed by the domain they were sent from or on behalf of.

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. This authentication of an email's origin with DMARC also greatly improves deliverability.

How DMARC works



Email is sent

Verifies if the email is sent from an authorized sender

SPF

DKIM

Verifies if the email has been signed by the same domain it was sent from

Authentication identifiers

Authentication identifiers

DMARC

Aligns authentication identifiers

Email passes or fails authentication

Fail

Pass

The email is blocked

The recipient receives your email

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

The delivery of emails is handled by DMARC through 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 domain owner to help identify the email sources with appropriate authentication, and those without (these are unauthorized).

Which organizations are already using DMARC?

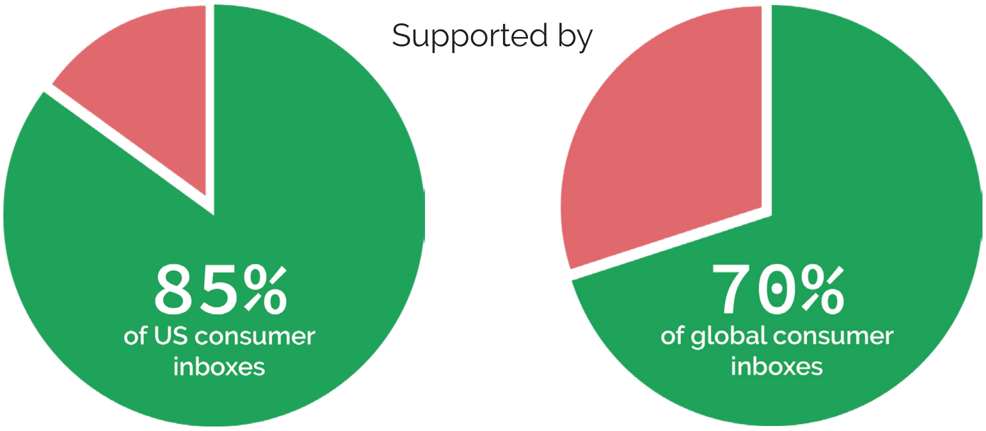
Senders
DMARC has already been implemented by a number of large brands and organizations, most of which are already in protection mode, including:

- 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] They also published the Minimum Cyber Standard Framework, defining the minimum security measures that Departments shall implement with regards to protecting their information, technology and digital services.

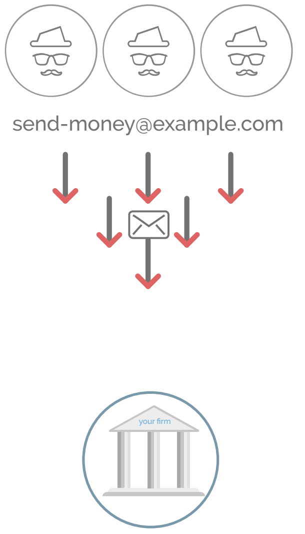
Making the case for DMARC

You can check your organization's current DMARC set-up at ***www.ondmarc.com*** using the free domain checker tool, 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

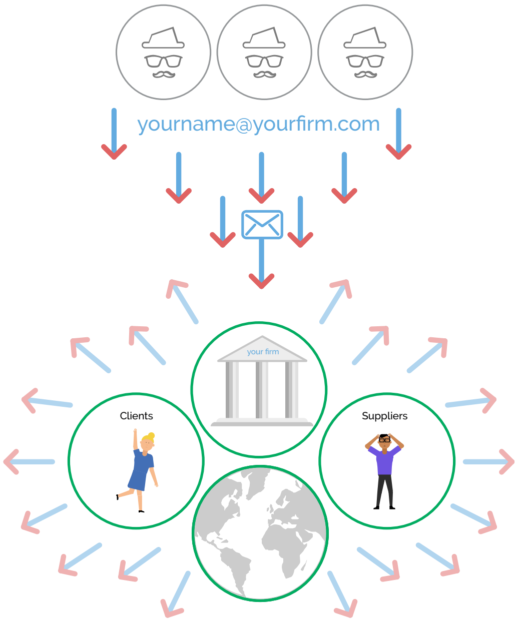
DMARC provides reports to users showing most, if not all, emails that come from a user's domain, not just those that cross the organization's network boundary. This contrasts with traditional cybersecurity solutions, such as MessageLabs and Mimecast, which only pick up phishing emails that cross the 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 globally

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 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."*** 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.

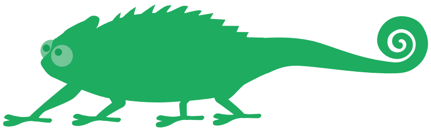
- **I'm concerned that implementing DMARC is going to affect our current email deliverability.**

  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.



What you should look for in your DMARC provider?

Supplier checklist

- **What are their security accreditations?** It is important to check if the DMARC provider has the appropriate security accreditations. Check if they are ISO27001 certified or have Cyber Essentials.

- **Are they using the p=reject policy themselves?** In order to trust that a provider can implement DMARC effectively within your organization, you should check if they have been able to properly implement DMARC themselves. You can easily check using free online tools.

- **What do existing customers think?** If possible, try to speak to one of their current customers to get an insight on the provider's product and services.

- **What does their roadmap look like?** You might be buying the product for what it currently offers today, but also consider what other innovations are being developed that may be of interest in the future.

- **How are their support services?** Without in-house IT systems expertise, DMARC may appear to be complex to implement in smaller organizations or to deploy across larger organizations. A provider's support services may therefore be integral to fast and effective implementation of DMARC. Support teams will also be invaluable to ongoing implementation and refinement of DMARC over time.

Product Checklist

What you should look for in your DMARC solution

The basics

- **Reporting and dashboards:** You need to be able to see all the email validations taking place within your domain. The best tools will simplify the complex DMARC XML reports so that you can quickly get an overview of the DMARC compliance of your emails. Simple dashboards will enable you to easily identify any misconfigurations, as well as to see the scale and frequency of spoofing attacks. For those looking for an in-depth understanding of their phishing attacks, forensic reports provide greater insight into how an organization's domain is being exploited.

- **Configuration:** Once you have used DMARC to understand the security of your domain, you can put in place a solution which will enable you to configure your SPF and DKIM policies to ensure that your organization's identity can only be used by legitimate users. A clearly structured solution is important for organizations which do not have specialist in-house DMARC expertise and/or limited resources. The solution should help you to confidently move you through the various stages of DMARC implementation until the organization reaches the p=reject policy.

- **Ongoing protection:** As your organization grows and changes you will undoubtedly have to update your DMARC configuration to ensure that your domain continues to be protected and that deliverability is unaffected. A good DMARC solution will allow you to easily update and maintain your SPF and DKIM configurations, as well as provide clear alerts when one of these 'breaks'. A solution like ***OnDMARC*** will highlight any changes that need your attention and provide clear instructions on how to resolve it quickly.

Helpful extras available from some providers

- **Dynamic SPF:** The SPF protocol is limited to 10 DNS lookups. This is often an issue for organizations with a complex email infrastructure or those that use a number of cloud services, since they will quickly reach this limit. Once this limit has been reached, legitimate emails may fail SPF authentication. The Dynamic SPF feature, which is available from ***OnDMARC***, overcomes this problem by allowing an organization to use only 1 SPF lookup to connect to OnDMARC's system, from where it will have unlimited lookups.

- **API Access:** The ability to seamlessly integrate the data from your DMARC solution into your existing security dashboards is a useful way to create a one-stop-shop for all email security analysis.

- **Single-Sign-On (SSO):** Some providers, including ***OnDMARC***, enable an organization to integrate DMARC with other key IT systems, such as Okta, so that it can be accessed with a single sign-on to an organization's security setup.

- **ChatBot:** A chatbot can deliver real value by allowing an organization to receive and action DMARC alerts directly in Slack. This means you do not need to check your DMARC application regularly.

- **DMARC Checkup:** Typically when you make a DNS change, you have to wait for the first aggregate reports to arrive in order to see the impact of the change, this can take up to 24 hours. With ***OnDMARC*** the inspection tool 'Investigate' enables you to immediately check the results of changes to the configuration of 5 essential signals: DMARC, SPF, DKIM, FCrDNS and TLS in human readable dashboards.

- **Forensics:** Forensic reports for emails that have failed DMARC validation give you comprehensive and useful insight into the individual emails themselves. Be sure to double check that a provider does this after they've redacted the body of the email.

- **Email security profiles:** Being able to quickly compare your email configuration with an industry standard is a great way to guarantee you can meet the needs of any regulation in place. Providers like ***OnDMARC*** enable you to compare your compliance against the requirements of different security profiles such as the UK Minimum Security Standards or US Binding Operational Directive 18:01.

Implementation services

- **Implementation:** An implementation package can help an organization to put DMARC protection in place more quickly, minimizing its exposure to email impersonation. The services included should enable you to identify valid sources of email within your organization, configure them correctly and then put DMARC into quarantine or reject.

- **Managed Services:** The benefit of having a managed service is that you secure access to a team of experts who are available at all times. These experts can notify you of incident alerts and suggest resolutions, freeing your team up to focus on other tasks.

- **Support:** Customer support is a great way to tackle any ad hoc troubleshooting or get help using the DMARC tool. Some solutions, such as ***OnDMARC*** incorporate chat functions into their DMARC portal, so with a single click of a button you can be connected to an engineer ready to help solve your query.

- Also check to see if your provider's services include a knowledge base, including answers to frequently asked questions and handy hints and tips to enable you to optimize your implementation of DMARC and in-life management.

Time to make DMARC work for your organization

Setting up the basics of DMARC

DMARC does not require installation of any software or special devices - it relies simply on the configuration of three types of DNS records:

SPF Record

This provides a list of IP addresses for the users that are authorized to send emails on behalf of your domain.

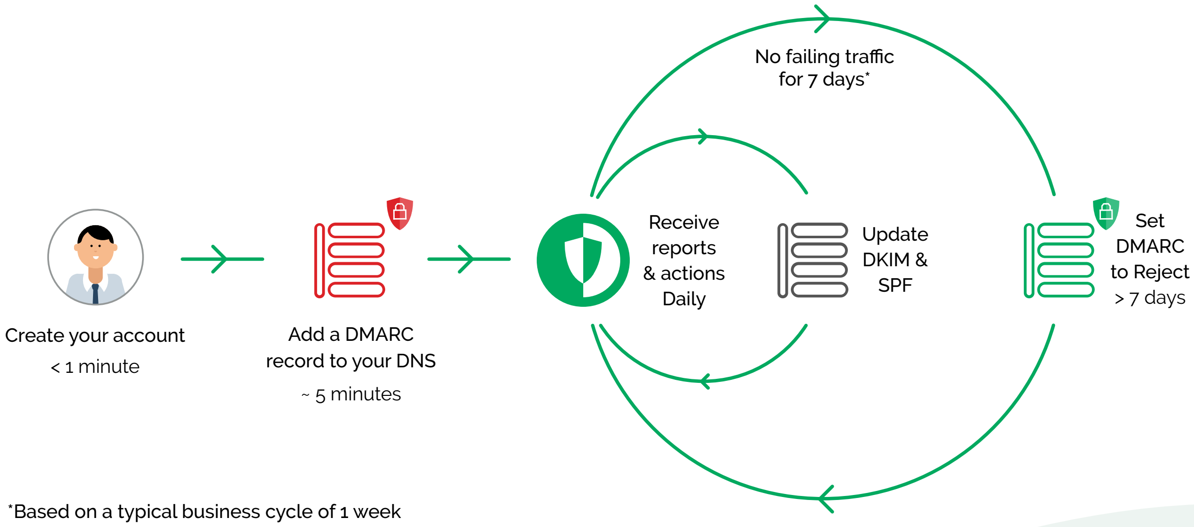
DKIM Records

Services sending emails on your behalf should sign every message using DKIM. The public key for these signatures are hosted as DNS records, against which receiving servers validate emails.

DMARC Record

This declares the policy to be applied when validating emails sent from your domain.

While SPF and DKIM are used by DMARC to enforce a policy the first phase of DMARC implementation is simply reporting. This means you don't need to have SPF and DKIM configured before you set up DMARC, it's afterwards, once you have insight into your domain traffic, that your provider can help set up these protocols.



No failing traffic for 7 days*
Create your account
< 1 minute
Add a DMARC record to your DNS
~ 5 minutes
Receive reports & actions Daily
Update DKIM & SPF
Set DMARC to Reject
> 7 days

*Based on a typical business cycle of 1 week

Who should manage DMARC?

The individual responsible for an organization's email system will be best placed to implement DMARC, as they are likely to have the necessary access to edit the organization's DNS settings.

They will have 3 key tasks:

Gather insight

To avoid any impact on their email traffic, set up DMARC in their DNS in reporting-only mode. Once this DNS record is set up, your DMARC provider will receive reports indicating whether the organization's emails would pass or fail DMARC validation. The provider should analyze these reports for seven days before suggesting next steps.

Determine action

Your provider will offer recommendations on how to set up their SPF and DKIM records to ensure the organization's email traffic is DMARC compliant. They will not be able to implement the highest policy of protection until all of their legitimate email traffic is confirmed as DMARC compliant.

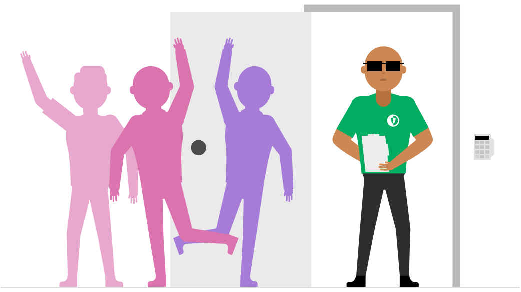
Maintain protection

Once they have received confirmation that all of their legitimate email traffic is DMARC compliant, they can then modify the policy on their DMARC DNS record to instruct receivers of emails from your domain to reject emails that fail DMARC validation. At this point, their domain will be effectively protected from phishing attacks using email impersonation. By implementing DMARC, the organization is confirming to receivers that their emails are authorized and should be directed to the inbox rather than junk or spam folders. Your provider should continue to monitor their email traffic.

What's next?

As with any software or hardware, DMARC requires regular maintenance. Once you have received a series of DMARC reports, you may wish to refine the features of the product. Your provider should have support engineers who can work with you to undertake the necessary improvements.

Your provider can also advise on the steps to take if your organization reaches the maximum number of DNS lookups provided for by the SPF protocol, for example implementing Dynamic SPF.



Remember, DMARC is only designed to protect against phishing attacks that use your domain to send emails that impersonate someone in your organization. It does not protect against phishing attacks from lookalike domains. For example, if you own "example.com" and implement DMARC on that domain, scammers can still use "examples.com" or "examplesbilling.com" if those domains are not DMARC protected.

It is generally considered a best practice to purchase lookalike domains and park them. Parking a domain involves using DMARC to protect domains that are not used to send emails so that they cannot be used by spammers.

Good luck on your DMARC journey!

We hope that you found this guide a useful way to start building your understanding of DMARC and all its security benefits. We appreciate it's a lot to take in but remember, if you can find yourself a trusted and proven provider you'll have an expert by your side for your whole DMARC journey.

If you have any further questions about how DMARC works or how you can make it work for your organization then get in touch with one of the team at ***contact@redsift.com*** - we'll be happy to help.

Stay secure,

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. http://www.documentwereld.nl/files/2018/Verizon-DBIR_2018-Main_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

Start your DMARC conversation today!

www.ondmarc.redsift.com

Member CyberExchange

Member of Microsoft Intelligent Security Association Microsoft

UK CLOUD AWARDS 2019 WINNER

2017 Computing Security Awards WINNER Anti Phishing Solution of the Year

bsi. ISO/IEC 27001 Information Security Management IS 672913

GLOBAL CYBER ALLIANCE

ONDMARC

Red Sift is a data-driven cybersecurity company on a mission to democratise the technology vital for organisations of any size or sectors to defend against security threats. With a platform based on machine learning technology, Red Sift offers users a dashboard of tools – from network monitoring to email analysis and authentication – designed to safeguard users and brand reputation.

Founded in 2015 by serial entrepreneurs Rahul Powar and Randal Pinto, Red Sift is headquartered in London, UK, and boasts an impressive client roster including TransferWise, Telefonica, Action for Children, and top UK law firms. Find out how Red Sift is delivering actionable cybersecurity insights to its global customers at www.redsift.com.

🌐 www.ondmarc.redsift.com
✉ contact@redsift.com
🐦 @redsift