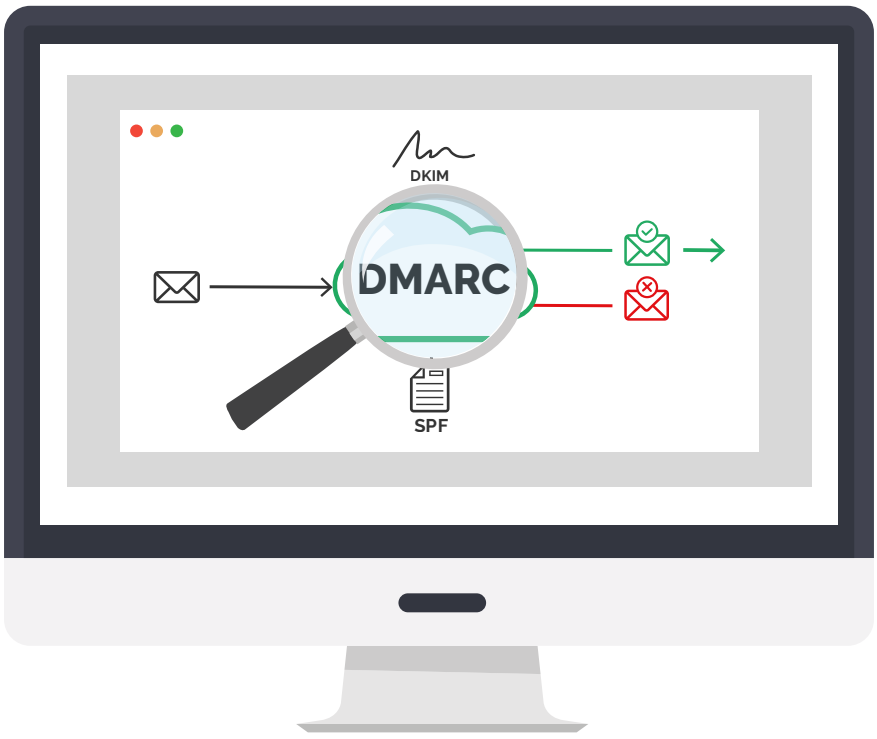
ONDMARC by RED SIFT

A Buyer's Guide to DMARC

Meet the email security 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 emails sent everyday[1]

2018
DMARC adoption rises by 51%[2]

2021
Google announces general availability of BIMI

Email: the easy way in for attackers

According to Verizon's 2021 Data Breach Report[3], email continues to be one of the most common vectors for phishing attacks. So, securing email domains should be a **key concern** for organizations.

Email phishing: an age-old threat

Email phishing is when an attacker or 'bad actor' sends fraudulent emails pretending to be from a reputable organization, with the purpose of getting the recipient to reveal sensitive information like bank details or personal data. Sometimes, phishing emails are sent with the intention of deploying malicious software to the victim's infrastructure.

The UK Government's 2021 Cyber Security Breaches Survey found that **93% of businesses have experienced a phishing attack in the past year[4].**

The rise of social engineering

A traditional phishing attack usually involves one fraudulent email being sent to multiple recipients. However, phishing attacks are becoming increasingly personalized thanks to the rise in Social Engineering, the practice of using psychological tactics to get victims to divulge sensitive information. There's a lot more information readily available online, and attackers can use this to craft more specific and targeted attacks.

These include:

Spear Phishing

A targeted phishing attack, usually aimed at one individual.

Whaling

A targeted phishing attack aimed at a senior individual in an organization.

Battling business email compromise

While some phishing attacks focus on the consumer, bad actors know that there is much more to be gained by targeting an organization. Business Email Compromise (BEC) is an umbrella term used to describe phishing attacks that target an organization by impersonating its domain. The attacker relies heavily on Social Engineering, and crafts a phishing email designed to look like one from someone inside the business (usually the CEO). The main aim of this type of attack is to steal money or sensitive data. Most often, the attack impersonates the exact domain of the business they're attacking, so attacks can be very hard to spot.

The types of attack that come under the umbrella term **Business Email Compromise** include:

Ransomware

When the attacker uses encryption to delete a sensitive data ransom, threatening to release it unless the price is paid.

CEO Fraud

When the attacker poses as the CEO or another senior executive and targets employees.

Invoice or Vendor Fraud

When the attacker tries to trick the recipient into paying an invoice or multiple invoices.

Data Theft

An attack targeting those with access to Personally Identifiable Information (PII), such as HR managers.

Account Compromise

When the attacker hacks a victim's account to send invoices.

More than 45% of email traffic is spam, and this is regularly used as a vehicle for malware by attackers[5].

Email security isn't as secure as you thought

Email security technologies come in many forms. But ultimately, all have a common set of goals: keeping the volume of spam emails down, detecting threats, and stopping them from reaching your (the user's) inbox.

More often than not, these technologies work by looking for the most common traits of a malicious email - like a blacklisted IP address or a suspicious domain - and then blocking it from reaching your inbox.

Exact domain impersonation (otherwise known as email spoofing) is when an attacker **uses your domain to send a fraudulent email**.

All email security measures (apart from DMARC) are ineffective at spotting a malicious email when it appears to come from a legitimate domain.

This is because of a flaw in Simple Mail Transfer Protocol (SMTP), the internet standard for transmission of electronic messaging. When it was designed, it overlooked this security issue, meaning it's easy for attackers to impersonate a domain, and so standards for sending email today have been left open to attacks resulting in data and financial theft.

Can anyone pretend to be you?

Anyone with a very basic knowledge of coding can learn the 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 doesn't have the typical indicators of a phishing attack, such as a suspicious email address. A recipient email server will then allow this email into the user's inbox (if the right security measures are not in place). It's then hard for the user to see that the email is in fact a phishing attack using a spoofed domain.

Phishing attacks have varying levels of sophistication

1 Clearly suspicious
examplebrand@yourbank123.com

2 Could pass as genuine
customercare@examp1ebrand.com

3 Impersonated (spoofed)
info@examplebrand.com

Email Impersonation vs Exact Domain Impersonation. What's the difference?

Email impersonation is an encompassing term which describes an attacker using your domain, or one which looks very similar, to send phishing emails. Exact domain impersonation is when the attacker spoofs your exact domain only.

It's not surprising that many users are deceived by phishing emails. When done well, they can be almost impossible to spot. Organizations that experience phishing attacks haven't necessarily done anything wrong, and the attacker doesn't even need access to their systems to carry one out. But regardless, many governments and regulators consider organizations to have a responsibility to safeguard their customers against phishing attacks. So organizations that haven't taken appropriate measures to safeguard their customers may be liable for a data breach - and penalties.

Potential spoofing scenarios

A phishing email usually contains instructions like these:

Internal - to your staff	*External - to your customers*	*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...	Ransomware or DOS attack

Exact domain 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 try and improve email security, but email impersonation bypasses many of these.

Time to meet DMARC

What is DMARC?

In 2012, several of the major global email providers came together in an attempt to put an end to phishing, in particular attacks carried out using exact domain impersonation.

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

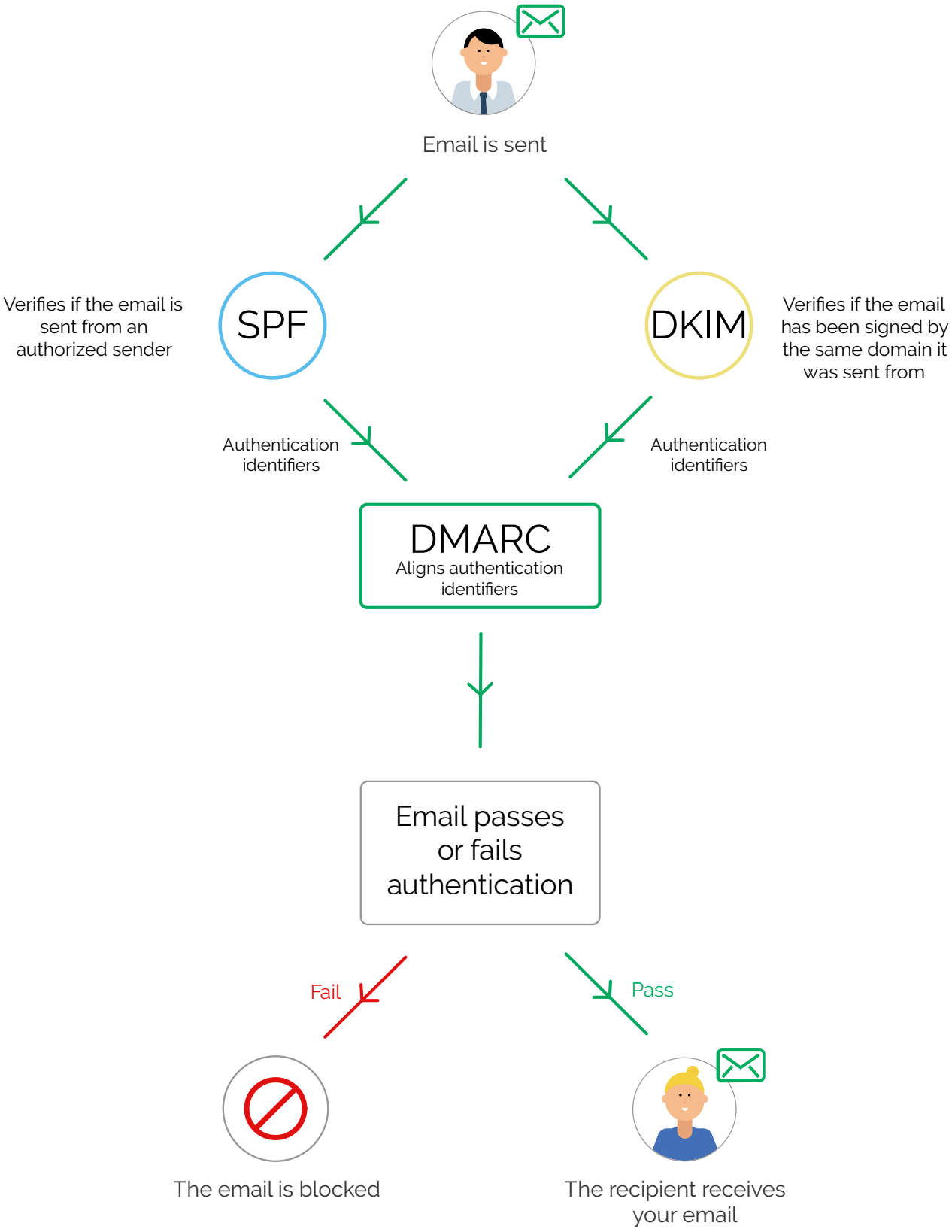
This protocol verifies that the received emails have been digitally signed by the domain they were sent from or on behalf of.

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 spoofed.

DMARC

In 2012, **Domain-based Message Authentication, Reporting, and 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



How each DMARC policy works

Your DMARC policy is essentially the instruction you give to receiving servers, telling them what to do with emails that come from your domain. There are three DMARC policies to choose from:

None policy

p=none

This policy tells the recipient server to accept all emails from your organization's domain, regardless of whether they pass authentication or not.

Quarantine policy

p=quarantine

This policy tells the recipient server to send any emails from your organization's domain that fail authentication to spam.

Reject policy

p=reject

This policy tells the recipient server to reject any emails coming from your organization's domain that fail authentication.

DMARC reporting

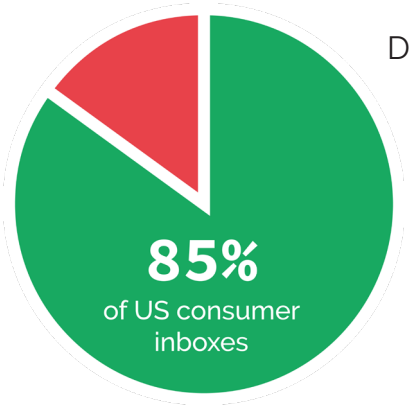
Regardless of which policy the domain is set to, reports will be sent to your organization's domain owner to help identify the email sources using your domain and where emails are being sent from.

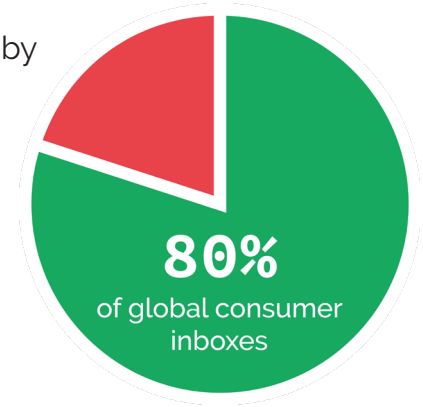
Who is DMARC supported by?

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 US consumer inboxes and approximately 80% of consumer inboxes worldwide from phishing emails, provided that the organization being impersonated in a phishing email has a published DMARC record.

It's important to note that an organization that 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.

DMARC is supported by





DMARC up until now:

- **2015**: Gartner includes DMARC as a qualifying feature for its Magic Quadrant for Secure Email Gateways 'leader' position.
- **2016**: UK Government mandates DMARC as a must-have for all gov.uk domains by March 2019.
- **2017**: US Government mandates DMARC for its Department of Homeland Security domains.
- **2018**: NCSC (Part of GCHQ) issues guidance to make DMARC a top 5 priority for business boards, and includes it in their Minimum Cyber Standard Framework[6].
- **2019**: ARC Protocol published as RFC 8617, to solve issues with forwarded and altered emails failing DMARC authentication checks.
- **2020**: DMARC policies increase by 43% to a total of 2.7million[7].
- **2021**: Google announces its support for BIMI, the new standard which enables registered logos to appear in the avatar slot of DMARC authenticated emails.

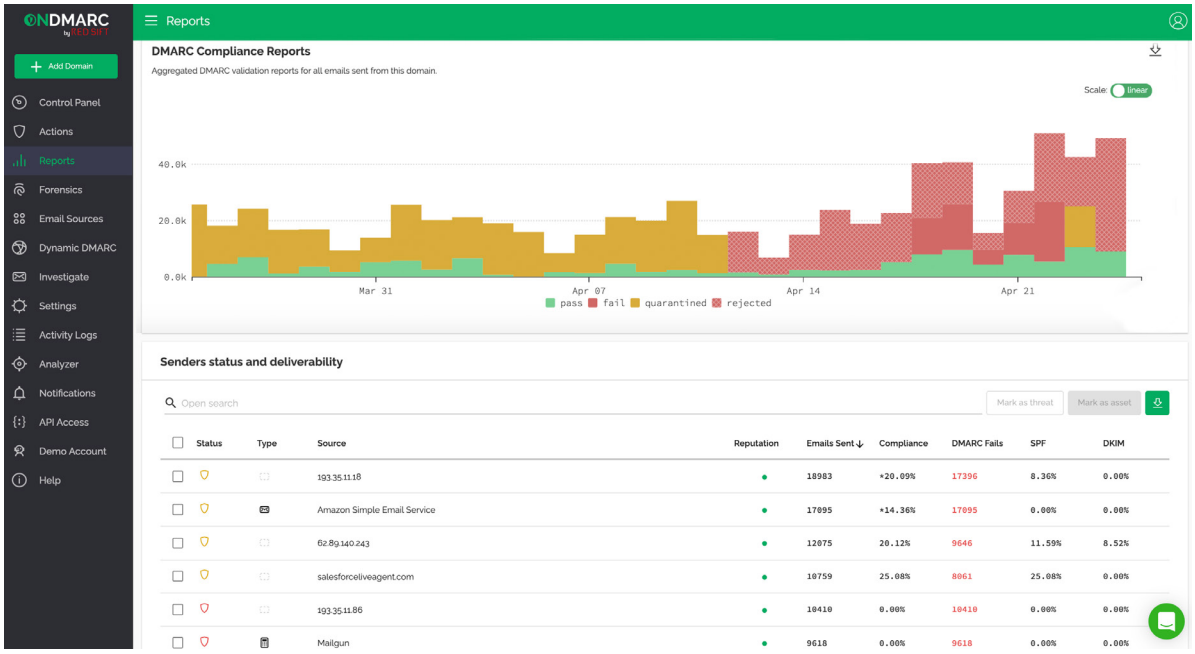
Why implement DMARC?

Check your organization's current DMARC setup using our free domain checker tool.

Find out more

Enjoy complete visibility

DMARC provides reports showing most, if not all, emails that come from your organization'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 not getting a complete picture of the number and scale of attacks against them.



Protect your reputation

Phishing attacks that use exact impersonation can cause considersable reputational damage. Phishing scams attract negative press, with liability often attributed to the organization that has been impersonated.

Ensure financial security

Paying fake invoices or completing wire transfers from emails impersonating a business' CEO are common. In fact, the financial cost of spoofing attacks has consistently increased, according to The UK Government's 2021 Cybersecurity Breaches Survey[8].

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.

Get your registered logo on your emails

BIMI (Brand Indicators for Message Identification) is a standard that enables your registered logo to be visible in the avatar slot of any DMARC authenticated emails you send, by using Verified Mark Certificates. BIMI increases your brand impressions, and research has found it has a significant positive impact on consumer trust, interaction, and purchasing decisions. Being DMARC compliant means you're eligible to take advantage of this brand-enhancing reward.

Improve email deliverability

Email providers, such as Gmail, Yahoo and Hotmail, are becoming more protective of their users' inboxes. An email provider may refuse to deliver an email to a user's inbox if it does not have an SPF and/or DKIM signature. With DMARC, emails are reliably authenticated, improving deliverability of legitimate emails to the 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 supposedly come from these organizations and could be deterred from using email to communicate with them, which can impact on those organizations' ability to communicate effectively with their customers. By implementing DMARC, you're putting a robust measure which confirms your organization's identity in place

Identify and remove shadow IT

Shadow IT refers to legacy systems or technology set up by various departments in a business to plugs a gap in existing infrastucture, and it's not always easy to identify or remove. DMARC gives you the visibility necessary to identify and resolve any outlying software or systems, meaning nothing will accidentally be sent out by these legacy systems. Implementing DMARC uncovers all the email services sending email from your domain, whether you officially know about them or not.

The cost 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**.

What to look for in a DMARC provider

Checklist:

- **Relevant security accreditations:** It's important to check if the DMARC provider has the appropriate security accreditations. Check if they are ISO27001 certified or have Cyber Essentials.

- **DMARC in p=reject themselves:** In order to trust that a provider can implement DMARC effectively within your organization, you should check if they have properly implemented DMARC themselves. You can easily check using free online tools.

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

- **Continuous product improvement:** 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.

- **Comprehensive customer support:** Without in-house IT systems expertise, DMARC will be complex to implement in smaller organizations and difficult to deploy across larger ones. So, your provider's support services will likely be integral to your fast and effective implementation of DMARC. Support will also be invaluable to ongoing implementation and refinement of your DMARC policy over time.

What to look for in a DMARC product

Essential features:

- **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 allow you to easily identify any misconfigurations and see the scale and frequency of spoofing attacks. For a more in-depth view, forensic reports provide detailed insight into how your organization's domain is being exploited.

- **SPF and DKIM Configuration:** Once you've used reports to understand the current security of your domain, you should start to configure your SPF and DKIM policies to ensure that your organization's identity can only be used by legitimate users. A clearly structured process for this is important for organizations that don't have specialist in-house DMARC expertise or vast resources. The process should help you to confidently move you through the various stages of DMARC implementation until your organization reaches the p=reject policy.

- **Ongoing protection and support:** 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 product will allow you to easily update and maintain your SPF and DKIM configurations, as well as provide clear alerts if or when one of these breaks. **ONDMARC** highlights any changes that need your attention and gives you clear instructions on how to resolve these quickly.

Additional features:

Included with ONDMARC

Brand Indicators for Message Identification (BIMI): This is a standard that enables the use of registered logos in the avatar slots of DMARC authenticated emails. This means your logo appears on every DMARC authenticated email you send, and you can stand out in the inbox while increasing brand impressions. It's not a security standard, but instead a reward for implementing DMARC that has some sizeable benefits for consumer interaction with your emails too. Partnered with Entrust, OnDMARC is the first and only provider that offers an end-to-end BIMI certification solution. ✓

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. OnDMARC's Dynamic SPF feature overcomes this problem, by allowing an organization to use just 1 SPF lookup to connect to OnDMARC's system, from where it has unlimited lookups. ✓

Dynamic DMARC: Dynamic DMARC allows you to edit and make changes to your SPF, DKIM, and DMARC records from inside your user interface without having to go into your DNS. It gives users autonomy and flexibility, as usually if you want to make DNS changes, you need to request these from your DNS administrator which takes time. ✓

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.
ONDMARC's Investigate tool allows you to check the results of changes to the configuration of your SPF, DKIM, FCrDNS, and TLS immediately. ✓

Additional features (continued):

Included with ONDMARC

Email security comparison: 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.
With ONDMARC you can compare your compliance against the requirements of different security profiles like the UK Minimum Security Standards and US Binding Operational Directive 18:01. ✓

API Access: Seamless integration of data from your DMARC solution with your existing security dashboards creates a one-stop-shop for all email security analysis. ✓

Single-Sign-On (SSO): This allows your 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 your organization to receive and action DMARC alerts directly in Slack, meaning you don't need to check your DMARC application regularly. ✓

Forensic reporting: Clear 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. ✓

Implementation services

Included with ONDMARC

Implementation: An implementation package can help your organization put DMARC protection in place more quickly, minimizing your exposure to exact domain 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 have 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.

Customer support: This is a great resource to have for tackling any ad hoc troubleshooting or getting help using your DMARC tool.
ONDMARC incorporates chat functions into its DMARC portal, so with a single click of a button you can be connected to an engineer ready to help solve your query.

✓

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

✓

Getting started on your DMARC journey

A quick recap of the DMARC basics:

You don't need to install any software or special devices to make DMARC work. It relies on the successful configuration of three types of DNS records:

SPF Record

This provides a list of IP addresses for the users/services authorized to send emails using your domain.

DKIM Records

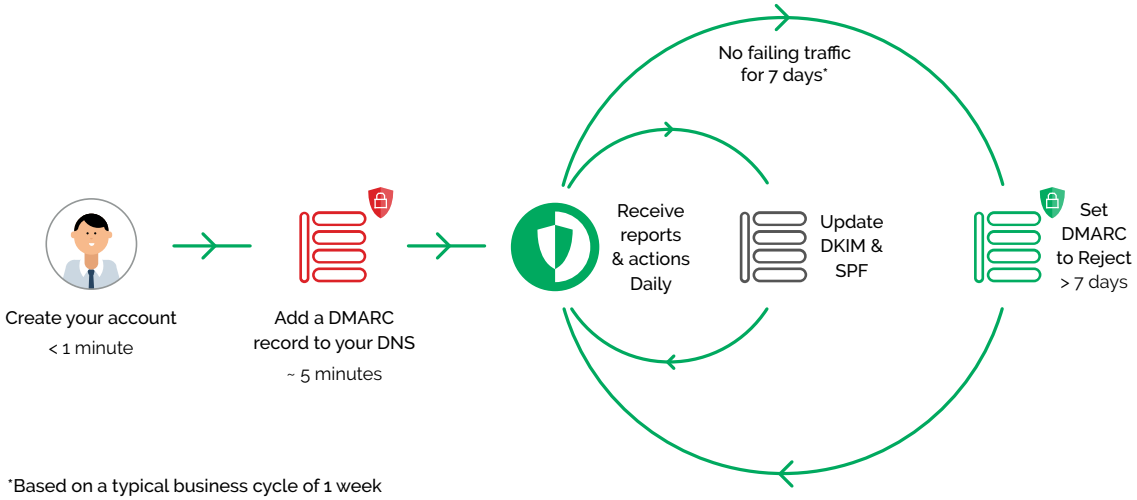
Services sending emails on your behalf should sign every message using DKIM. The public keys for these signatures are hosted as DNS records, against which receiving servers validate emails.

DMARC Record

This declares your DMARC policy (none, quarantine, or reject) and gives the recieving server instructions on what to do with emails coming from your organization's domain.

Start reporting

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.



*Based on a typical business cycle of 1 week

Who in your business should manage DMARC?

The person responsible for your organization's email system is best placed to implement and manage DMARC, as they're likely to have the necessary access to edit your organization's DNS settings.

There are 3 key tasks for successful DMARC set up and management:

1. Gather insight

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

2. Determine action

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

3. Maintain protection

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

Answering common questions

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

  DMARC is fundamental to cybersecurity. The UK's National Cyber Security Centre has declared that, "Widespread adoption of the DMARC protocol is essential to defend against targeted cyber threats[9]." An organization which spends money on sophisticated and expensive security measures but fails to deploy DMARC is like 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 complex, lengthy, and require staff resourcing to interpret the data and make adjustments accordingly. DMARC providers, like **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 really complex to deploy, is there a way to make it easier?**

  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 significantly simplify this process and help you to reach full protection mode.

- **Will implementing DMARC affect our current email deliverability?**

  DMARC will improve your email deliverability significantly, providing that it is correctly configured. If implemented incorrectly, then your deliverability could suffer. A reliable and easy-to-use DMARC tool like **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 than without it.

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

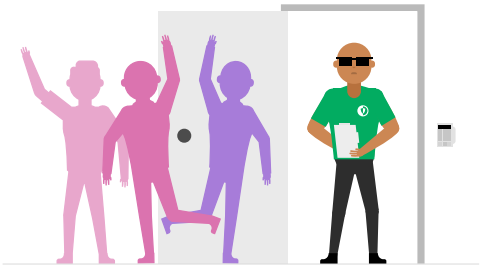
  Most of the email security solutions currently available do not give organizations total protection against exact domain impersonation. This is because they focus on preventing security breaches which result in spam emails being sent from within an organization's network boundary. They do not prevent 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 cost of data theft and loss of services continue to escalate. Simple measures such as DMARC could save single organizations thousands, if not millions, of dollars.

What's next?

As with any software or hardware, DMARC requires regular maintenance. Once you've received a series of DMARC reports, you may want 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 organization's exact domain to send emails, impersonating 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 these domains are not DMARC protected.

To combat this, it's generally considered 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 attackers.

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 DMARC provider, you'll have an expert by your side for your whole DMARC journey, making it easier, quicker and painless.

If you have any further questions about how DMARC works or how to get started with implementing it 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 by RED SIFT

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://www.verizon.com/business/en-gb/resources/reports/dbir/
4. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021
5. https://www.statista.com/statistics/420391/spam-email-traffic-share
6. https://www.gov.uk/government/publications/the-minimum-cyber-security-standard
7. https://dmarc.org/2021/02/dmarc-policies-increase-43-over-2020/
8. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021
9. https://www.ncsc.gov.uk/
https://dmarc.org/
https://www.globalcyberalliance.org/

Start your DMARC journey today!

www.ondmarc.redsift.com

Member of Microsoft Intelligent Security Association

Microsoft

Global Infosec Awards Winner Cyber Defense Magazine 2021

2020 Fortress Cyber Security Award

British Legal Technology Awards 2020 Winner for 'IT Security Provider of the Year'

bsi. ISO/IEC 27001 Information Security Management IS 672913

Global Cyber Alliance

ONDMARC by RED SIFT

Founded in 2015, Red Sift is a global cybersecurity company whose clients include organizations such as Wise, Telefonica, Pipedrive, ITV, and top global law firms.

The Red Sift Open Cloud is a data analysis platform that is purpose-built for the challenges of cybersecurity. Products on the Red Sift platform include OnDMARC, OnINBOX, and OnDOMAIN, SaaS applications that work together to close the net on the phishing problem by blocking outbound phishing attacks, analyzing the security of inbound communications, and providing domain impersonation defense.

www.ondmarc.redsift.com

contact@redsift.com

@redsift

v3.3 | Sep 21