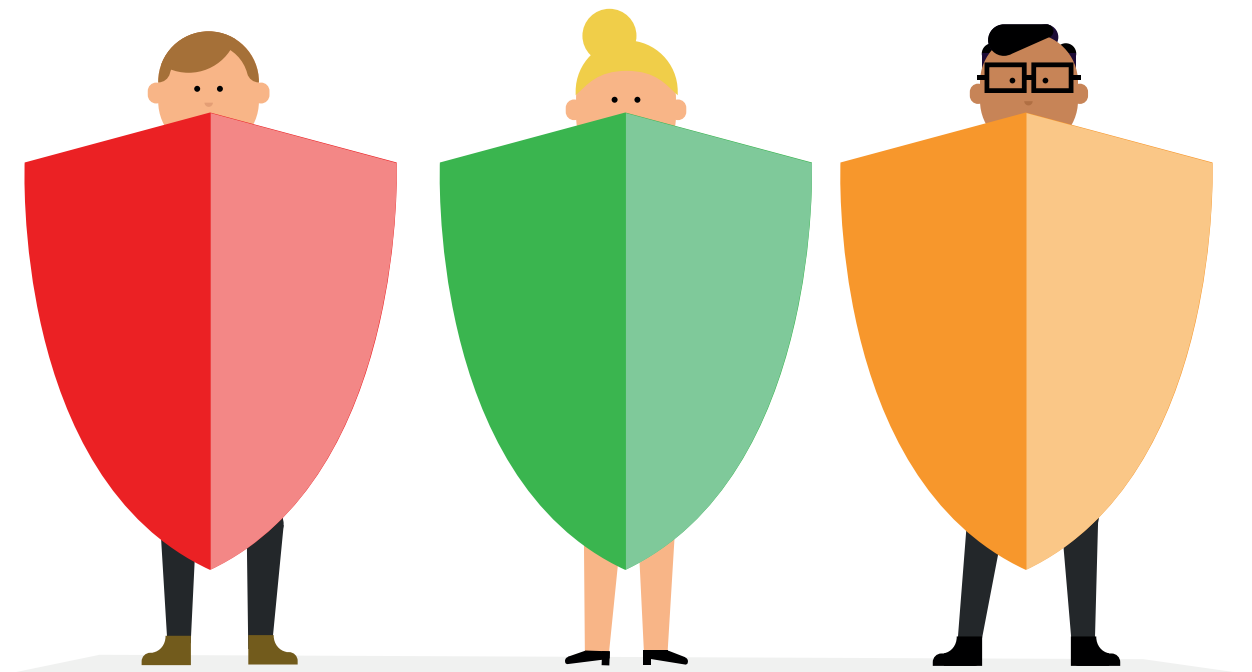


A Buyer's Guide to DMARC

Meet the cyber security protocol that reduces phishing attacks and improves email deliverability



1971

First email sent

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

2015

DMARC was ratified

2017

269 billion
emails sent everyday¹

Email: The easy way in?

According to a recent report published by LinkedIn, phishing is the **top cyber security concern** for organizations².

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 scams³)

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, and then tailor the email content accordingly.

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.

Not all email security measures are created equal



Cloud



Server



Hardware

Whilst email security measures come in many forms, all are intended to keep the volume of spam emails to a minimum, detect unwanted content (from malware to suspicious links) and prevent it reaching the user's mailbox.

But what if the email comes from a legitimate domain?

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



There is a fundamental flaw in the global email infrastructure which exposes every organization to financial and data theft.

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, making it difficult for the user to identify whether the email is a phishing attack.

Email impersonation bypasses the following security measures:



Strong Passwords



Biometrics



Two-factor Authentication



Dongle

Potential spoof scenario

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 the contract?	I need to confirm your personal details	Data loss
See the attached HR	Follow this link to reset your password...	Cyber attack

Sophistication levels of phishing attacks

1 Obviously suspicious
hsbc@yourbank.com

2 Harder to spot
customercare@hsbo.com

3 Looks genuine
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 have accessed their systems, 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.

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.

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

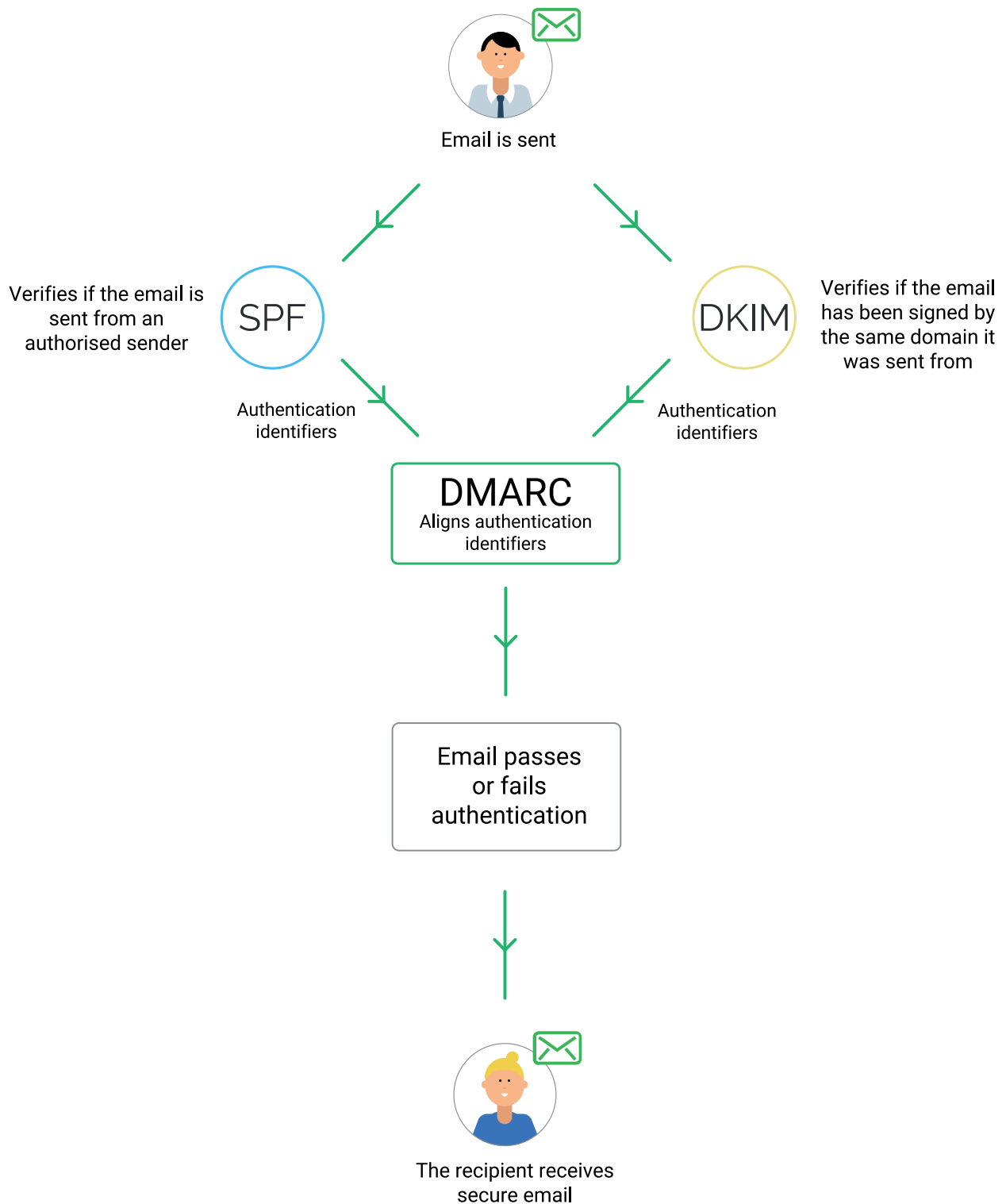
This protocol verifies emails which have been signed by the domain they were sent from or on behalf of (by using encryption in the header of an email).

While these protocols had been accepted by the major global email providers, a secondary layer was required to block the phishing emails which were being identified by the protocols.

DMARC




In 2015, the ***Domain-based Messaging, Authentication and Reporting Conformance*** (DMARC) was ratified to report on these individual protocols, accurately validate emails and block phishing attacks.

How DMARC works



Enforcement through an authentication policy

The delivery of emails is handled by DMARC by reference to one of the following three policies, which can be set by the user:
















-  **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 the policy that a user sets, reports will be sent identifying emails which have appropriate authentication, as well as those which are unauthorized.

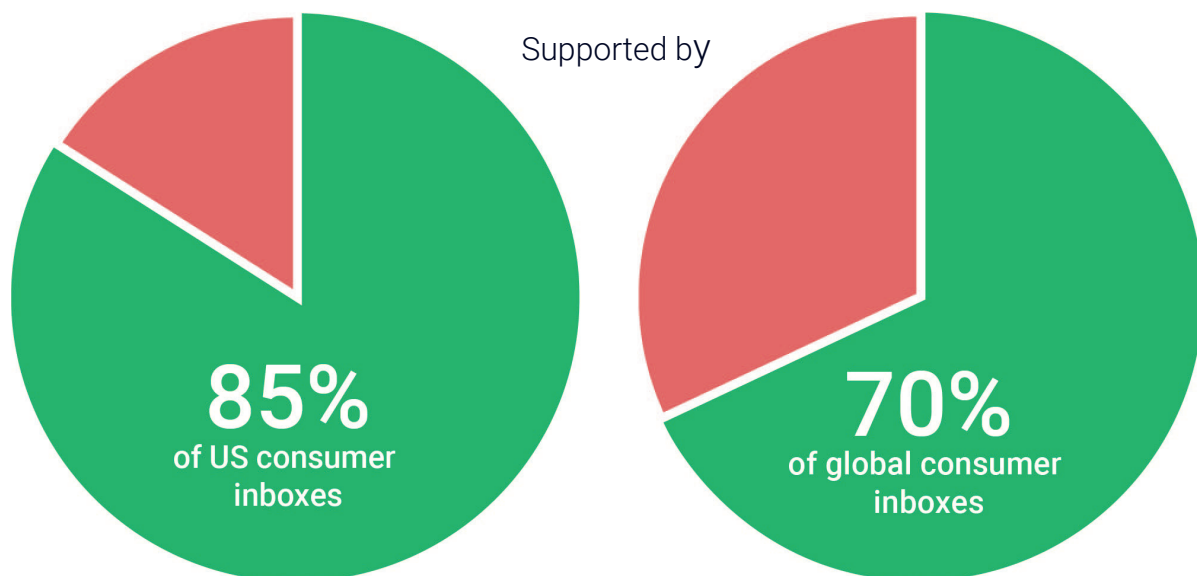
Which organizations are already using DMARC?

Senders

DMARC has already been implemented in “p=quarantine/reject” by a number of large brands and organizations, including:

 Adobe	 Facebook	 Pinterest
 Amazon	 Google	 Twitter
 AOL	 Instagram	 Verizon
 CNN	 Microsoft	 Yahoo
 Dropbox	 PayPal	 YouTube

Enforcement through an authentication policy



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

It is 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 adopted DMARC.

2015

Gartner included the provision of DMARC as a qualifying feature for its **Magic Quadrant for Secure Email Gateways** 'leader' position.

2016

The UK Government mandated DMARC for its ".gov.uk" domains.

2017

The Department of Homeland Security mandated DMARC for federal government agencies.

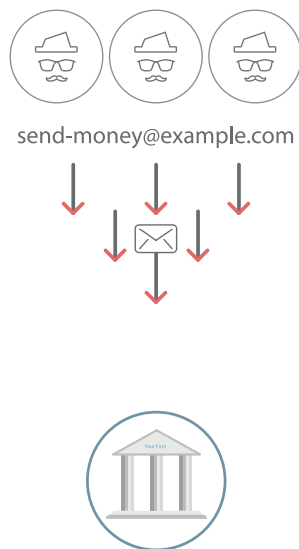
Making the case for DMARC

You can check your organization's current DMARC set up at www.ondmarc.com, which will provide clear information on the status of DMARC, SPF and DKIM. The site will also indicate whether your inbox and DNS are compatible.

Complete visibility

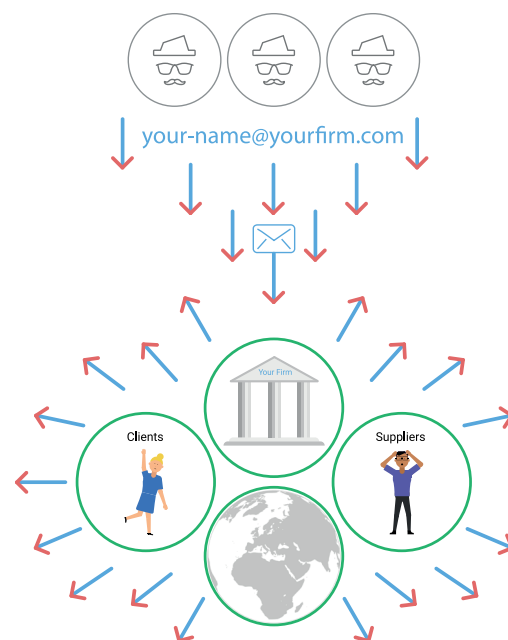
DMARC provides users with reports showing most, if not all emails that purport to come from a user's domain rather than just those which cross the organization's network boundary. This contrasts with traditional cyber security gateway appliances which only pick up phishing emails that cross the network 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.

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 an SPF and/or DKIM signature, or if the user has previously marked the sender's emails as "junk".

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



No DMARC



DMARC none



DMARC quarantine



DMARC reject

Protect reputation

Organizations that are subject to regular email spoofing suffer considerable reputational damage. Phishing scams often attract negative press, with liability often attributed to the organization which has been impersonated.

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; this can affect the ability of the organization to communicate effectively with its customers.

Ensure financial security

Finally, and perhaps most critically, serious financial penalties may be incurred as a result of email spoofing. Put forward earlier this year, the UK Government's GDPR proposal to impose fines on organizations with inadequate cyber security measures has gathered much debate.

Whilst the costs of data theft as a result of spam emails continues to escalate, 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 cyber security. 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 that spends money on complex 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 an open standard protocol?**

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. 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 cyber security 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.**

Provided that it is correctly configured, DMARC will improve your email deliverability significantly. A DMARC expert 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.

Whilst the costs of data theft as a result of spam emails continues to escalate, adopting DMARC could save an organization 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.



What support can they provide you?

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.

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, ensuring 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 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 continued protection of your domain and that deliverability remains unaffected. A good DMARC solution will allow you to easily update and maintain your SPF and DKIM configurations.

The basics

Dynamic SPF

This is often an issue for organizations with a complex email infrastructure or those that use a number of cloud services as they will quickly reach this limit. 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 here 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

Some providers, including **OnDMARC**, enable an organization to integrate DMARC with other key IT systems such as Okta. This ensures 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.



Implementation services

Implementation

An implementation package can help an organization to put DMARC protection in place more quickly, minimizing its exposure to email impersonation. 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.

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

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



ChatBot

 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.

Making DMARC work for your organization

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.

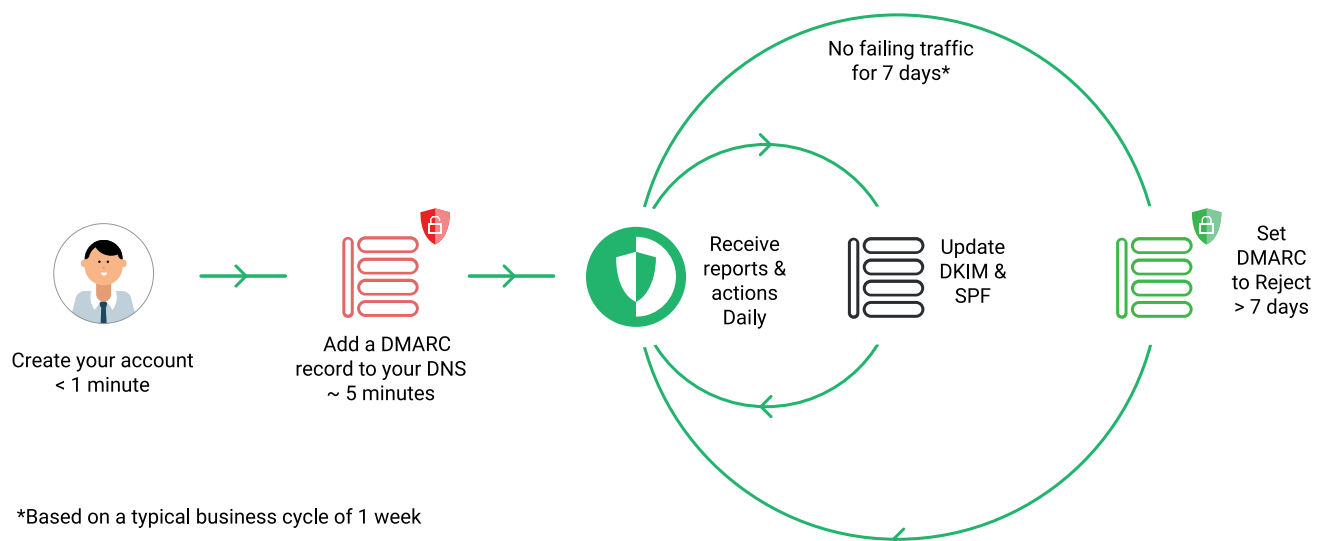
DKIM records

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.



Setting up DMARC

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



Insight

To avoid any impact on your email traffic, set up DMARC in your DNS in reporting-only mode. Once this DNS record is set up, your 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 the next steps.



Action

Your provider will offer recommendations on how to set up your SPF and DKIM records to ensure the 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.



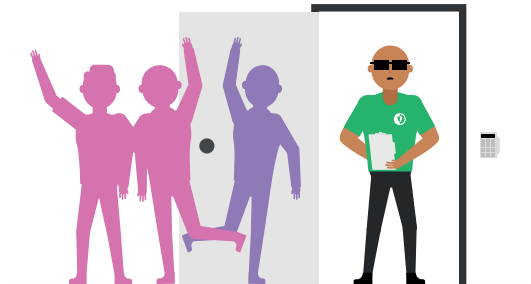
Protection

Once you have 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 email 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 provider should continue to monitor your 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(s) 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 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; this ensures that they cannot be used by spammers.

References

1. <http://www.radicati.com/wp/wp-content/uploads/2017/01/Email-Statistics-Report-2017-2021-Executive-Summary.pdf>
2. <http://www.newsweek.com/origins-nigerias-notorious-419-scams-456701>
3. <https://www.linkedin.com/pulse/top-mind-threats-cisos-2017-chris-mixter/>
4. <https://dmarc.globalcyberalliance.org/>



Start your DMARC conversation today

www.lawyerchecker.co.uk

www.lawyerchecker.co.uk

support@lawyerchecker.co.uk

[@LawyerChecker](https://twitter.com/LawyerChecker)

[linkedin.com/company/lawyer-checker](https://www.linkedin.com/company/lawyer-checker)

A BUYER'S GUIDE TO DMARC - WWW.LAWYERCHECKER.CO.UK