Making DMARC work for your organization

No matter the size of your business or the complexity of your email landscape DMARC should be easy to set up and secure your domain.

Contents

1. 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.

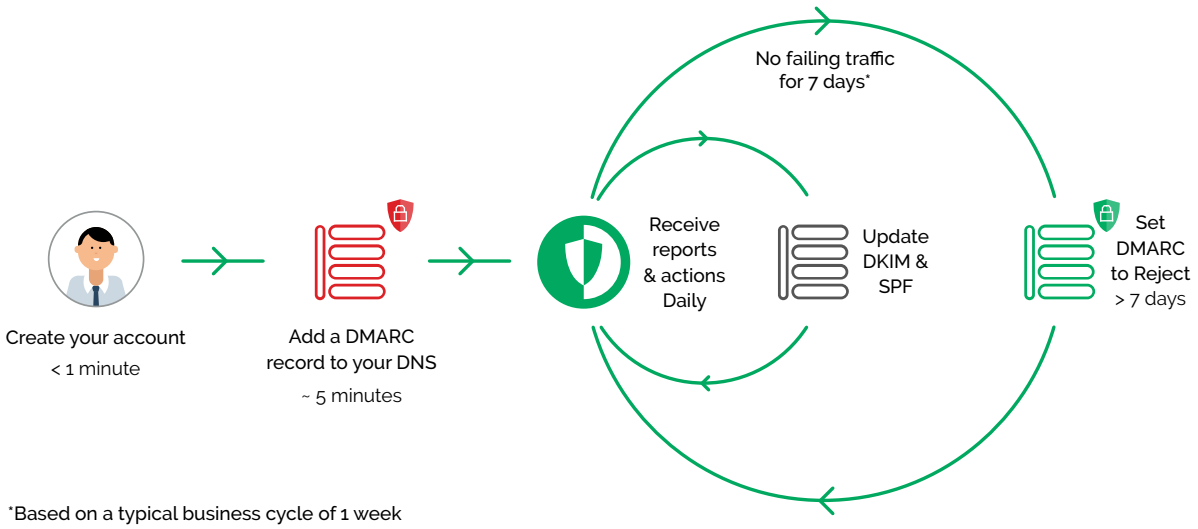
DKIM Records

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.



*Based on a typical business cycle of 1 week

2. 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 your email traffic, 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 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 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.

Maintain 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.

3. What to expect from a useful free trial

Most DMARC providers offer a 'try before you buy' service for a limited time which we hope you will always choose to take full advantage of. However, getting to grips with a brand new dashboard and doing enough to demonstrate success by the end of day 7 or 14 can seem like a bit of a headache if your provider hasn't given you enough guidance.

Your free trial checklist

Stage 1 - Simple set up

- ☐ Friendly onboarding walking you through the key features you need to know about.
- ☐ Were you able to quickly identify how to add your domain and start reporting?
- ☐ Check your emails for a nice welcome and free trial guide to refer back to at any time.

Stage 2 - Full visibility of your email landscape

- ☐ With most providers, your first reports are ready in as little as 24 hours - no time to waste!
- ☐ Are the reports easy to read? Multiple report types with comprehensive visuals should be easy to digest and include Compliance, Locations, Senders, Receivers and Delivery.

Stage 3 - Do you know which actions to take?

- ☐ Once the reports are in, any useful and easy-to-use solution should be immediately highlighting what to do next and where to start with crystal clear Actions listed out.
- ☐ Being confident in taking the right actions comes with the right guidance. Highlighting the issues without step-by-step guides to fix them is a big red flag - look for instructions!

Stage 4 - Confidently demonstrating success

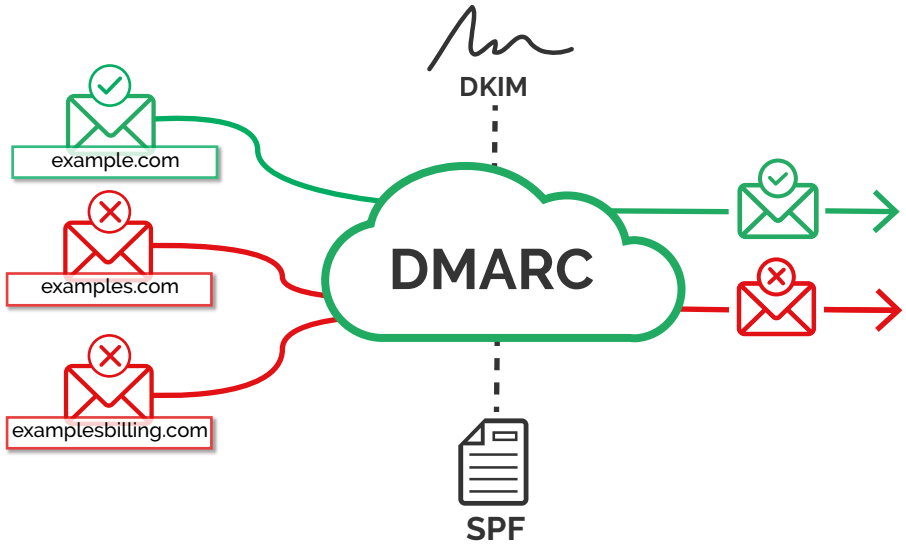
- ☐ From the moment you entered your free trial, the provider should have made helpful resources available to you; access to a Help Center, free trial guide or in-app live chat.
- ☐ It should be swift and easy to take a look at the stats in your account to identify how your first steps to configuration have made a difference to items such as deliverability, authentication and legitimate vs unauthorized senders by email source or location.

4. Handy hints and tips

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.

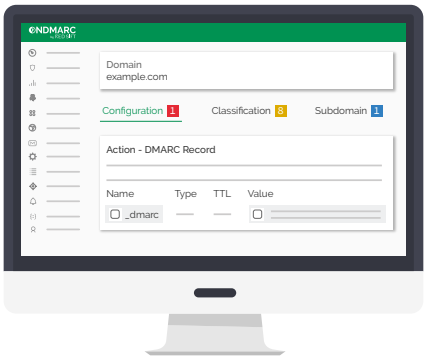
5. Good luck on your DMARC journey!

We hope you found this final part our DMARC Digest useful in understanding how DMARC can work for your organization, in fact, any organization that wants to protect their brand, customers, partners, and other stakeholders by securing their domain from impersonation. In case you missed it, check out Part 1 of this series 'What is DMARC and why should it be your next priority?' and Part 2 'Finding your perfect DMARC provider'.

If you can find yourself a trusted and proven provider you'll have an expert by your side for your whole DMARC journey. To learn more, simply get in touch with one of our team today at contact@redsift.com - we'll be happy to help!

Ready 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

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