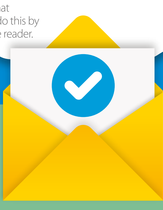
Email security to protect your brand and business

DMARC Demystified

Spoof emails can be difficult to spot.

They look real, because they appear to use a genuine email address, and are used to instigate phishing attacks, distribute malware or obtain access to confidential or sensitive data – risking business continuity, profitability, and brand reputation.

Without DMARC, spoofers can send emails that appear to originate from your domain. They do this by falsifying the 'from' address that's visible to the reader.



What is DMARC?

DMARC is the email protocol that verifies the authenticity of messages sent by your company's authorized servers, helping to prevent unauthorized senders from impersonating your email domains. This also improves delivery rates for your genuine emails, reducing their chances of being marked as spam. DMARC monitors email traffic and identifies potential spoofing threats, telling you which emails passed or failed the authentication checks, and which IP addresses were used.

DMARC been a requirement for all US federal agencies since 2017, and for UK government since 2016. The Australian government recommends DMARC, and the Dutch government has used DMARC in the Netherlands since 2017.

What to look for in a DMARC solution

1 Anyone can use it

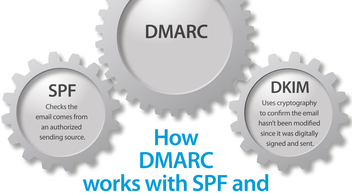
DMARC can be complex to configure and implement. Look for a solution that simplifies the process, does not require a high level of expertise, and that avoids you having to go into individual DNS records and manually edit them.

2 User-friendly Reporting

DMARC reports are in XML format, and finding the data you want takes time. Your DMARC solution should quickly deliver the right information in an easy-to-read format, with recommendations for action.

3 No 10 lookup limit

Standard DMARC is constrained by the SPF limit of 10 lookups. Companies can easily exceed ten authorized domains, as third-party service providers (such as SurveyMonkey, HubSpot or Salesforce) need to be included in the verification process.



How DMARC works with SPF and DKIM to prevent spoofing

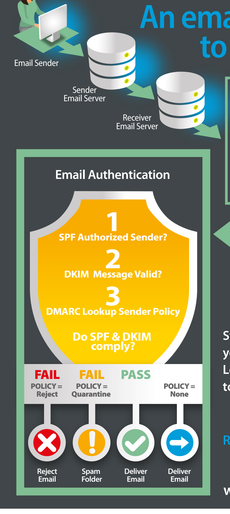
DMARC (domain-based message authentication, reporting and conformance) uses SPF (sender protection framework) and DKIM (DomainKeys Identified Mail) to check the authenticity of an email, and then tells the receiving server what to do if it fails these checks (either or both), based on the policy you set.

DMARC reports on your authorized domains, showing authenticated emails, quarantines and failures.

DMARC authentication increases the chance of email delivery for the domains you authorize.

DMARC applies its policy to all emails associated with your domain (although it won't spot lookalikes or 'close cousins').

An emails journey to your inbox



Stop others impersonating your brand with Libraesva LetsDMARC, the best way to prevent spoofing.

Ready to get started?

www.libraesva.com

/LIBRAESVA

Libraesva is an award-winning email security company, named as Category Leader for 2023 in Email Security by GetApp, a Gartner company. Libraesva is consistently certified by Virus Bulletin as one of the best email security systems, and is trusted by leading brands around the world.

© Copyright Libraesva 2023