For Email Protection and Enhanced Deliverability, EasyDMARC It

What is the risk?

Email remains the primary risk vector for all organizations to become victims of cybercrime, with over **90%** of phishing, spoofing, and ransomware attacks originating from this channel.

A business reputation that has taken years to build can be destroyed in a matter of minutes.

However, simple, cost-effective protection is available with DMARC (Domain-based Message Authentication, Reporting, and Conformance). In short, DMARC is an email protocol that checks whether every email sent from your domain is legitimate.

Driven by the Email Service Providers

DMARC has been available as a form of email protection since 2022, but with a reputation for being complex to implement, even for enterprise-level organizations, uptake was initially slow.

Since then, two changes have occurred: Vendors such as EasyDMARC have developed a platform and supporting services to manage the implementation process for companies of all sizes. Secondly, email service providers such as Google, Yahoo, iCloud, and Microsoft Outlook have begun making DMARC mandatory, first for bulk email senders but increasingly for all email senders.

The result is that without a DMARC record in place on the sender domain, there is a higher chance of email, both **promotional and transactional**, ending up in the targeted recipient's spam folder or being rejected completely.

A Source of Industry Compliance

Increasingly, both the Public and Private sectors are using DMARC as a way of indicating email compliance in broader cybersecurity initiatives.

As an example, within the **Payment Card Industry**, the introduction of **PCI DSS v4.01** has made DMARC a mandatory compliance standard, protecting cardholder data from phishing and spoofing globally.

Within the Enterprise environment, the demonstration of practical steps to secure emails is becoming an auditor prerequisite.

EASYDMARC

What is DMARC?

DMARC works in conjunction with the SPF and DKIM email protocols, verifying their authenticity. If any communication fails either SPF or DKIM checks, then DMARC determines its handling. Setting the DMARC Record at '**None**' enables the monitoring of the email, but it will still be delivered to the recipient. Set at '**Quarantine**', the email will be delivered to their spam folder, and if set at '**Reject**', the email will be returned.

Together With EasyDMARC, We Simplify, Manage, and Automate Your DMARC Journey

Securing Your Domain

Our Services	The Business Benefit
Managed Services	We provide a safe and comprehensive set-up and management of DMARC, SPF and DKIM. From configuration to enforcement, we ensure your email authentication is accurate, secure and aligned with best practices.
DMARC Monitoring and Reporting	We'll show you exactly who's sending emails using your domain and block the unauthorized sources.
Real-Time Threat Alerts	With Instant notifications, we can see if someone tries to impersonate your domain and take immediate action.
Improved Email Deliverability	Legitimate transactional and promotional emails are more likely to reach the intended recipient's inbox rather than the spam folder.
Brand & Reputation Protection	We can ensure that your brand appears alongside your email, building trust and confidence in your brand.

Contact us, and we can begin protecting your domain today.

Contact:
Email:
Website: