mimecast

4 Reasons DMARC Is Right for Your Organization

Email security is being driven by DMARC services. Are they right for you?

Reduced domain spoofing

DMARC reduces the spoofing that occurs in BEC (business email compromise) and on counterfeit websites. In **Mimecast's State of Email Security 2023** survey, 91% of companies say they are being spoofed, and 44% are seeing an increase in this type of fraud.

It's time for zero trust

DMARC is a key element in zero-trust architectures. The U.S. government has been driving DMARC's use by its agencies and contractors for several years, and it is now mandating a zero-trust architecture. Zero-trust strategies are also being mainstreamed in Europe.

It's never been easier

Solutions such as **DMARC Analyzer** reduce the complexity and time requirements of implementing DMARC. Including record setup wizards and user-friendly reports, some solutions can also be integrated across various security tools for even greater ease of use.

Deliver email securely

DMARC determines whether outbound emails are accepted or rejected by email providers, who increasingly view non-standardized email as suspect. This allows organizations to deliver email much more securely.

The global email authentication standard is known as **DMARC** (domain-based message authentication, reporting, and conformance). DMARC allows email senders and receivers to share information about an email's legitimacy as well as instructions for handling any mail coming from spoofed domains run by cyber attackers.

Putting DMARC to work

Going forward, 88% of SOES 2023 survey respondents say their organizations are looking to implement DMARC in the next 12 months to combat email spoofing, with many indicating that they have an active plan underway. **Get a free trial** of Mimecast's DMARC Analyzer.