What is DMARC and why do I need it?

Author:
Webservio Inc.

Created On: 12 Dec 2017 12:39 PM

DMARC is a protocol that stands for "Domain-based Message Authentication, Reporting and Conformance."Â It uses SPF and DKIM to determine the legitimacy of an email message and requires both to fail in order to take action on a message.

DMARC is a way to make it easier for email senders and recipients to determine if a message is truly from the sender and what to do if it isn't.Â This makes it easier to identify spam and phishing messages, and keep them out of users' inboxes.

DMARC gives the legitimate owner of the domain a way to request failing messages - spoofed, spam, and phishing - be put directly in the spam folder or rejected altogether.

DMARC policies remove the guesswork from email recipient's handling of these failed messages, which eliminates or limits the user's exposure to potentially fraudulent and malicious messages.

DMARC only protects against direct domain spoofing and will not protect against attacks using similar domain names (ie sending from a domain that looks similar to the target), or display name abuse.