Domain-based Message Authentication, Reporting and Conformance

DMARC enhances email security by guiding how to handle emails that fail SPF or DKIM checks.

DMARC allows domain owners to set policies for handling failed SPF or DKIM checks.

Policies are published in DNS records, dictating whether to quarantine or reject suspicious emails.

The recipient mail server checks SPF and DKIM alignment with the DMAR policy to check authenticity.

Emails that fail DMARC are then subject to the policy dictated by the domain owner, either to monitor, quarantine or reject these emails.

Tech Service Partner Limited,
Unit 1 Oak House Business Centre,
Samuel Brunts Way,
Mansfield, NG18 2AH

01623 259372

TSP
TECH SERVICE PARTNER