What is DMARC?

DMARC stands for **D**omain-based **M**essage **A**uthentication, **R**eporting and **C**onformance.

DMARC is a technical standard that helps protect email senders and recipients from advanced threats. It also allows website operators to detail their authentication practices and specify the actions to be taken when an email fails authentication. DMARC also provides a way for email recipients to report any email that fails authentication.

DMARC serves as a vital tool for email domain owners to safeguard their domains against unauthorized usage, particularly email spoofing—a deceptive tactic commonly employed in phishing attacks and cyber threats. Email spoofing involves the manipulation of email headers to mimic legitimate sources, aiming to trick recipients into divulging sensitive information, downloading malware, or participating in actions that compromise security.

Not sure how to implement DMARC? Get Managed DMARC Services from GlowHost. We'll do it for you!

By integrating with established authentication protocols such as Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM), DMARC empowers administrators to identify and block emails sent by cyber attackers masquerading as legitimate entities. More than 90% of cyber attacks begin with an email, and DMARC makes it incredibly difficult for hackers and criminals to impersonate a sender. DMARC protects senders, recipients and can even stop many breaches by adding an extra layer of protection to your security policies.

- **SPF (Sender Policy Framework)** allows domain owners to specify which email servers are permitted to send email on behalf of their domain. When an email is received, the receiving email server checks the SPF record to verify that the email comes from an authorized server.
- **DKIM (DomainKeys Identified Mail)** involves adding a digital signature to outgoing emails. This signature is validated against a public key in the domain's DNS records, confirming that the email content hasn't been tampered with during transit.
- **DMARC** ties SPF and DKIM together by allowing domain owners to specify a policy in their DNS records that dictates how receiving email servers should handle emails that fail SPF and DKIM checks. DMARC also provides a mechanism for reporting back to the domain owner about emails that pass or fail these checks, giving insights into potential authentication issues or spoofing attempts.

By implementing a **DMARC policy**, you're requesting that recipient mail servers how to handle unauthorized use of your domain's email. You could strictly monitor email traffic ("**p=none**"), quarantine email traffic to be on the safe side ("**p=quarantine**"), or completely reject all unauthorized messages ("**p=reject**").

Make sure to check out our **DMARC Policy Cheat Sheet** (quick reference guide) to see how DMARC policy selectors work.

Related Topics:

- DMARC Policy Selectors & Tags Quick Reference
- DMARC None or Ignore Policy
- DMARC Quarantine Policy
- DMARC Reject Policy
- DMARC Policy Percentages
- DMARC RUA Reporting - Aggregate Reports (rua)
- DMARC RUF Reporting - Forensic Reports (ruf)
- DMARC Subdomain Policy (sp)
- DMARC DKIM Alignment (adkim)
- DMARC SPF Alignment (aspf)
- What is BIMI?
- What is a VMC?
- DMARC, DKIM, SPF and BIMI Info

DMARC can be configured on all GlowHost plans with self-service options, or the GlowHost team can do it for you!