DMARC Reject Policy

DMARC's Reject Policy Explained

"**p=reject**"

The most stringent of the DMARC policies, the "**p=reject**" selector offers robust protection against email spoofing and phishing attacks by instructing recipient mail servers to outright reject emails that fail DMARC authentication. These rejected emails are typically returned to the sender (bounced) during the SMTP handshake, ensuring they don't reach the intended recipients' inboxes. This policy helps ensure that only emails authenticated using **SPF (Sender Policy Framework)** and **DKIM (DomainKeys Identified Mail)** pass through to recipients' inboxes, thereby reducing the risk of malicious emails reaching users

While effective in blocking malicious emails, implementing the "**p=reject**" policy requires careful consideration and thorough testing to avoid disrupting legitimate email delivery. Most organizations will choose a **Percentage Selector** in the early phases of deploying the "**p=reject**" policy.

Domain owners must ensure that all legitimate emails are authenticated correctly to prevent false positives. Additionally, organizations should communicate the implementation of the *Reject* policy to stakeholders and provide guidance on email authentication best practices to minimize any potential disruptions. In simpler words, tell your people that you are about to "flip the switch" so they are on the lookout for any potentially negative impact before deploying a DMARC reject policy.

Related Topics:

- What is DMARC?
- DMARC Policy Selectors & Tags Quick Reference
- DMARC None or Ignore Policy
- DMARC Quarantine 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
