DMARC Quarantine Policy

DMARC's Quarantine Policy Explained

"**p=quarantine**"

The Quarantine policy "**p=quarantine**" takes a step further in email security over "**p=none**" by requesting remote mail servers to divert suspicious emails to a separate folder in the recipient's mailbox. These mail folders are often labeled as spam, junk, junkmail, quarantine or similar, instead of delivering them directly to recipients' inboxes.

This policy provides an intermediate level of protection against potentially malicious emails while still allowing legitimate messages to be delivered. By implementing the *Quarantine* policy, domain owners can reduce the risk of users interacting with phishing attempts or malware-laden emails. However, it's important for organizations to regularly monitor the quarantine folder to ensure legitimate emails aren't inadvertently categorized as suspicious. This can be done by setting up a test email account on a third party mail server and observing the behavior of delivered email. It also allows 3rd party organizations to review potentially suspicious emails that arrive on their mail server before deciding whether to deliver them to the recipient or permanently discard them.

Additionally, recipients should be educated on how to access and review quarantined emails, as some critical communications may end up there. Organizat ions should eventually aim to move towards a policy of "**p=reject**" once they are comfortable with their quarantine policy for a stronger email security posture.

Related Topics:

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