DMARC Subdomain Policy (sp)

In DMARC, the "sp" tag stands for "Subdomain Policy." It specifies the DMARC policy to be applied to subdomains that do not have their own DMARC record published.

Here's how the "sp" tag works in DMARC:

1. **Setting the sp tag**: In your DMARC record, you can specify the "sp" tag followed by one of the three DMARC policy values: "none," "quarantine," or "reject."
2. **Fallback policy and default behavior for subdomains**: The fallback policy for subdomains refers to the behavior of DMARC policy enforcement when a subdomain does not have its own DMARC record published. If a subdomain does not have its own DMARC record published, DMARC policy enforcement falls back to the parent domain's DMARC policy. In other words, this means that the DMARC policy specified in the organizational domain's DMARC record (the parent domain) is inherited by its subdomains. This allows you to enforce consistency in policy enforcement across their entire domain hierarchy.
3. **Policy values**:
    - "**sp=none**": No specific action is taken. This is often used for monitoring purposes without enforcement.
    - "**sp=quarantine**": Messages failing DMARC authentication are quarantined.
    - "**sp=reject**": Messages failing DMARC authentication are rejected.
4. **Considerations**: It's essential to carefully consider the DMARC policy applied to subdomains, as it may impact email delivery and security across your organization. Enforcing a strict policy (such as "quarantine" or "reject") on subdomains can help prevent email spoofing and phishing attacks, but may also increase the risk of legitimate emails being quarantined or rejected if proper authentication mechanisms are not in place.

In summary, the fallback policy for subdomains in DMARC helps organizations maintain consistent email authentication and security measures across their entire domain hierarchy, even when individual subdomains do not have their own DMARC records published.

Related Topics:

- What is DMARC?
- 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 DKIM Alignment (adkim)
- DMARC SPF Alignment (aspf)
- What is BIMI?
- What is a VMC?
- DMARC, DKIM, SPF and BIMI Info

Don't have the time or energy to learn, setup, monitor and maintain DMARC? What if you had a team of DMARC experts to do this for you?

Let us do DMARC for you. Check out Managed DMARC Services by GlowHost.