Understanding Email Security Results

The Email Security section presents the results of security checks on key email authentication protocols, including DMARC, SPF, MX, and DKIM. This information helps users assess the email security configuration of the scanned domain, ensuring that measures are in place to prevent email spoofing and protect against phishing attacks.

DMARC (Domain-based Message Authentication, Reporting, and Conformance):
DMARC is an email authentication protocol that builds on SPF and DKIM to ensure that emails sent from your domain are properly authenticated. It provides domain owners with a mechanism to specify how to handle emails that fail authentication checks, offering options such as rejecting or quarantining suspicious messages. DMARC also generates reports on email authentication activity, giving you insights into who is sending emails on behalf of your domain and helping identify potential abuse.

SPF (Sender Policy Framework):
SPF is an email authentication method that allows domain owners to define which IP addresses or servers are authorized to send emails on their behalf. This is done by publishing an SPF record in the domain's DNS settings, listing the permitted mail servers. When an email is received, the recipient's mail server checks the SPF record to verify that the email came from an authorized source. If the sending server is not listed in the SPF record, the email may be marked as spam or rejected.

MX (Mail Exchanger) Records:
MX records are a type of DNS record that specify the mail servers responsible for receiving emails on behalf of a domain. They direct incoming email to the correct mail servers, ensuring that messages are delivered to the right destination. Proper configuration of MX records is crucial for ensuring reliable email delivery, as incorrect settings can lead to misrouted or undelivered emails.

DKIM (DomainKeys Identified Mail):
DKIM is an email authentication technique that allows the sender to sign their emails with a digital signature. This signature is included in the email header and is used to verify that the message was not altered in transit. The public key required to verify the signature is published in the sender's DNS records. By using DKIM, recipients can be confident that the email genuinely originated from the stated domain and was not tampered with during transmission.

ReConfirm checks a default list of DKIM selectors to verify the authenticity of your emails. If your organization uses custom selectors for DKIM, you can add them for scanning by clicking "Check Selectors" and entering the relevant selectors. This ensures a comprehensive evaluation of your email security configuration.

Revision #2
Created 16 September 2024 11:57:14 by Raphael
Updated 16 September 2024 12:03:22 by Raphael