Email Authentication and Security

There are 3 authentication methods to verify email coming from a specific domain is authentic; SPF, DMARC and DKIM. This reduces or eliminates spammers and phishers from using a domain to falsely appear authentic.

How does SPF work?

Sender Policy Framework (SPF) is a way for a domain to list all the servers they send emails from. Think of it like a publicly available employee directory that helps someone to confirm if an employee works for an organization. SPF records list all the IP addresses of all the servers that are allowed to send emails from the domain, just as an employee directory lists the names of all employees for an organization. Mail servers that receive an email message can check it against the SPF record before passing it on to the recipient's inbox.

How does DKIM work?

DomainKeys Identified Mail (DKIM) enables domain owners to automatically "sign" emails from their domain, just as the signature on a check helps confirm who wrote the check. The DKIM "signature" is a digital signature that uses cryptography to mathematically verify that the email came from the domain.

Specifically, DKIM uses public key cryptography:

- A DKIM record stores the domain's *public key*, and mail servers receiving emails from the domain can check this record to obtain the public key
- The *private key* is kept secret by the sender, who signs the email's header with this key

- Mail servers receiving the email can verify that the sender's private key was used by applying the public key

How does DMARC work?

Domain-based Message Authentication Reporting and Conformance (DMARC) tells a receiving email server what to do given the results after checking SPF and DKIM. A domain's DMARC policy can be set in a variety of ways — it can instruct mail servers to quarantine emails that fail SPF or DKIM (or both), to reject such emails, or to deliver them. DMARC policies are stored in DMARC records. A DMARC record can also contain instructions to send reports to domain administrators about which emails are passing and failing these checks. DMARC reports give administrators the information they need to decide how to adjust their DMARC policies (for example, what to do if legitimate emails are erroneously getting marked as spam).

Source: https://www.cloudflare.com/learning/email-security/dmarc-dkim-spf/

NEXT STEPS

Configure SPF Policy

Configure DKIM Signature

Configure DMARC Reports

Revision #6
Created 20 August 2024 18:43:02 by orngbnch
Updated 20 August 2024 19:35:43 by orngbnch