email authentication protocols like SPF, DKIM, and DMARC

SPF, DKIM, and DMARC are email authentication protocols that **verify an email's sender to prevent spam and phishing**. SPF checks if the sending server is authorized, DKIM verifies the email's integrity with a digital signature, and DMARC tells receiving servers how to handle emails that fail SPF or DKIM checks.

SPF (Sender Policy Framework)

What it is: A DNS record that lists the IP addresses authorized to send emails for a specific domain.

How it works: When an email arrives, the receiving server checks the sender's IP address against the SPF record in the domain's DNS to see if it's on the approved list.

Purpose: To prevent spammers from sending emails with a forged sender address from your domain.

DKIM (DomainKeys Identified Mail)

What it is: A cryptographic signature added to email headers.

How it works: The sending server uses a private key to sign each outgoing email. The public key, stored in the domain's DNS, is used by the receiving server to verify the signature and confirm the message content hasn't been altered.

Purpose: To ensure the email originated from the domain it claims to be from and that its contents have not been tampered with in transit.

DMARC (Domain-based Message Authentication, Reporting, and Conformance)

What it is: A policy that leverages both SPF and DKIM.

How it works: It provides instructions to the receiving server on what to do with emails that fail SPF and/or DKIM checks. It can tell servers to do nothing (`p=none`), send failing emails to spam (`p=quarantine`), or reject them entirely (`p=reject`). It also sends reports back to the sender to provide visibility into email traffic and authentication results.

Purpose: To give domain owners control over how unauthenticated emails are handled and to protect their domain's reputation by preventing fraudulent emails from reaching inboxes

---

Revision #2
Created 29 October 2025 02:43:42 by AI API
Updated 1 December 2025 14:24:37 by AI Channel