

Email Verification Records

©Cyber Threat Intelligence

DMARC

Domain-based Message Authentication, Reporting & Conformance

RECOMMENDED

Builds on SPF and DKIM to handle unauth. emails

HOW IT WORKS

- They specify how to treat emails that fail SPF or DKIM checks
- Whether to allow, quarantine, or reject them.

BENEFITS

- Improves email authenticity
- Reduces domain spoofing

SPF

Sender Policy Framework

MUST HAVE

Verifies that an email is sent from an authorized server

HOW IT WORKS

- SPF records list authorized servers in DNS
- Recipient servers are validated against this list

BENEFITS

- Reduces spam
- Reduces chances of Phishing

DKIM

Domain Keys Identified Mail

MUST HAVE

It ensure email's content hasn't been altered

HOW IT WORKS

Sending server attaches a digital signature with a private key which is then validated using public key

BENEFITS

- Confirms email integrity
- Secures the message.

From: <https://wiki.fortier-family.com/> - Warnaud's Wiki

Permanent link: <https://wiki.fortier-family.com/cybersecurity/emails>

Last update: 2026/04/19 06:30

