

EMAIL AUTHENTICATION (DMARC).



SPF can pass on a completely different domain than the one shown in the visible From field. **DMARC exists specifically to close that gap, requiring the authenticated domain to actually align with what the recipient sees — without it, a spoofed email can pass every individual check.**

- SPF & DKIM
- DMARC ALIGNMENT
- DOMAIN SPOOFING
- AGGREGATE REPORTING

01 THE MECHANISM



SPF Authorizes Servers, Not the Visible Sender

SPF checks whether the sending server is authorized for the technical envelope sender, which is **often not the same domain** as the "From:" address a user actually sees.



DKIM Cryptographically Signs the Message

A private key signs specific headers and the body, so DKIM verifies both who sent it and **that the content wasn't altered in transit**, something SPF alone never checks.



DMARC Requires the Visible Domain to Align

DMARC ties SPF and DKIM together and requires the authenticated domain to **match the domain the recipient actually sees**, closing the gap that lets SPF pass while the visible sender is spoofed.

02 THE FLOW

DMARC Enforced at Reject

CONTAINED

- An attacker attempts to send an email with the company's exact domain forged in the visible From field, **routed through an unrelated, unauthorized server**.
- SPF and DKIM alignment checks against the visible domain both fail, since **neither the sending server nor any valid signature** corresponds to that domain.
- The receiving server enforces the published DMARC policy and **rejects the message outright**, before it ever reaches an inbox.

SPF and DKIM With No DMARC Enforcement

EXPOSED

- The same forged email arrives, technically failing alignment, but with **no DMARC policy published, or one set to monitor-only**, nothing tells the server to act.
- The receiving server delivers the message to the inbox looking completely legitimate, with the **company's real domain visible in the From field**.
- The recipient has no technical reason to doubt it, and the **organization never even sees a report** that the spoofing attempt happened.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
SPF Record Accuracy	A published, correctly maintained list of servers authorized to send mail for the domain, kept under the 10 DNS lookup limit.
DKIM Signing	Cryptographic signatures on outgoing mail verifying both sender authenticity and message integrity, with the public key correctly published in DNS.
DMARC Alignment & Policy	A published policy requiring SPF or DKIM to align with the visible From domain, graduated from monitoring to actual enforcement.
DMARC Reporting Review	Regularly reviewing aggregate reports to discover unauthorized senders, misconfigured legitimate services, or active spoofing attempts.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
SPF Alone, No DKIM or DMARC	No	SPF can pass on a completely different domain than what's shown in the visible From field, leaving the displayed sender unprotected.
DMARC Published at Monitor-Only (p=none) Indefinitely	No	Monitor-only mode collects visibility but takes no action, so a spoofed email still reaches the inbox exactly as before.
DKIM Signing Without SPF or DMARC Alignment Requirements	No	A valid signature alone doesn't stop a message from a different domain claiming to be the trusted one in the visible From field.
Assuming Your Own Domain Protection Stops Look-Alike Domains	No	DMARC only protects your exact domain from being spoofed; it does nothing for a typosquat or homograph domain impersonating you.
SPF + DKIM + DMARC at Enforcement + Ongoing Report Review	Yes	Closes the alignment gap SPF and DKIM leave open individually and actually acts on what the reports reveal.

EMAIL AUTHENTICATION (DMARC).

AUTHENTICATE · ALIGN · ENFORCE

05 PROGRAM OPERATIONS

SPF authenticates the technical envelope sender, not necessarily the address a recipient actually sees, which is exactly the gap DMARC alignment exists to close.

DMARC deployment is meant to be graduated, starting at monitor-only to build confidence that legitimate mail passes, before moving to quarantine and then reject.

DMARC aggregate reports are genuinely actionable intelligence, often the first place an organization discovers shadow IT email senders or an active spoofing campaign.

Protecting your own domain with DMARC does nothing for a look-alike or typosquat domain impersonating you, which is why this control and user awareness address different parts of the same threat.

06 CONTROL MAPPING

RFC 7208 (SPF)

The technical standard defining how Sender Policy Framework records are published and evaluated, including the 10 DNS lookup limit.

RFC 6376 (DKIM)

The technical standard defining DomainKeys Identified Mail signing and verification.

RFC 7489 (DMARC)

The standard defining DMARC policy, alignment requirements, and aggregate/forensic reporting formats.

M3AAWG BEST PRACTICES

Industry messaging security guidance commonly referenced for email authentication deployment and abuse mitigation.

07 WHAT THIS DOES NOT SOLVE

Look-Alike and Typosquat Domains

DMARC only protects the exact domain it's published for; it does **nothing to stop an attacker registering a similar-looking domain.**

Compromised Legitimate Accounts

A properly authenticated email sent from an actually compromised mailbox **passes every check**, since the authentication is technically valid.

Message Content and Social Engineering

Authentication confirms who sent a message, not whether its content is legitimate; a **properly authenticated email can still be a convincing scam.**

Mail Forwarding Breakeage

Legitimate forwarded mail can fail SPF and sometimes DKIM checks, creating **false positives that require specific handling**, not just stricter enforcement.

08 MYTHS VS. REALITY

MYTH "SPF alone stops email spoofing."	REALITY SPF can pass on a completely different domain than the one shown in the visible From field, leaving the displayed sender unprotected without DMARC alignment.
MYTH "If our domain has SPF and DKIM, we're protected from impersonation."	REALITY Without a DMARC policy actually enforcing alignment, a spoofed email can still pass individual checks on an unrelated domain and reach the inbox.
MYTH "DMARC at monitor-only is basically the same as full protection."	REALITY Monitor-only mode collects visibility into what's happening but takes no action to actually block a spoofed message.
MYTH "Once our own domain is protected, we're safe from impersonation attacks."	REALITY DMARC does nothing for a look-alike or typosquat domain that never uses your actual domain at all.
MYTH "Email authentication catches every BEC attempt."	REALITY A properly authenticated email from a genuinely compromised account, or a convincing scam from a look-alike domain, passes every technical check.

09 SPEAK THE PROGRAM — KEY TERMS

SPF (SENDER POLICY FRAMEWORK)

A DNS record listing servers authorized to send mail for a domain, **checked against the technical envelope sender.**

DKIM (DOMAINKEYS IDENTIFIED MAIL)

A cryptographic signature on outgoing mail **verifying sender authenticity and message integrity.**

DMARC ALIGNMENT

The requirement that an authenticated SPF or DKIM domain **match the domain visible in the recipient's From field.**

DMARC POLICY (NONE/QUARANTINE/REJECT)

The graduated enforcement level a domain owner publishes, **from monitor-only through actually blocking** failing mail.

AGGREGATE REPORT (RUA)

A regular report showing which servers are sending mail claiming to be from a domain and **whether they passed authentication.**

ENVELOPE SENDER

The technical Return-Path address SPF actually checks, **often different from the visible From address** a recipient sees.