DKIM selector health

The question

Verify DKIM on a real message

Finding a DNS key gives you a lead. A successfully verified signature shows what happened to a particular outgoing message.

01 Understand

02 Observe

03 Verify

A practical briefing for the people who own your domain.

DKIM selector health

The mechanism

A selector points to the key

The signature names its domain and selector. The recipient retrieves the public key and checks the signed content.

01 Sender signs message

↓

02 Recipient gets selector's DNS key

↓

03 Recipient verifies actual signature

The scanner samples public key locations only. It does not perform the message signature verification shown here.

DKIM selector health

The evidence

Four samples cannot prove absence

> Our scanner checks four common selectors. A broken publication costs points even when another selector has a usable key. Verify signing on a real message.

PUT THE OBSERVATION IN CONTEXT

Public signal

Service context

Operational validation

Use the finding to start an owned review.

DKIM selector health

The handoff

Ask the email service owner

Send representative messages from each provider. Inspect the signature domain, selector and trusted recipient authentication result.

BRING THE RIGHT OWNERS TOGETHER

01 Email service owner

02 Mail provider with DNS administrator

DKIM selector health

Your checklist

Keep the DKIM evidence checklist

- ✓ List sending services
- ✓ Record active selectors
- ✓ Confirm verification and DMARC alignment
- ✓ Plan rotation

> Read the full DKIM discovery explainer.
>
> **/learn/dkim**