

Email authentication report

Prepared for Your client

5 domains checked on 2026-10-13, from public DNS: SPF, DKIM and DMARC for each.

2 need a fix	3 pass SPF, DKIM and DMARC	0 not found or not readable
------------------------	--------------------------------------	---------------------------------------

Domain	SPF	DKIM	DMARC
example.com	■ Pass	■ Not found	■ Pass
example.net	■ Pass	■ Not found	■ Pass
stripe.com	■ Pass	■ Pass	■ Pass
github.com	■ Pass	■ Pass	■ Pass
basecamp.com	■ Pass	■ Pass	■ Pass

Findings and fixes, domain by domain

example.com

■ Pass	SPF	SPF is published and needs 0 of 10 DNS lookups.
■ Not found	DKIM	No DKIM key at the 10 common selector names (default, google, selector1, selector2, k1, k2, s1, s2, dkim, mail). Your mail provider may use a custom name, which one header of a sent email shows.
■ Pass	DMARC	DMARC is published with p=reject.

Fix first

1. Add MX records for example.com, or use a Reply-To address on a domain that receives mail.

example.net

■ Pass	SPF	SPF is published and needs 0 of 10 DNS lookups.
■ Not found	DKIM	No DKIM key at the 10 common selector names (default, google, selector1, selector2, k1, k2, s1, s2, dkim, mail). Your mail provider may use a custom name, which one header of a sent email shows.
■ Pass	DMARC	DMARC is published with p=reject.

Fix first

1. Add MX records for example.net, or use a Reply-To address on a domain that receives mail.

stripe.com

■ Pass	SPF	SPF is published and needs 7 of 10 DNS lookups.
■ Pass	DKIM	A DKIM key is published at selector google.
■ Pass	DMARC	DMARC is published with p=reject.

github.com

■ Pass	SPF	SPF is published and needs 10 of 10 DNS lookups.
■ Pass	DKIM	A DKIM key is published at selector google.
■ Pass	DMARC	DMARC is published with p=quarantine.

basecamp.com

■ Pass	SPF	SPF is published and needs 3 of 10 DNS lookups.
■ Pass	DKIM	A DKIM key is published at selector google.
■ Pass	DMARC	DMARC is published with p=quarantine.

Next step

Your Company can send the exact records to publish for each domain marked Fail or Not found, and check them again once they are live. Contact Your Company at hello@your-company.example.

What the three records do

SPF lists the servers allowed to send mail for the domain. Receivers check the sending server against it.

DKIM signs each message with a key published in DNS, so a receiver can tell the message was not changed and came from the domain.

DMARC tells receivers what to do with mail that fails SPF and DKIM (nothing, spam folder or reject) and where to send reports.

Since 2024 Gmail and Yahoo, and since 2025 Microsoft, ask bulk senders for all three; mail without them is more likely to land in spam or bounce.

What this report cannot see

This report reads public DNS only. It does not send a test message, so it cannot see the sending server's reputation, blocklists or message content. DKIM is looked up at the selector named for the domain, or at the 10 common selector names; a key at a custom name shows as not found. Records change: run the check again after any DNS change.