

Sender Health Audit

Newsletter A

65

/ 100

Authenticated but unprotected: the p=none gap is the priority fix.

Method: generated from public DNS records plus the Authentication-Results of one real send. No access to the sending platform or list was required.

How the last email was actually judged

Check	Result on a real message
SPF	pass
DKIM	pass
DMARC	pass policy p=none
One-click unsubscribe	present
Sending platform	SendGrid

Findings, ranked by deliverability impact

HIGH

DMARC is published but at **p=none**: your mail authenticates, but you have **no protection**: anyone can spoof example-newsletter.com and mailbox providers won't stop it. Move to p=quarantine, then p=reject.

LOW

SPF ends in ~all (softfail): acceptable, but -all is the stronger posture.

LOW

No TLS-RPT record: a cheap add for visibility into TLS delivery failures.

LOW

No MTA-STTS policy: enforces TLS on inbound; a posture point for a polished setup.

Why this matters now

Google and Yahoo have required authenticated, one-click-unsubscribe bulk mail since February 2024, and Microsoft began rejecting non-compliant bulk senders in May 2025. Publishing DMARC at **p=none** meets the letter of the rule but leaves the domain spoofable; moving to enforcement (**p=reject**) is what actually protects sender reputation, and your open rates.