inboxposture

Sender Health Audit

Newsletter B

80
/ 100

Good foundation: one step (p=reject) from full protection.

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=quarantine**
One-click unsubscribe	**present**
Sending platform	SendGrid

Findings, ranked by deliverability impact

MED DMARC at **p=quarantine**: spoofed mail is sent to spam, not rejected. You're most of the way; graduate to **p=reject** for full protection.

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-STS 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.