GROWTH CAB | VERSION 2 | REVIEWED 6 OCTOBER 2026

Deliverability diagnosis: worked example

Illustrative incident. Every domain in it ends in .example, a name reserved for documentation, so none of them receives mail.

Illustrative incident with a fictional team and synthetic header facts. Diagnose your own environment before you change DNS or sending settings.

Observation and scope

A fictional team reports that replies declined after moving one campaign to a new sending service. There is no reliable inbox-placement measurement. Campaign copy, audience and infrastructure changed together, so reply rate alone cannot isolate the cause.

SPF pass
bounce.vendor.example

DKIM none
no signature on the sample

DMARC fail
From sender.example, no alignment

1 retest
authorized message, same path

Evidence ledger

A received test-message header shows SPF=pass for bounce.vendor.example, DKIM=none and DMARC=fail for visible From sender.example. These are synthetic header facts. The two organizational domains do not align. A separate campaign message received an SMTP rejection: read its exact enhanced status code, timestamp and destination provider in the bounce itself.

Interpretation

The successful SPF check authenticates the envelope sender in this example, and that identity belongs to a different domain from the visible From domain. With no aligned DKIM pass either, the sample fails DMARC. This is an authentication finding for that one message. The cause of each missing reply, and the behavior of each provider, need their own evidence.

Bounded action

The messaging administrator inventories legitimate senders and follows the service's documented setup for signing with the correct domain and aligning the relevant identities. Preserve existing legitimate senders and validate proposed DNS changes before publishing. Keep the DMARC policy, the domains and the volume as they are while the failure is open, so nothing hides it.

Retest and decision

Send one authorized diagnostic message through the same affected path. Inspect the received Authentication-Results header and the actual SMTP outcome. If aligned authentication passes, mark this defect corrected for the tested path. If it still fails, compare the service, signing domain, selector and DNS state. The copy stays as it is, because authentication lives in the sending setup.

Then assess provider-specific rejections, complaints, recipient quality and sending changes one by one. A passing authentication check proves the setup for that path. Inbox placement, reputation and replies each need their own evidence. Write unknowns down as unknowns, so no arbitrary score hides them.

Official references

Google's sender requirements distinguish personal Gmail recipients and sender-volume categories. Apply each provider's own requirements to the mail it receives. Reference: https://support.google.com/mail/answer/81126?hl=en

Microsoft explains the separate roles of SPF, DKIM, DMARC and composite authentication. Reference: https://learn.microsoft.com/en-us/defender-office-365/email-authentication-about

Reusable incident record

Record provider; UTC time window; sending service; visible From domain; envelope domain; DKIM signing domain; message/SMTP evidence location; observation; hypothesis; approved owner/action; retest result; remaining unknowns. Keep full private headers in an access-controlled location.

Source page: https://www.growthcab.com/email-deliverability-consultant