



Email Deliverability Audit Checklist

What we check before a single cold email goes out, and what we check when mail starts landing in spam. Written for Google Workspace inboxes sending through Smartlead, and applies to most setups.

Covers DNS auth · domains · warm-up · lists · content · monitoring

Access Read-only is enough

Output Written findings within 2 business days

01 SPF: who is allowed to send

- ☐ Exactly **one** `v=spf1` TXT record per hostname
Two SPF records = a permanent error; many receivers then treat SPF as failed.
- ☐ **10 or fewer DNS lookups** in total, counting nested includes
`include`, `a`, `mx`, `exists`, `redirect` each count; `ip4` / `ip6` don't. Over 10 = permerror.
- ☐ Every real sender is listed (Workspace, CRM, helpdesk, billing tool), unused ones removed
- ☐ **~all vs -all** chosen deliberately
`~all` (softfail) is safer while you're still finding senders; move to `-all` once the list is complete. With DMARC enforcing, DMARC usually decides, but some receivers reject an SPF `-all` failure before DMARC runs, so get aligned DKIM working first.
- ☐ No deprecated `ptr` mechanism
- ☐ SPF checked on the **Return-Path** domain, which isn't always the visible From domain

```
# good shape for a Workspace-only sending domain
example-sending.com. TXT "v=spf1 include:_spf.google.com ~all"
```

02 DKIM: is the mail signed?

- ☐ DKIM **enabled for every sending service**, each with its own selector
Google Workspace (`google._domainkey`), Microsoft 365 (`selector1/2`), CRMs and ESPs (e.g. `s1/s2`). A published key isn't proof; confirm "signing on" in each admin console.
- ☐ **2048-bit** keys wherever the provider supports them
- ☐ Signing domain (`d=`) matches the From domain, so DKIM **aligns** for DMARC
- ☐ Old selectors from retired tools removed; rotation owner named
- ☐ Test message headers show `dkim=pass` with the right `header.d`

03 DMARC: policy, reporting, alignment

p=none

Monitor. Collect reports, find every legitimate sender.

p=quarantine

Failing mail goes to spam. Test first with `t=y` (RFC 9989); the old `pct=` tag is now historic.

p=reject

Failing mail is refused. Full protection against spoofing.

- ☐ One record at `_dmarc.`, valid syntax
- ☐ **Progression** none → quarantine → reject, moving only when reports show all legitimate mail passing
- ☐ `rua=` aggregate reports go to a mailbox or tool **someone actually reads**
If `rua` points at another domain, that domain must publish an authorization record.
- ☐ Alignment understood: relaxed (default) lets `mail.example.com` align with `example.com`; strict does not
- ☐ At least one of SPF or DKIM **passes and aligns** for every stream
- ☐ Gmail and Yahoo expect bulk senders to publish DMARC (`p=none` is accepted); check the current sender guidelines

04 Subdomain inheritance gotchas

- ☐ **DMARC inherits; SPF doesn't.** A subdomain with no `_dmarc` record uses the parent's policy (or its `sp=` tag). A new `mail.example.com` under a parent at `p=quarantine` is quarantined from day one if it doesn't authenticate and align.
- ☐ Each hostname used as a Return-Path needs **its own SPF**; the parent's SPF doesn't cover it. DKIM is per signing domain.
- ☐ Use `sp=` or a subdomain-specific `_dmarc` record on purpose, not by accident. Give non-sending subdomains a null SPF (`v=spf1 -all`).

05 MX & security gateways

- ☐ MX records point where mail is really received, and **priority order matches intent**
If a gateway (Proofpoint, Mimecast, etc.) should filter first, its MX needs the lowest number. Otherwise mail can skip the gateway.
- ☐ Sending domains have working MX so replies arrive (Workspace MX on each secondary domain)
- ☐ If outbound mail relays through a gateway, SPF includes it and DKIM still aligns after relay
- ☐ Gateway rules aren't quarantining your own test sends or rewriting links in ways that break DKIM

06 Secondary sending domains

- ☐ **Cold email never goes out from the primary domain**; it protects business and client mail
- ☐ Close, honest variants of the brand (e.g. `getexample.com`), `.com` preferred
- ☐ Registered and set up some weeks before sending, not the day of
- ☐ Each has its own SPF, DKIM and DMARC, and its website forwards to the main site
- ☐ 2–3 Google Workspace inboxes per domain, with real names, photos and signatures
- ☐ Custom tracking domain per sending domain (if tracking is used)

07 Inbox warm-up & daily send limits

- ☐ Warm-up on in Smartlead for each inbox **before** cold sends, typically a few weeks
- ☐ Warm-up keeps running at a low level during campaigns
- ☐ "Pre-warmed" inboxes still start slow
- ☐ **Conservative daily cap per inbox:** we start at 10 cold sends per inbox per day and ramp slowly toward 50 (never more), only while bounces and replies look healthy
- ☐ Sending windows in business hours, randomized gaps between sends
- ☐ Total daily volume per domain tracked, not just per inbox

08 List hygiene

- ☐ **Every address verified** just before upload; re-verified if older than 30 days
- ☐ **Bounce threshold:** we aim for hard bounces under 2% a day; our stop rule pauses a campaign when they reach 3% or more, until the cause is found
- ☐ **Catch-alls** excluded, or sent separately in small capped batches, never mixed in
- ☐ Role addresses (info@, sales@) removed by default
- ☐ **Global suppression list:** opt-outs, bounces, complaints, customers and open deals, synced across every campaign and tool
- ☐ Opt-outs honored the same business day (CAN-SPAM allows at most 10 business days)

09 Content & tracking domain

- ☐ Plain text; no attachments or images in first touches
- ☐ 0–1 links; no URL shorteners; link domains match the sender
- ☐ Open-tracking pixel off (or minimal) on step 1
- ☐ **Custom tracking domain** (CNAME, with SSL) instead of the tool's shared domain
- ☐ Physical postal address and a clear opt-out line in every email
- ☐ Tokens have fallbacks; every lead previewed for blank or broken variables

10 Blacklists & Google Postmaster monitoring

- ☐ Domains and sending IPs checked against major blocklists (Spamhaus, Barracuda, SURBL via MXToolbox or similar)
- ☐ **Google Postmaster Tools** verified for every sending domain; spam rate and compliance status reviewed weekly
- ☐ Spam complaints kept well under Google's published 0.3% ceiling (Google advises staying below 0.1%)
- ☐ **One-click unsubscribe** (RFC 8058 [List-Unsubscribe](#) + [List-Unsubscribe-Post](#) headers) on bulk marketing mail, per Gmail and Yahoo sender rules; unsubscribes honored the same business day (Gmail and Yahoo require within 2 days)
- ☐ DMARC aggregate reports reviewed for new or failing senders
- ☐ Microsoft SNDS checked where dedicated IPs are used
- ☐ **Microsoft consumer mailboxes** (Outlook.com, Hotmail, Live), since May 5, 2025: a From domain sending 5,000+ messages a day there needs SPF and DKIM to pass plus a DMARC record (at least p=none) that passes with alignment; non-compliant mail is rejected with [550 5.7.515](#)
- ☐ Seed / placement tests treated as a signal, not proof; a sudden drop in replies is often the first warning

11 Quick reference: example records

```
# one _dmarc record at a time: each record below replaces the one before it
# DMARC, step 1: monitor (reports to a mailbox someone reads)
_dmarc.example-sending.com. TXT "v=DMARC1; p=none; rua=mailto:dmarc@example-sending.com"
# step 2, test quarantine first (publish ONE of these two): new syntax, RFC 9989 (May 2026) test-mode flag
_dmarc.example-sending.com. TXT "v=DMARC1; p=quarantine; t=y; rua=mailto:dmarc@example-sending.com"
# or, to cover receivers on either spec, one combined record: t=y (RFC 9989)
# plus pct=0 (RFC 7489, pct is now historic). Never publish two _dmarc records.
_dmarc.example-sending.com. TXT "v=DMARC1; p=quarantine; t=y; pct=0; rua=mailto:dmarc@example-sending.com"
# then, once reports stay clean: drop t=y (and pct=0)
_dmarc.example-sending.com. TXT "v=DMARC1; p=quarantine; rua=mailto:dmarc@example-sending.com"
# step 3: reject (test first with t=y the same way)
_dmarc.example-sending.com. TXT "v=DMARC1; p=reject; rua=mailto:dmarc@example-sending.com"
# a subdomain that never sends mail: null SPF
files.example.com. TXT "v=spf1 -all"
```

Example domains only. Real records depend on which services send for you, and that's what the audit finds.

12 What you get

Written findings within 2 business days. No calls needed; everything is async and in writing.

Pass / fail per item

Every check above, with the evidence (record, header or screenshot).

Prioritized fix list

Critical, important and nice-to-have, in the order to do them.

Exact DNS changes

Copy-paste records, plus who makes each change: you, your IT provider or your ESP.

Honest timeline

Authentication fixes take days. Sender reputation takes weeks to recover.

Access: read-only is enough (a DNS view and a view of the sending platform). Add us as a user; never share passwords in chat.

Sitrep Leads: nearly 10 years in the U.S. Army Signal Corps, then NOC Manager at Nextel, Senior Engineer at Sprint, Director of the Global Network Operations Center at Time Warner Cable, Neustar, and Director, Data Center and ITIL Project Management at ThruPoint (now Accuative). Now applied to cold email. Michael reviews every finding.