

The 25 checks that keep cold email out of spam

If your cold email lands in spam, nothing else matters: not the copy, not the offer, not the list. This checklist covers what small teams most often miss.

1. Authentication (do these first)

- ☐ **SPF** published on your sending domain, listing every service that sends as you (your mailbox provider plus any tools). One SPF record only; stay under 10 DNS lookups.
- ☐ **DKIM** turned on in your mailbox provider (Google Workspace: Admin › Gmail › Authenticate email; Microsoft 365: Defender › Email authentication › DKIM), with a 2048-bit key where offered.
- ☐ **DMARC** published at `_dmarc.yourdomain.com`. Start at `p=none` with a report address (`rua=`) you actually read, then move to `quarantine` once reports show your mail passing.
- ☐ **Alignment**: the domain in your From address matches the domain that passes SPF or DKIM.

Since 2024, Gmail and Yahoo require bulk senders to have SPF, DKIM and DMARC, plus a one-click unsubscribe, and to keep spam complaints under 0.3%. Treat those as the floor, even at low volume.

2. Domain and mailbox

- ☐ Consider a **separate sending domain** for cold outreach (e.g. `getyourbrand.com`), so your main domain's customer email is protected.
- ☐ The domain has a real website and has existed for a while: brand-new domains are treated with suspicion.
- ☐ Each mailbox has a real name, a signature and a profile, and receives replies.
- ☐ Set up **Google Postmaster Tools** for your domain to watch spam rate and reputation.

3. Warm-up and volume

- ☐ New mailboxes start with **real, wanted mail**: replies, conversations, newsletters you signed up for. Avoid paid “warm-up networks” that trade fake opens; mailbox providers treat them as manipulation.
- ☐ Ramp slowly: about **5–10 cold emails a day per mailbox** in week one, adding a few each week. Most small teams stay under 30–50 a day per mailbox.
- ☐ Spread sends through the working day; don't blast at once.
- ☐ Pause and investigate if bounces go above about 2% or replies say “spam”.

4. List hygiene

- ☐ **Verify every address** before the first send. Bounces are the fastest way to damage a domain.
 - ☐ Write to business addresses of people whose role fits your offer, not scraped lists or purchased databases.
 - ☐ Keep a **do-not-contact list** (customers, opt-outs, competitors) and check it before every send.
 - ☐ Remove anyone who bounces or asks to stop, and never add them back.
-

5. The message

- ☐ Plain text, short, one link at most, no attachments on a first email.
 - ☐ Personal to the recipient: what you know about them and why it matters now.
 - ☐ No spam-trigger tricks: misleading subjects, “Re:” on a first email, fake urgency.
 - ☐ Stop the sequence as soon as someone replies.
-

6. The law (US basics, CAN-SPAM)

- ☐ Honest From name and subject line.
 - ☐ Identify the message as an ad where it’s clearly promotional.
 - ☐ Include a **valid postal address** for your business.
 - ☐ Give a clear way to opt out, and honour it within 10 business days.
 - ☐ Writing to the EU, UK or Canada? Their rules are stricter (GDPR, PECR, CASL). Check before you send.
-

This checklist isn’t legal advice.

Sources: Google: Email sender guidelines (<https://support.google.com/a/answer/81126>); Yahoo: Sender best practices (<https://senders.yahooinc.com/best-practices/>); FTC: CAN-SPAM Act compliance guide (<https://www.ftc.gov/business-guidance/resources/can-spam-act-compliance-guide-business>).

How Artificial Outreach helps: it sends from your own Gmail or Microsoft 365 mailbox, checks your domain’s mail records, verifies addresses before writing, honours a do-not-contact list, and stops a sequence when someone replies. The first message to anyone waits for your approval. 14-day trial, no card. www.artificialoutreach.com