

The Deliverability Field Guide

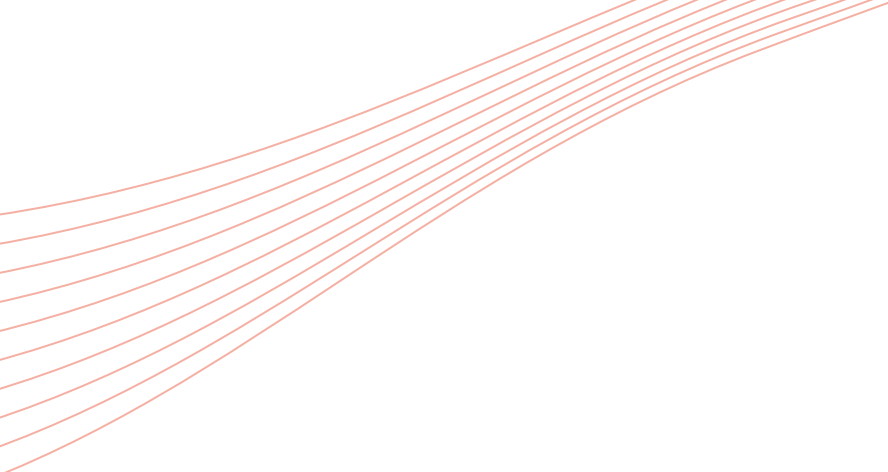
How to keep your domain out of spam



LEAD ^H_Q

Table of contents

Introduction	3
Deliverability is a data problem first	4
Protect your main domain	5
Set up SPF, DKIM, and DMARC	6
Warm-up and volume discipline	7
Write emails for deliverability, not like newsletters	8
Test your setup	9
Monitor: the numbers that matter	10
The recovery playbook	11
The full deliverability checklist	12
Frequently asked questions	13
About LeadHQ	14



Introduction

Every outbound campaign is judged twice. Once by the prospect who reads it, and once, before that, by the mail provider that decides whether the prospect ever sees it.

Most teams obsess over the first judgment and never measure the second. They rewrite subject lines, test new angles, and change sequences, while a growing share of their email quietly lands in spam or never arrives at all. No reply data ever tells them, because a message nobody received looks exactly like a message nobody answered.

This guide covers the second judgment: how Gmail, Outlook, and the other providers decide whether your email deserves the inbox, and how to set up and run your sending so it consistently does.

What decides deliverability

Providers score every sender on reputation. That reputation is built from a handful of signals:

- **The quality of your list.** How often you hit dead addresses and spam traps.
- **Your technical setup.** Whether your domain proves it is who it claims to be.
- **Your sending behavior.** Volume, consistency, and how fast you ramp up.
- **How recipients react.** Opens, replies, deletions, and spam complaints.

Copy matters, but it is the last filter, not the first. A perfectly written email sent from a damaged domain to an unverified list still ends up in spam. That is why this guide starts where most guides end: with the data.

Deliverability is a data problem first

Every email sent to a dead address registers as a hard bounce. Providers read your bounce rate as a direct signal of sender quality: legitimate senders know who they are emailing, spammers do not.

The thresholds: keep hard bounces under 2 percent of sends. Above that, providers start discounting you. Sustained rates above 5 percent do lasting damage to domain reputation.

The problem is that lists go stale fast. MarketingSherpa research puts B2B contact data decay at just over 2 percent per month. People change jobs, mailboxes get closed, companies get acquired. A list that was accurate in January is measurably worse by summer, even if nobody touched it.

Spam traps: the silent killers

Some dead addresses do not bounce. Providers and blacklist operators recycle abandoned mailboxes into spam traps: addresses that accept mail but exist only to catch senders with poor list hygiene. Hitting them repeatedly can put your domain on a blacklist. Bought lists and old exports are where they live.

The fix: verify before every campaign

- Run every list through a verification service before it enters a sequence, even lists from reputable databases. Verification is about freshness, not source.
- Remove invalid addresses entirely. Do not keep them "just in case".
- Treat catch-all and risky addresses as a separate segment. Send to them last, at low volume, and watch the bounce rate.
- Re-verify anything older than 30 days before reusing it.

Everything else in this guide protects your reputation. This step is what stops you burning it in the first place.

Protect your main domain

Never run cold outreach from your main business domain. Instead, register a separate domain or subdomain used only for outbound, such as:

- getcompany.com
- trycompany.com
- hello.company.com

Main domain only (not recommended)

- Spam complaints hit the domain your whole business runs on.
- If reputation drops, everyday communication suffers with it: invoices, support, internal mail.
- Scaling outreach volume becomes impossible without risking the brand.

Separate sending domain (best practice)

- Your main domain stays protected. Outreach reputation issues never touch core operations.
- The sending domain can be warmed up gradually and replaced if it is ever damaged.
- Volume can scale in a controlled way across multiple mailboxes and domains.

Think of it as a business extension line: professional, but separate from the main channel. Register the domain through your existing provider, set up a redirect to your main website, and create two to four mailboxes per domain rather than pushing one mailbox to its limit.

Set up SPF, DKIM, and DMARC

These are email authentication records that prove your messages really come from your domain. Without them, providers may treat your mail as untrusted or fraudulent.

Setting	Purpose	What it does
SPF	Defines which services may send on behalf of the domain	Checks the email comes from an approved server
DKIM	Adds a cryptographic signature to each email	Proves the message was not tampered with and is from the stated sender
DMARC	Sets the policy for mail that fails SPF or DKIM	Tells providers what to do when something looks suspicious

All three are DNS records. An IT admin or your domain provider can add them in 10 to 15 minutes, and most sending platforms provide ready-made values to copy and paste. Recheck them whenever you change sending platforms or domains.

DMARC: start monitoring, then tighten

Begin with a policy of `p=none`, which monitors without blocking. Once reports show your legitimate mail passing consistently, move to `p=quarantine` and eventually `p=reject` for full protection against spoofing.

This is no longer optional. Since 2024, Google and Yahoo require authentication from bulk senders, and Google's sender guidelines require keeping spam complaint rates below 0.3 percent, with under 0.1 percent as the safe target. Unauthenticated cold email is increasingly rejected outright.

Warm-up and volume discipline

A new domain has no reputation. Providers treat sudden volume from an unknown sender as a spam signal, so the first weeks decide how you are classified.

The warm-up sequence

1. **Start with 10 to 20 emails per day per mailbox.** Give each mailbox a recognizable sender name (for example, John from Company) and a complete signature.
2. **Increase gradually over 2 to 4 weeks.** Roughly 10 to 20 percent more per week, not per day.
3. **Watch open and reply rates while ramping.** If they drop suddenly, hold or reduce volume until they recover.

Once warmed up, a properly set up mailbox can handle 100 to 200 emails per day safely, depending on engagement. Most sending platforms include automated warm-up that exchanges mail with real inboxes. Use it for new domains, and keep it running at low volume in the background.

Consistency beats bursts

Reputation rewards steady behavior. Sending 50 emails a day, every weekday, builds trust. Sending 500 on Monday and nothing for two weeks looks like a compromised account. Plan campaigns so daily volume stays level, and spread sends across working hours rather than firing everything at 9:00.

Rule of thumb: if you plan to send more than 30 emails per day from a mailbox, it needs a warm-up phase first. No exceptions for deadlines.

Write emails for deliverability, not like newsletters

Cold outreach works best when it looks like a personal one-to-one message rather than a promotional campaign. Providers reward mail that appears human and relevant.

Best practices

- **Plain text format.** Avoid heavy HTML designs, images, and tracking-laden templates.
- **No attachments.** They increase spam flags and bounce rates. Link to a hosted document instead.
- **Short subject lines.** Ideally under five words. Avoid salesy or clickbait language.
- **Single clear purpose.** One question or one call to action. Avoid multiple links or requests in one email.
- **Natural tone.** Write the way someone would write to a colleague.
- **Limit links.** Zero or one link per email in early touches. Every extra link raises the filter score.
- **Include a clean opt-out.** A simple line makes complaints less likely and keeps you compliant. A recipient who unsubscribes costs you nothing; one who clicks "mark as spam" costs reputation.

Personalization protects deliverability too

Generic blasts get deleted or flagged, and providers watch how recipients react. Emails that reference something real about the prospect earn replies, and replies are the strongest positive signal a sender can get. Good data does not just improve response rates. It keeps you in the inbox.

Test your setup

Step 1: Test deliverability with mail-tester.com

- Go to mail-tester.com. It gives you a temporary email address.
- Send a real outreach email to that address. Do not use "send test email" buttons from tools like HubSpot; they bypass your normal sending setup and do not reflect real-world deliverability.
- Use the same email content you normally send to prospects, especially any message that seems to underperform.
- Repeat the test for every sending platform and mailbox you use.
- Check your score. Aim for 10 out of 10; anything below 9.5 usually indicates a problem.

Step 2: Check your domain setup

- Visit dmarcchecker.app and email the provided address.
- The tool scans your domain for security and deliverability issues.
- Review the SPF, DKIM, and DMARC reports. If any are missing or misconfigured, your emails are far more likely to land in spam, even if the content is perfect.

Step 3: Register with Google Postmaster Tools

- Free, and it shows how Gmail specifically rates your domain: reputation, spam complaint rate, and authentication results.
- Since Gmail hosts a large share of business mailboxes, this is the closest thing to seeing your reputation the way a provider sees it.

Run all three whenever you launch a new domain, change platforms, or create a new sequence. Then repeat monthly.

Monitor: the numbers that matter

Deliverability is not a one-time setup. It is a set of numbers you watch, with thresholds that tell you when to act.

Metric	Healthy	Act when
Hard bounce rate	Under 2%	Above 2%: re-verify the list. Above 5%: stop sending.
Spam complaint rate	Under 0.1%	Approaching 0.3%, Google's stated limit: pause and review targeting and opt-out.
Open rate trend	Stable for your list	A sudden drop across campaigns usually means inbox placement fell, not that copy got worse.
Reply rate trend	Stable for your list	Replies falling while volume is constant is an early reputation warning.
Blacklist status	Not listed	Listed on Spamhaus or similar: follow the recovery playbook on the next page.

Make it a routine

- **Weekly:** scan bounce and reply rates per mailbox in your sending platform.
- **Monthly:** run mail-tester and dmarcchecker, and review Google Postmaster Tools.
- **Every new sequence:** test before launch, then check the first 100 sends for bounce spikes.

Fifteen minutes a week is enough. The teams that get burned are not the ones who skipped a tool. They are the ones who never looked at the numbers until replies stopped.

The recovery playbook

Symptoms of a damaged domain: open rates collapse across all campaigns at once, replies dry up, mail-tester scores drop, or Postmaster Tools shows reputation falling. If that is where you are, more volume makes it worse. Here is the sequence:

1. **Stop all outbound sending.** Immediately. Keep only warm-up traffic running.
2. **Diagnose.** Run mail-tester and dmarcchecker. Check blacklists. Review Postmaster Tools. Find out whether the cause is authentication, list quality, volume behavior, or content.
3. **Fix the root cause.** Repair DNS records, re-verify the entire list and delete invalid and risky addresses, or correct the volume pattern. Skipping this step means repeating the damage.
4. **Rest the domain.** Give it one to two weeks of warm-up-only traffic.
5. **Restart like a new domain.** Begin at 10 to 20 emails per day to your most engaged, freshly verified segment. Their opens and replies are what rebuild reputation. Ramp slowly over 2 to 4 weeks while watching the numbers from page 10.

When to retire a domain: if reputation has not recovered after 4 to 6 weeks of clean, disciplined sending, or the domain sits on a major blacklist that will not delist it, move to a fresh sending domain and start the warm-up process properly.

This is exactly why outreach never runs on the main company domain: a sending domain is replaceable, your brand's domain is not.

The full deliverability checklist

1. Data and list hygiene

- ☐ Verify every list before it enters a sequence, whatever the source
- ☐ Remove invalid addresses; segment catch-all and risky addresses separately
- ☐ Re-verify any list older than 30 days before reuse
- ☐ Keep hard bounces under 2 percent

2. Domain and mailbox setup

- ☐ Use a separate domain or subdomain for outreach (e.g. trycompany.com)
- ☐ Redirect the sending domain to your main website
- ☐ Create mailboxes with recognizable sender names and full signatures
- ☐ Use a central sending platform to manage mailboxes and rotation

3. Authentication

- ☐ Set up an SPF record: only approved platforms send on your behalf
- ☐ Enable DKIM signing on every mailbox
- ☐ Activate a DMARC policy (p=none to start), tighten once reports are clean
- ☐ Confirm SPF, DKIM, and DMARC all show "pass" when tested

4. Warm-up (when sending more than 30 emails per day)

- ☐ Start at 10 to 20 emails per day per mailbox
- ☐ Increase gradually over 2 to 4 weeks; keep daily volume consistent
- ☐ Watch open and reply rates; slow down if they drop

5. Testing and monitoring

- ☐ Send a real outreach email (not a "test email") to mail-tester.com; aim for 9.5 or higher
- ☐ Email dmarcchecker.app and review the SPF / DKIM / DMARC report
- ☐ Register the domain with Google Postmaster Tools
- ☐ Check bounce and reply rates weekly; repeat the full test monthly and per new sequence

Frequently asked questions

Can emails be sent from a regular Gmail or Outlook account instead?

Not recommended. Personal inboxes are not designed for bulk or automated sending, and providers strictly limit volume. A dedicated domain and professional sending system delivers better and protects personal accounts.

What happens if SPF, DKIM, or DMARC are not configured?

Emails may still send, but a large portion will be filtered into spam or rejected. In some cases the domain gets flagged for suspicious activity, affecting all outgoing mail.

Is it legal to send cold emails?

Yes, as long as the message is relevant, not misleading, includes an easy opt-out, and follows local regulations such as GDPR, CAN-SPAM, or PECR where applicable. Professional outreach tools support these compliance features.

How many emails can be sent per day?

A new mailbox should begin with 10 to 20 emails per day. After a proper warm-up, 100 to 200 per day is generally safe, depending on engagement levels.

Our list comes from a well-known database. Do we still need to verify it?

Yes. Verification is about freshness, not source. Contact data decays at more than 2 percent per month, so even a list from a reputable provider contains dead addresses by the time you send. Verify before every campaign.

We are already in spam. Can the domain be saved?

Usually, yes. Follow the recovery playbook on page 11: stop sending, fix the root cause, rest the domain, and restart at warm-up volumes. If reputation has not recovered after 4 to 6 weeks of clean sending, retire the sending domain and start fresh. This is why outreach should never run on your main domain.

Can attachments such as PDFs or brochures be added?

Attachments significantly increase the chance of being flagged as spam. Include a link to a hosted document or webpage instead.

About LeadHQ

Sales reps spend around 70 percent of their time on non-selling tasks. LeadHQ exists to take that work off their plate.

We run the operational side of outbound for B2B sales teams:

- **Prospecting as a Service.** Targeted, verified lead lists built on business logic and buying triggers, so reps never work from stale data.
- **LinkedIn Outreach.** Fully managed LinkedIn campaigns that save teams 40+ hours per month.
- **SDR as a Service.** Vetted SDRs who plug into your team within days, without the cost and risk of hiring.

Everything in this guide, from list verification to domain infrastructure, is part of the system we run for our clients every day, backed by a toolstack worth over 250,000 EUR.

Want your outbound infrastructure handled for you?

Book a Discovery Call and we will walk through your current setup, where email is leaking, and what your team could do with their selling time back.

[Schedule a Discovery Call](#)

The Deliverability Field Guide, July 2026. Published by LeadHQ (Sales Optimization B.V.). You are welcome to share this guide with your team. For questions, reach us at support@leadhq.io.