How to send cold emails without getting blacklisted.

Why this guide is for

You have a great product worth talking about and a list of people who should hear about it. The data is straightforward and the math works. Then you hit send and something goes wrong. The first few days look fine. Then your domain starts showing up in blacklists you didn't know existed, and your sending volume drops before you realize why.

Most cases of cold email failure aren't dramatic. Nothing blows up publicly. A spamtrap quietly logs your domain, a few mailbox providers start routing your messages to spam, and by the time you notice, the damage has been building for weeks. This guide covers the specific mechanics behind those outcomes, so you can avoid them entirely. It assumes you're sending to lists you've legitimately acquired and want to know what technically separates campaigns that land in inboxes from those that don't. It covers DNS authentication, IP reputation, list hygiene, and the ongoing monitoring that keeps deliverability from slowly degrading. It doesn't cover copywriting, offer design, or whether cold email is the right channel for your product. Those are real questions, but they're not the ones that get your domain blacklisted.

SECTION 1

What this guide covers

This guide is about, underneath the surface, what separates the sender, platform, or brand in Gmail's and Yahoo's eyes from a spammer.

- Why some domain reputation is seeing its decline
- Why some domains are being blocked or sent to the spam folder or short-lived sender reputation
- What provides mailbox providers, the signals behind the trust scores
- How authentication, reputation, and engagement work together to determine inbox placement
- What email warm-up actually does
- How to build a sending infrastructure, IP, and a domain strategy
- The tools needed, and how to automate
- How to monitor, diagnose, and recover from blacklisting
- Ongoing maintenance and compliance

The Gmail 5000 standard means sending domain level, subdomain or primary mailbox

Gmail's and Yahoo's bulk sender requirements, Microsoft's Outlook.com and Hotmail.com

Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, Reporting and Conformance (DMARC)

Spamhaus, Barracuda, Google Postmaster Tools, Microsoft SNDS, and blacklist monitoring

SECTION 2

Why a new domain lands in spam by default

Mailbox providers don't start every new domain with a blank slate. They start with a default assumption that most unknown senders are spam. This is not personal. It is a statistical decision based on what the majority of new domains have historically been. Your domain has to earn its way out of that default, and the mechanics of how it does that are specific and measurable.

Sender reputation is a score that mailbox providers assign to your domain and IP based on how recipients have interacted with your mail in the past. Opens, replies, deletions, spam complaints, and bounces all feed into that score. The new domain's reputation is a blank slate, and every signal from your first sends is being weighed against a system that has seen millions of other domains behave in ways that predicted spam. Your first 500 sends are not just sends. They are the data that determines whether your domain gets a reputation worth building on or one that requires months of recovery before it can send at any volume.

Spamhaus, Barracuda, and Google Postmaster Tools provide visibility into your domain's and IP's reputation. Microsoft SNDS covers Outlook.com and Hotmail.com. Yahoo does not publish a comparable tool, so we infer Yahoo reputation from bounce rates, complaint rates, and how your messages are being routed.

What providers measure: the signals behind the trust scores

Sender reputation is not one number. It is a weighted score built from several different signals, and each mailbox provider weights them differently. Understanding what each signal measures and why it matters is the foundation of everything else in this guide. The signals fall into three categories: authentication, reputation, and engagement. Authentication proves you are who you claim to be. Reputation shows how other senders from your domain and IP have behaved. Engagement shows how recipients actually treated your mail when it arrived. Strong scores across all three are what separate a domain that lands in the inbox from one that lands in spam, even when the content and the offer are identical.

Authentication Proves you are who you claim to be. Without it, everything else is weaker. Missing or broken authentication records are the first thing a mailbox provider checks and the first thing that gets your domain flagged.

Reputation Shows how other senders from your domain and IP have behaved. Spam complaints, bounces, and blacklist hits all feed into this score. Reputation is cumulative and slow to recover once it drops.

Engagement Shows how recipients actually treated your mail when it arrived. Opens, replies, deletions, and time spent reading all contribute. Low engagement across a large sending volume is the strongest signal that your mail is being filtered or ignored.

Sender Score A third-party reputation score from 0 to 100 based on spam complaints, blacklist hits, and sending behavior. Mailbox providers don't use it directly, but it correlates with how they treat your domain. Scores below 80 typically indicate problems that will show up in inbox placement.

Postmaster Tools Gmail's free dashboard for domain reputation, spam rate, and authentication pass rates. Microsoft SNDS covers Outlook.com and Hotmail.com. Yahoo does not publish a comparable tool, so we infer Yahoo reputation from bounce rates, complaint rates, and how your messages are being routed.

Consistency: the signal that is easy to break

Mailbox providers track your sending behavior over time and flag sudden changes as a signal that something is wrong. A domain that sends 50 emails per week for six months and then suddenly sends 5,000 in a single day looks like a compromised account or a new spam operation. Ramp your volume gradually, keep your sending times and patterns roughly consistent, and avoid long gaps followed by sudden spikes. Consistency is not about being slow. It is about being predictable, so your reputation builds on a stable foundation rather than triggering anomaly detection every time you change your volume.

What email warm-up actually does

Warm-up is the process of sending low-volume, high-engagement mail from a new domain or IP so mailbox providers can observe that your sending behavior matches what they expect from legitimate senders. It is not a hack or a shortcut. It is the mechanism by which a new domain builds a reputation on a schedule rather than all at once.

Warm-up works because mailbox providers weight recent behavior heavily when they calculate reputation. A domain that sends 5,000 emails on its first day and gets 2,000 bounces and 300 spam complaints will be treated differently than a domain that sends 50 emails on its first day and gets zero bounces and zero complaints. The first domain's reputation is damaged before it has sent anything meaningful. The second domain is still unknown, but it has demonstrated that its senders are careful and that its recipients want its mail. Warm-up is how you create that second pattern on purpose.

Volume ramp vs. full-volume warm-up

Two approaches exist. Volume ramp means sending real campaigns at low volume and gradually increasing it as sender reputation builds. This works if your list is small enough that the volume you can send during the ramp period is sufficient for your campaign. Full-volume warm-up means sending high-volume, high-engagement mail from the start, typically through a dedicated warm-up tool that simulates opens, replies, and time spent reading across a large network of real inboxes. Full-volume warm-up is faster and more predictable for any campaign that needs to reach a meaningful number of recipients within a few weeks. The tradeoff is cost and complexity: you need a warm-up tool or a sending partner that can generate the engagement signals at scale.

What warm-up actually does

Warm-up is not something you finish. It continues running weeks, sometimes months, after your first campaign goes out. The goal is to keep your reputation stable while your volume grows and your list changes. Stopping warm-up the moment you start sending campaigns is how most domains get into trouble.

- Warm-up is not something you finish. It continues running weeks, sometimes months, after your first campaign goes out.
- The goal is to keep your reputation stable while your volume grows and your list changes.
- Stopping warm-up the moment you start sending campaigns is how most domains get into trouble.
- Warm-up generates the sending history a provider needs before it will trust your domain.
- Without it, your first campaign looks like a brand-new domain sending at scale, which is exactly what spam filters are designed to catch.
- Warm-up builds the sender reputation and engagement signals that make inbox placement possible.
- Warm-up operations automate what manual warmed-up mailboxes used to do, sending real messages between internal mailboxes.

SECTION 3

The six warm-up schedule

Warm-up works because it gives mailbox providers a gradual, predictable pattern to observe instead of a sudden spike they can't explain. The schedule below is a starting point for most domains sending cold outreach. Adjust the volume based on your list size and how your first few weeks of sends are performing. The pattern matters more than the exact numbers: steady increase, consistent timing, and no long gaps followed by sudden jumps.

Week	Daily volume	Focus
Week 1	10–20	Establish a baseline. Send to engaged, trusted contacts only.
Week 2	30–50	Keep volume low and consistent. Watch for any early bounces.
Week 3	80–150	Begin adding cold contacts. Monitor open rates closely.
Week 4	200–300	Continue ramping. Check Postmaster Tools for reputation signals.
Week 5	400–500	Approach your target volume. Watch for any reputation drop.
Week 6	500+	Hold at target volume. Monitor weekly for any reputation shift.

The first week of the schedule. Week 1 sends 10 to 20 emails per day, all to contacts you have a real relationship with or who have opted in recently. Week 2 holds at 30 to 50 with no increase. Week 3 begins adding cold contacts and doubles the volume. Week 4 continues the ramp. Week 5 approaches your target volume. Week 6 holds at target and monitors for any reputation shift. The exact numbers depend on your list size and your category, but the pattern of slow, steady increase with no sudden jumps is what matters.

The pre-send checklist

Before you send the first email from a new domain, there are a few things that need to be in place. Skipping any of them creates problems that show up weeks later and are harder to diagnose than to prevent.

- **Domain age and reputation** Check your domain's age and any existing reputation history. Brand-new domains start at the lowest trust level. Tools like Google Postmaster Tools show what mailbox providers already know about your domain.
- **Blacklist check** Run your domain and IP through major blacklists before you start. Spamhaus, Barracuda, and SURBL are the ones that most commonly affect cold email. Delisting takes time, so you want to find any issues before you need to send.
- **DNS authentication** Confirm that SPF, DKIM, and DMARC are set up correctly. Misconfigured records are worse than missing ones because they create ambiguous signals that mailbox providers treat as a red flag.
- **Inbox placement baseline** Send a few test messages to seed addresses across Gmail, Outlook, and Yahoo and check where they land. This gives you a baseline before you start ramping volume.
- **Warm-up tool configured** Set up your warm-up tool with the schedule you want to follow and confirm that it is sending real engagement signals, not just empty messages.
- **Suppression list ready** Import your bounce and unsubscribe lists before the first send. Sending to addresses that have already bounced or unsubscribed is the fastest way to damage your reputation.

Authentication: SPF, DKIM and DMARC without the jargon

Three DNS records prove to mailbox providers that you are who you claim to be. Without them, your mail looks like anyone could have sent it, and mailbox providers treat that as a default assumption of spam. Setup takes about an hour if your DNS access is straightforward. The ongoing maintenance is minimal once the records are in place.

SPF, who is allowed to send

SPF is a DNS record that lists the mail servers that are allowed to use your domain, and mailbox providers check it against the server that actually sends your mail.

- Create the record as a DNS TXT entry listing your sending servers, including your ESP and any other sending platforms.
- Keep it under 10 DNS lookups. Exceeding that limit causes the record to fail validation entirely.
- Merge multiple records into one. Two separate records for the same domain will both fail validation.

DKIM, proof the message was not altered

DKIM adds a cryptographic signature to every outgoing message. The receiving mailbox provider checks that signature against a public key published in your DNS records to confirm the message arrived unchanged and from an authorized sender.

- Generate a key pair in your ESP or email platform and publish the public key as a DNS TXT record.
- Rotate the key every six to twelve months. Most platforms can automate this.
- Use a 2048-bit key if your platform supports it. Older 1024-bit keys are considered weaker and some providers flag them.

DMARC, tells mailbox providers what to do with failures

DMARC builds on SPF and DKIM by telling receiving mailbox providers what to do when authentication fails: quarantine the message, reject it, or just report it. Start with a monitoring policy (`p=none`) so you can see what is being sent under your domain before you start blocking anything.

- Start with `p=none` to collect reports without affecting delivery.
- Move to `p=quarantine` and then `p=reject` once you are confident your legitimate mail is passing authentication.
- Set `rua=mailto:dmarc@yourdomain.com` to receive aggregate reports showing which sources are sending under your domain.

SECTION 4

How fast that data produces a warm-up

Warm-up is not a fixed schedule you can copy from someone else's playbook. The right pace depends on your list size, your category, and how your first few weeks of sends are performing. Three to six weeks is the typical range for most domains sending cold outreach, but the signals you are watching matter more than the calendar. If your open rates are holding and your bounce rate is low, you can move faster. If you see any reputation drop, slow down and let the data settle before you push volume back up.

Why warm-up addresses are the specific danger

Mailbox providers treat unknown domains with a default assumption of spam. Warm-up is the process of building enough sending history and engagement data to override that default. Skipping it or rushing it means your first campaign looks like a brand-new domain sending at scale, which is exactly what spam filters are designed to catch. The reputation you build during warm-up is what allows your campaigns to land in the inbox when you actually need them to.

What protecting the warm-up reputation looks like

Once your domain has a reputation worth protecting, the goal shifts from building it to not losing it. Bounces, spam complaints, and blacklist hits all feed into that score, and they can undo weeks of warm-up work in a few days if they are not caught early. Monitoring bounce rates, complaint rates, and blacklist status daily is the difference between a small problem you can fix and a domain you can no longer use.

The cost of a domain that's burned

Replacement costs are low: a new domain and a new IP can be set up in a few hours. The real cost is the warm-up time you start over from zero and the campaigns you miss while the new domain is being built. Keeping the current one healthy is almost always faster than starting over.

Recovering it with the tools that show provider data

Google Postmaster Tools shows how Gmail is treating your domain, including spam rate and reputation. Microsoft SNDS covers Outlook.com and Hotmail.com. Yahoo does not publish a comparable tool, so we infer Yahoo reputation from bounce rates and how your messages are being routed.

Why warm-up actually matters