

Email going to spam: 7-check triage

EngageMKTG | Checked 17 October 2026 | Planning and operational guidance; provider requirements and local policy may differ.

Check / completed	What to inspect
[] 1. Does authentication pass and align? (3 minutes)	Send a test message to a personal Gmail address. Open it, choose "Show original," and read the three lines: spf=pass, dkim=pass, dmarc=pass. Then check the domains next to them. The DKIM signing domain or the SPF domain must be your From domain (or a subdomain of it) for DMARC to pass. If any line says fail, softfail, temperror or none, you have found the problem. Common causes: an expired or rotated DKIM key, an ESP migration that left the old DNS records in place, an SPF record that now exceeds 10 DNS lookups (Microsoft flags this one explicitly), or a new sending subdomain that was never authenticated.
[] 2. What is your Gmail spam rate? (2 minutes)	Open Postmaster Tools. The rule is below 0.10% to be safe, never at or above 0.30%. If you are above 0.3%, Google will not offer mitigation until the rate "remains below 0.3% for 7 consecutive days." Look at the trend, not one day: a single spike after one send is a list problem; a slow climb over weeks is a content or frequency problem. Then open the Compliance status dashboard, which shows whether you meet each sender requirement.
[] 3. What changed in the last 14 days? (3 minutes)	List every change: a new segment (especially one that had not been mailed in months), a volume jump, a new sending domain or subdomain, a new template, a new link-tracking domain, a new ESP or IP pool, a DNS change, a domain renewal, a new team member with send access. The answer is usually in this list. A send to a dormant segment is the single most common trigger we see for a "sudden" spam problem on an otherwise compliant program.
[] 4. Did bounces or complaints spike on a specific send? (2 minutes)	In the ESP, sort recent sends by hard-bounce rate and complaint rate. A send with hard bounces above 2% or complaints above 0.1% is your culprit. Note its audience: that segment needs suppression and a different treatment, not another send.
[] 5. Content and links (2 minutes)	Check the links in the suspect email: URL shorteners, a tracking domain that differs from your From domain and has no reputation, links to a domain on a blocklist, or a link to a site that was recently compromised. Check for a sudden shift to image-only content or a template with broken HTML. Content is rarely the sole cause of a sudden drop, but a bad link can be.
[] 6. Blocklists and shared infrastructure (2 minutes)	Look up your sending IPs and domain on Spamhaus and a multi-blocklist checker. If you are on a shared IP pool at your ESP, check the ESP's status page and ask support whether the pool had an incident. Yahoo's permanent rejections explicitly include "IP listed by Spamhaus" as a cause.
[] 7. Unsubscribe mechanics (1 minute)	Confirm the one-click unsubscribe headers (List-Unsubscribe and List-Unsubscribe-Post) are present on marketing mail and that the visible unsubscribe link works without login. A broken unsubscribe turns people who would have left quietly into complaints.

Full guidance and source links: <https://engagemktg.com/knowledge/emails-going-to-spam-all-of-a-sudden>