

# Email Deliverability Audit Kit.

27 checks every business must complete  
before sending any email campaign.

**\$100K+**

Revenue Generated

**58%**

Avg Open Rate

**4+**

Years Exp.

**3**

Continents

## WHAT THIS KIT DOES

This is the exact 27-point checklist Laib Studios runs before every email campaign launch.

Work through each section to protect your domain reputation, improve inbox placement,  
and maximize ROI on every campaign you send.

**SECTION 01 · DOMAIN AUTHENTICATION**

Authentication is the foundation of email deliverability. Without it, your emails will be filtered or rejected regardless of content quality.

**DMARC record published and valid**

A DMARC record instructs receiving servers what to do with emails failing SPF or DKIM. Without it your domain is vulnerable to spoofing and your campaigns may be filtered entirely. Check at [mxtoolbox.com/dmarc](https://mxtoolbox.com/dmarc).

**SPF record configured correctly**

SPF lists which servers are authorized to send on your domain's behalf. A misconfigured SPF is one of the most common causes of inbox filtering. Validate at [mxtoolbox.com/spf](https://mxtoolbox.com/spf). Ensure you have not exceeded the 10 DNS lookup limit.

**DKIM signature active and passing**

DKIM adds a cryptographic signature to every email so receiving servers can verify authenticity. All major email platforms support DKIM setup. Verify your DKIM is passing using Google's toolbox or MXToolbox.

**DMARC policy set to p=quarantine or p=reject**

A p=none policy collects data but does not protect you. Move to quarantine or reject once you have verified all legitimate email streams are passing authentication checks.

**BIMI record configured (bonus)**

BIMI displays your brand logo next to your sender name in Gmail and Yahoo inboxes. It requires a passing DMARC policy at enforcement level and a Verified Mark Certificate from a trusted authority.

**SECTION 02 · DOMAIN AND IP REPUTATION**

Your sender reputation determines whether emails land in the inbox or spam folder. It takes months to build and days to destroy.

**Domain is not on any blacklist**

Check your sending domain and IP against major blacklists using MXToolbox Blacklist Check. A single blacklisting can devastate deliverability overnight. Monitor this weekly as a minimum.

**Sending IP has been properly warmed up**

New IPs must be warmed gradually — start with your most engaged subscribers and increase volume slowly over 4 to 6 weeks. Skipping warmup results in immediate filtering by Gmail and Microsoft.

**Sending domain is at least 30 days old**

Brand new domains have zero reputation. Google and Microsoft treat emails from new domains with extreme suspicion. Use a domain that has been active for at least 30 days before sending campaigns.

**Reverse DNS (PTR record) is configured**

Your sending IP should resolve back to your sending domain via a PTR record. Many receiving servers check this and may reject emails where it is missing or does not match.

## SECTION 03 · LIST HYGIENE

A clean list is more valuable than a large one. Sending to bad addresses and unengaged contacts is the fastest way to destroy your sender reputation.

**All invalid email addresses removed**

Hard bounces above 2% will get your account suspended on most platforms. Use NeverBounce or ZeroBounce to clean any list you have not sent to recently. Run a full list clean at least every 90 days.

**Unengaged subscribers suppressed or re-engaged**

Subscribers who have not opened or clicked in 90+ days drag down your engagement metrics. Run a re-engagement campaign first, then suppress non-responders from regular sends.

**Unsubscribes processed within 10 business days**

This is a legal requirement under CAN-SPAM. Most platforms handle this automatically, but verify your suppression lists are synced if you use multiple sending tools or CRMs.

**No purchased or rented email lists in use**

Purchased lists destroy sender reputation instantly. Every major platform prohibits them. Receiving servers detect unusual engagement patterns from cold lists immediately. Never use them under any circumstance.

**Double opt-in enabled where possible**

Double opt-in subscribers are more engaged, less likely to report spam, and more likely to convert. If you cannot use double opt-in, use confirmed opt-in at minimum to verify email addresses.

**Complaint rate is below 0.1%**

Monitor your complaint rate in Google Postmaster Tools and Yahoo Complaint Feedback Loop. If it exceeds 0.08% you must clean your list and review your content immediately to avoid filtering.

## SECTION 04 · EMAIL CONTENT AND DESIGN

Spam filters analyse your content in detail. Even a perfect technical setup can be undermined by content that triggers filtering.

**Subject line is under 50 characters**

Subject lines over 50 characters are truncated on mobile devices. Keep them concise and front-load the most important information. A/B test subject lines on every campaign send.

**No spam trigger words in subject or body**

Words like free, guaranteed, no risk, winner, and cash trigger spam filters. Scan your content before sending using Mail Tester at [mail-tester.com](https://mail-tester.com) to get a deliverability score.

**Plain text version included with every HTML email**

Every HTML email must have a plain text alternative. Emails sent without a plain text version are flagged as suspicious by many spam filters and email clients.

**Unsubscribe link is visible in every email**

This is legally required. The unsubscribe link must be clearly visible — not hidden in 6pt grey text — and must process the request within 10 business days under CAN-SPAM law.

**All images have descriptive alt text**

Over 60% of email clients block images by default. Every image must have descriptive alt text so your email is readable and functional even when images do not load.

**Email renders correctly on mobile devices**

Over 60% of emails are opened on mobile. Test every campaign on iOS Mail, Gmail app, and Outlook mobile before sending. Use Litmus or Email on Acid for comprehensive testing.

**Text to image ratio is at least 60% text**

Emails that are mostly images are penalized heavily by spam filters. Maintain at least 60% text content in your emails and avoid using a single large image as the entire email body.

**SECTION 05 · SENDING INFRASTRUCTURE**

How you send is as important as what you send. Inconsistent sending patterns and poor infrastructure configuration trigger spam filters.

**Sending volume is consistent day to day**

Sudden spikes in sending volume are a major red flag for spam filters. Maintain consistent daily sending volumes and use scheduled sending to distribute campaigns over time rather than sending all at once.

**Dedicated IP used for high-volume sending**

If you send more than 50,000 emails per month you should be on a dedicated IP rather than a shared pool. Shared IPs mean your reputation is directly affected by other senders' behaviour.

**Sending domain matches the From header domain**

The domain in your From address and the domain your emails are actually sent from must match. Mismatches are a significant spam trigger that immediately raises suspicion with receiving servers.

**Email authentication results monitored weekly**

Use Google Postmaster Tools and Yahoo Complaint Feedback Loop to monitor your domain reputation, delivery errors, and complaint rate. Set up alerts for any sudden drops in reputation scores.

**SECTION 06 · CAMPAIGN PERFORMANCE BENCHMARKS**

Track these metrics after every send. If your numbers fall below these benchmarks, act immediately before your reputation degrades further.

**Click-to-open rate is above 10%**

Click-to-open rate measures how many openers actually clicked. Below 5% means your content is not delivering on the subject line promise. Review your offer, copy, and call-to-action positioning.

**Hard bounce rate is below 2%**

Hard bounces above 2% will get your account suspended on most platforms. Clean your list before every large send and remove hard bounces immediately after every campaign.

**Soft bounce rate is below 5%**

Monitor soft bounces carefully and suppress addresses that soft bounce more than 3 times in a row. Consistently soft-bouncing addresses are often invalid or permanently unreachable.

**Revenue per email is tracked and improving**

Every campaign should have a measurable revenue outcome. Track revenue per email sent and revenue per recipient who opened to understand true ROI and optimize future campaign strategy.

**Google Postmaster Tools is set up and monitored**

Google Postmaster Tools provides direct insight into your domain reputation with Gmail. Set it up immediately if you have not already and monitor your reputation score and spam rate weekly.

# Need help implementing all of this?

That is exactly what Laib Studios does.

We build complete email marketing infrastructure, automation systems,  
and lifecycle flows that generate revenue on autopilot. From DMARC  
setup to Klaviyo flows — we handle everything.

**laibahassan945@gmail.com**

- AI-Powered Lead Capture and CRM Systems
- Shopify and E-commerce Development
- Growth Marketing — Meta Ads, Google Ads, SEO
- Web Development and Brand Identity

[laibstudios.com](https://laibstudios.com) · [linkedin.com/in/laiba1931](https://linkedin.com/in/laiba1931)