THE NO BS DELIVERABILITY PLAYBOOK

This is not a guide full of fluff, theory, or recycled advice from five years ago. This is the No BS Deliverability Playbook — the exact methods, tools, and pro tips that actually move the needle and get your emails seen, opened, and clicked.

The No BS

DELIVERABILITY

PLAYBOOK

Introduction

Let’s face it — it doesn't matter how great your offer is if your emails aren’t landing in the inbox. Whether you're running affiliate promotions, sending newsletters, or building out automated sequences, deliverability is everything. If your emails end up in spam, promotions, or never show up at all, you're leaving money on the table.

This is not a guide full of fluff, theory, or recycled advice from five years ago. This is the No BS Deliverability Playbook — the exact methods, tools, and pro tips that move the needle and get your emails seen, opened, and clicked.

In this playbook, you’ll learn:

- How to prepare and protect your domain reputation
- Which tools to use (and why) for inbox testing, blacklist monitoring, and hygiene
- The exact practices that top senders use to keep their emails in the primary inbox
- How to warm up domains, structure your sender identity, and write emails that don’t trigger spam filters
- Plus, a few advanced tricks to resurrect dead lists and build sender authority the smart way

If you're serious about getting results from email, this is where you start.

1: Domain Quality – The Foundation of Good Inboxing

1. Medium/High Sending Reputation Domain

Before you send a single email, you need to know the quality of the domain you're sending from. If your domain has a poor reputation, it doesn’t matter how good your copy is or how well you've warmed it up — your emails will land in Promotions, or worse... Spam.

How to Check Domain Reputation

Use **Google Postmaster Tools** – the only official insight Google provides into your email reputation.

🔗 https://postmaster.google.com/

Once your domain is verified via DNS, you’ll get access to key metrics like:

- **IP Reputation** – Reputation of your sending IPs.
- **Domain Reputation** – How much Google trusts your sending domain.
- **Spam Rate** – The percentage of your emails marked as spam by recipients.
- **Feedback Loop** – Engagement signals from Gmail users.

Pro Tip:

If your domain drops to *Low reputation*, STOP all sending immediately and begin recovery:

- Restart warm-up using platforms like **Mailwarm, Lemwarm, Instantly**, etc.
- Send a few hundred **high-quality emails** to real inboxes that open, click, and reply.
- Link your domain to **G Suite** and start sending manually to known contacts — encourage **replies**.

Important: Never start sending large volumes from a **new domain**. Google treats new domains with suspicion — a *cold start* problem. The goal is to teach Gmail (and other ESPs) that you’re a legitimate sender. As long as you maintain a **Medium or High reputation**, you have a real shot at hitting the inbox every time.

2. GlockApps – Real-Time Deliverability Diagnostics

Before you hit "Send" on your campaign, you need to know exactly where your emails are landing — **Inbox? Promotions? Spam? Trash?**

That's where **GlockApps** comes in — one of the most accurate tools for real-time deliverability testing.

🔗 https://glockapps.com/

What Does GlockApps Do?

When you send a test email to their **seed list** (a set of test inboxes across Gmail, Yahoo, Outlook, AOL, Zoho, and more), Glock shows you:

- Which **folder** your email lands in (Inbox, Promotions, Spam)
- Which **ESPs** are blocking or down-prioritizing your emails
- Whether **SPF, DKIM, and DMARC** are properly authenticated
- If your domain/IP is listed on **blacklists**

Free Trial

You get **3 free tests** when you sign up — perfect for testing multiple subject lines and content formats right away.

How to Use It:

1. Create a free account
2. Generate your seed list
3. Import the seed list into your email platform (e.g. Instantly, Lemlist)
4. Send a test campaign to those addresses
5. Analyze the report inside your GlockApps dashboard

Pro Tip:

Use Glock to run **A/B tests** on subject lines and preheaders. Sometimes, just **one emoji** or a sketchy-looking link is enough to push your email into the spam folder. Always test before sending to your main list.

3. SPF, DKIM & DMARC – Your Email’s Digital ID

If you don’t know what SPF, DKIM, and DMARC are, then sending email campaigns is like driving a car without license plates — it might work for a bit, but sooner or later, the system will shut you down.

These are **three DNS authentication records** that prove you're the rightful sender of emails from your domain. Without them, inbox providers won’t trust your messages — and you’ll end up in spam.

SPF – Sender Policy Framework

SPF tells email providers **which IP addresses and mail servers** are authorized to send on behalf of your domain. Without a valid SPF record, anyone can spoof your domain and damage your reputation.

Example SPF record:

```
v=spf1 include:_spf.google.com ~all
```

DKIM – DomainKeys Identified Mail

DKIM digitally **signs each email**, ensuring that the content hasn’t been altered in transit. The signature is verified through a **public key** in your DNS settings.

Example DKIM record (domain-level):

```
default._domainkey.yourdomain.com
```

DMARC – Domain-based Message Authentication, Reporting & Conformance

DMARC ties SPF and DKIM together and tells email providers **what to do if an email fails authentication** (reject, quarantine, or allow). It also gives you **reports** on attempted email spoofing using your domain.

Example DMARC record:

```
v=DMARC1; p=none; rua=mailto:report@yourdomain.com;
```

Where to Check If They're Working Correctly:

- GlockApps
- MailTester
- MXToolbox

Pro Tip:

- **SPF and DKIM are non-negotiable** — without them, you're almost guaranteed to hit the spam folder.
- **DMARC is strongly recommended** — it adds an extra layer of trust and protects your domain from spoofing.
- If you're using tools like **Instantly, Lemlist, G Suite**, etc., each of them will provide the DNS records you need to add. Just copy and paste those into your domain host (e.g., Cloudflare, GoDaddy, Namecheap).

---

4. Sender Identity – Your First Impression in the Eyes of Spam Filters

Your **sender email address** is the first signal email service providers (ESPs like Gmail, Outlook, etc.) use to determine **who you are** and whether you're a **real human or a spam machine**.

If you're using generic sender addresses like:

- admin@yourdomain.com
- info@yourdomain.com
- office@yourdomain.com
- contact@yourdomain.com

...there's a **high chance your email will go straight to Promotions or Spam**.

Why ESPs Dislike Generic Email Addresses:

- They're **overused** for bulk sending
- Lacking the **"human touch,"** — they look like automated systems
- Frequently used by **bots and blackhat spammers**
- Tend to have **low open rates**, which kills sender's reputation even more

The Fix: Use Personal Sender Addresses

Instead of faceless addresses, use **real, human-sounding email addresses** — ones that feel like a real person is reaching out.

Examples That Perform Way Better:

- mark@yourdomain.com
- tony@yourdomain.com
- michael@yourdomain.com
- team.mateja@yourdomain.com *(still okay if you need a team tone)*

Pro Tip:

- If you need to scale or rotate senders, create **multiple personal sender profiles** with names
- **Track performance (opens, clicks, replies)** by sender and kill off any underperformers
- Match your **subject line and preview text** to the personal tone
  (e.g. "Quick question", "Hey [Name] – saw this and thought of you...")

Warning:

Never send cold email campaigns from info@ or similar generic addresses. That's the equivalent of a 2010 SEO spammer — your inbox rate will tank no matter how good your copy is.

5. Domain Warm-Up – Build Your Reputation Before Sending Anything Serious

If your domain has no email-sending history, email service providers (Gmail, Outlook, Yahoo, etc.) will treat you as an **unknown sender** — which means:

- Increased risk of ending up in **Spam** or **Promotions**
- A **lower trust score**
- And in the worst case — **blacklisting**

That's why **warming up your domain is a non-negotiable step**.

What Does It Mean for a Domain to Be "Cold"?

- A **new domain** with **zero reputation**
- An **older domain** that hasn't sent emails in a while
- A domain that's been **previously flagged as spammy**

If you send a cold email campaign or a newsletter from a cold domain, ESPs will instantly flag it as suspicious.

How Does Domain Warm-Up Work?

The warm-up process **simulates real human email activity**. You send small volumes of emails to **verified inboxes**, where your emails:

- Get delivered to the **Inbox**
- Are **opened**
- Are **clicked**
- **Receive replies**
- And **aren't marked as spam**

These **positive engagement signals gradually build your domain's reputation**.

Tools for Automatic Warm-Up

Boxward

A dedicated warm-up service that automatically:

- Sends emails to other Boxward-controlled inboxes
- **Opens, replies**, and even **rescues emails from spam**

- Simulates organic engagement
- Provides a detailed **warm-up health score**

Instantly.io

A cold email platform with a **built-in warm-up module**:

- Adjustable daily email volume
- Auto-replies and smart timing
- Live deliverability stats
- Can connect multiple inboxes

Both platforms offer a fully **hands-off warm-up experience**.

How Long Does Warm-Up Take?

- **New domains**: at least **14–21 days**
- **Old domains** returning to use: **7–14 days**

Start with **5–10 emails/day**, gradually increasing to **30–50/day**.

How Do You Know Your Domain is Ready?

- You're hitting **80%+ Inbox rate** in GlockApps tests
- Google Postmaster Tools show a **"Medium" or "High" sender reputation**
- **No spam flags** or bounce issues
- Your emails get **opens, clicks, and replies**

Common Warm-Up Mistakes That Kill Your Reputation:

- Sending **too many emails too soon**
- Using **spammy or low-quality content**
- Sending to **unverified cold lists**
- Using **generic sender addresses** like info@ or admin@ (as mentioned earlier)

Pro Tip:

Even after you complete the warm-up, keep sending **engagement emails** (2–3 per week) to a seed list or trusted contacts, because **reputation decays 3x faster than it builds**.

6. Email List Hygiene – You're Not Just Sending to People, You're Sending to Your Reputation

There's a saying:

> "If you send to the garbage, you'll be treated like garbage."

And it couldn't be more true.

Even if your list is just 3 months old, if you haven't **validated** it, you're a **spam filter risk**. Why? Because ESPs (Gmail, Outlook, etc.) look at:

- **High bounce rates**
- **Dead inboxes** (nonexistent emails)
- **Spam traps** (emails set up to catch spammers)
- **Low engagement contacts**
- **Role-based emails** (info@, support@, etc.)
- **Spam complaints**

All of this **kills your sender reputation** and lands you in the spam folder — a place that's hard to escape from.

How Often Should You Clean Your List?

At **minimum, once every 2–3 months**, but ideally:

- Before every major send
- If you see a sudden drop in open rates
- If your bounce rate goes over 3%
- **Mandatory** if you use purchased, scraped, or old lists

Best Email List Cleaning Services:

NeverBounce

- Fast, accurate, with real-time API validation
- Flags invalid, role-based, and catch-all emails
- Claims **"97% deliverability guaranteed"** after cleaning

ZeroBounce

- Removes spam traps, abuse emails, and toxic domains
- Detects known complainers and dangerous contacts
- Great for **enterprise teams** with large databases

Debounce.io

- Budget-friendly and quick
- Ideal for smaller teams and fast processing
- Categorizes results: **valid, invalid, risky, unknown**

What Makes a List “Dirty”?

- Emails that **never open** your content
- **Spam traps** and honeypot addresses
- **Dead domains** (no longer exist)
- **Catch-all domains** with high bounce risk
- **Role-based emails** (info@, support@, admin@, etc.)

Pro Tip

- Monitor engagement: if someone hasn’t opened in **30, 60, or 90 days**, remove them or move them into a **re-engagement campaign**
- Use **double opt-in** when building a fresh list
- **Never send cold campaigns without cleaning the list first**

Pre-Sending Checkup: MailTester + MXToolbox – Your Deliverability X-Ray

Before you even *think* about launching a campaign, you need to know:

- Does your email pass SPF/DKIM/DMARC authentication?
- Do your links look spammy?
- Has your domain or IP landed on any blacklists?
- Are you “clean” in the eyes of spam filters?

That’s why you need these two tools:
👉 MailTester.com
👉 MXToolbox.com

1. MailTester – Quick Health Check for Your Email

How it works:

1. Go to Mail-Tester.com
2. You'll get a unique test email address (e.g., `test-q8w3t@mail-tester.com`)
3. Send your campaign or test email to that address
4. You'll receive a score from 0 to 10, based on:

✅ SPF / DKIM / DMARC validation
✅ Blacklist status
✅ Spam-trigger words in your message
✅ Email code quality (HTML structure)
✅ Images, links, unsubscribe link
✅ Gmail tab classification (Inbox vs Promotions)

If your score is below 8.5 – DO NOT send the campaign until it's fixed.

2. MXToolbox – Your Blacklist Radar

MXToolbox Blacklist Check scans whether:

- Your **domain**
- Your **sending IP**
- Or even your **email platform**

...have landed on any of **100+ major spam blacklists**, such as:

🚫 Spamhaus
🚫 SORBS
🚫 UCEPROTECT
🚫 Barracuda
🚫 And many more

If you're listed, your inbox rate is already dropping. You'll need to:

- Open a support ticket to request **delisting**
- **Pause sending** temporarily
- **Switch to a new IP/domain** if the reputation is beyond repair

When Should You Use These Tools?

- Before **EVERY major send**
- After completing your **warm-up phase**
- If you notice a drop in open/click rates
- When **GlockApps** shows poor inboxing
- When your **Google Postmasters** reputation drops

Pro Tip:

- Use **MailTester** to test different subject lines, links, and layouts – and see which version scores the highest.
- Use **MXToolbox Pro** to **automate blacklist monitoring** – it will notify you the moment you get listed.

---

7. Copywriting: Spam Trigger Words – More Words = Lower Deliverability

What are spam trigger words?

They're words frequently used in spam campaigns – especially in finance, health, sex industry, and affiliate marketing. When you use them, filters instantly raise red flags and push your emails to:

The **Promotions tab**
The **Spam folder**
Or block them entirely before delivery

❌ A Quick List of Words Affiliate Senders MUST Avoid:

Finance & Affiliate (high risk):

- make money
- earn $$$
- cash now
- fast income

- get rich
- passive income
- instant profit
- big payout
- money-back
- free access
- limited time offer
- act now
- no risk
- investment opportunity

Currency & Symbols (major triggers):

- $
- €
- £
- % OFF
- 100% free
- GUARANTEED

Aggressive or scammy CTAs:

- Click here now
- Buy direct
- Claim your prize
- Apply now
- Order today

How to Avoid Them?

Instead of:

"Make money online with this passive income system."

✅ Write: *"Discover a system designed to help you build recurring digital revenue."*

Instead of:

"Earn $5000/month fast!"

✅ Write: *"See how digital creators are generating recurring revenue streams."*

Instead of:

"Get instant access to a FREE affiliate system"

✅ Write: *“Explore our access-based platform for digital marketers – no upfront cost required.”*

Pro Tips:

- Use **only one call-to-action per email**
- **Never bold multiple sentences in a row**
- Use **storytelling and narrative** instead of aggressive sales pitches
- For **cold outreach**, send **plain-text emails with no images or links**
- Gmail prefers a **personal, short, human-like tone**

Remember:

Spam filters no longer look at just words – they analyze context, structure, and engagement too. But these words are still red flags. If you’re sending **cold** or **affiliate** emails, it’s safest to avoid them **entirely**.

PRO TIP #9: “Silent Warm-Up” – reply-focused campaigns without links

When you have:

📉 An email list you haven’t touched in a while
📉 Open rates below 15–20%
📉 Suspicion that you’ve landed in the promo/spam tab
📉 Or you’ve uploaded an old list from a hard drive...

DON’T immediately jump in with:
“Check out my offer!” → link → spam folder

Instead, send 2–3 **linkless**, **reply-focused** campaigns.
No CTAs, no links, no images — just plain text.

Example 1: Friendly Check-in

Hey [Name],

It’s been a while since I last reached out, but if you’re still active in [niche], I have a few things that might be useful.

Just reply “yes” if you want me to send you more details.

Cheers,
[Your Name]

Example 2: Micro Survey

Hey [Name],

I’m working on an internal update and wanted to ask:

👇 What’s your biggest challenge right now in [niche]?

Just reply with one sentence — I read every reply.

Thanks!

Why this WORKS:

- Engagement is the top signal for Gmail/Outlook
- When people reply to your email, you’re not spam — you’re a conversation
- **Replies > Clicks** in ESP eyes
- Replies are seen as friendly, organic exchanges
- Raising reply rates builds your sender reputation
- After 2-3 campaigns like this, your domain comes out of “cold mode” and gets the green light for serious sending
- You can reactivate “ghost” subscribers who stopped clicking/opening — some might reply, letting you re-engage them

Rules for this type of campaign:

- No links
- Keep it short and plain text

- Direct reply CTA (ask them to reply, not to click)
- Questions must be simple and human
- Use personalization in the subject line if possible

After 2–3 of these campaigns and some replies, you can send your next email with a link (but cautiously, avoiding trigger words).

This technique is like, instead of banging on the door, you quietly whisper the person's name and wait for them to open it themselves.

---

10. Use a Subdomain for Sending, Root Domain for Authority

If you're sending cold campaigns, newsletters, or mass emails — **never send directly from your root domain.**

Why?

The root domain (e.g., yourbrand.com) is your main domain used for:

- Website
- Business reputation
- SEO and brand presence
- Important communications (clients, support, etc.)

If you compromise it (reputation drops, you get blacklisted), everything else suffers.

That's why you use a dedicated sending subdomain.

Examples:

- mail.yourbrand.com
- news.yourbrand.com
- updates.yourbrand.com
- connect.yourbrand.com

How to set it up in practice?

- Create a subdomain in your DNS (e.g., mail.yourbrand.com)
- Set up SPF, DKIM, and DMARC records specifically for that subdomain
- Send all cold/newsletter campaigns from that subdomain
- Monitor reputation using Postmaster Tools, GlockApps, MailTester, MX Toolbox — all tracking the subdomain

Benefits:

- You warm up and build a reputation independently of the root domain
- If reputation drops, → only the subdomain is affected
- You can rotate multiple subdomains without damaging your brand
- Gmail and other ESPs track reputation by subdomain, not the root domain

Bonus: If you have multiple brands or clients, you can assign a separate subdomain for each, giving you modular control.

Examples:

- news.client1.com
- mail.client2.com
- outreach.client3.com

This practice provides a long-term shield and scalability without risking the domain that puts bread on your table.

Conclusion

Inbox deliverability isn’t just a technical issue — it’s a combination of strategy, reputation, behavior, and constant testing.
If you ignore even one of the points in this document, you risk your entire campaign ending up in the promo or spam folder.

But if you regularly:

- Clean your list
- Test your emails
- Write in a human, non-salesy way
- Build engagement instead of just blasting messages
- Monitor your reputation and use subdomains

You’ll be in the top 5% who don’t ask, “Why is my open rate dropping?” — but instead **know exactly what they’re doing.**

🎯 Email is alive. Algorithms are smart. Play smarter.