Email Health Audit Worksheet

A checklist for nonprofit organizations to diagnose and fix email deliverability problems.

missiontechadvisors.com

How to use this worksheet

Work through each section in order. Check off items as you confirm them. Any item you cannot check off is a potential cause of deliverability problems. Pay special attention to Section 1 (DNS Records) — missing records here are the most common root cause.

Status Key

✓ Pass — Configured correctly
✕ Fail — Needs attention
? — Not sure / needs checking

Section 1: DNS Authentication Records

These three DNS records tell receiving mail servers that your emails are legitimate. Missing even one can significantly hurt deliverability. Check each using a free online tool.

- [ ] **SPF Record exists and is valid**
  Your SPF record should list every service that sends email on behalf of your domain (Google Workspace, Mailchimp, your website host, etc.). If a sending service is not listed, its emails may be rejected.
  Tool: MXToolbox.com > SPF Record Lookup

- [ ] **SPF record covers all sending platforms**
  Common services to include: Google Workspace (include:_spf.google.com), Mailchimp (include:servers.mcsv.net), your web host. Check your email platform's documentation for the correct include statement.

- [ ] **DKIM configured for Google Workspace / primary email**
  In Google Admin > Apps > Google Workspace > Gmail > Authenticate email, generate and publish your DKIM key. Verify it is active and passing.
  Tool: Google Admin Console > Gmail > Authenticate email

- [ ] **DKIM configured for each email platform (Mailchimp, etc.)**
  Each sending platform needs its own DKIM record. In Mailchimp: Account > Domains > verify your domain and add the provided CNAME/TXT records. Check each platform you use.
  Tool: Each platform's domain verification settings

- [ ] **DMARC record exists**
  At minimum, a basic monitoring policy should be in place: v=DMARC1; p=none; rua=mailto:dmarc@yourdomain.org. This tells mail servers what to do with authentication failures and sends you reports.

  Tool: MXToolbox.com > DMARC Lookup

- [ ] **DMARC policy is appropriate for your situation**
  p=none (monitoring only) is a safe starting point. Once you have verified all legitimate sending sources are authenticated, consider moving to p=quarantine or p=reject. Do not move to a strict policy until all platforms are properly authenticated.

Section 2: Email Platform Settings (Mailchimp / ActiveCampaign / etc.)

- [ ] **Sending "From" address uses your custom domain**
  You should never send campaigns from a Gmail, Yahoo, Hotmail, or other free email address. These providers' DMARC policies actively block other platforms from sending as them. Use yourname@yourorganization.org.

- [ ] **Sending domain is verified in your email platform**
  Most platforms (Mailchimp, ActiveCampaign, etc.) require you to verify your sending domain. This involves adding DNS records they provide. Check your platform's domain settings to confirm the domain is verified and authenticated.

  Tool: Platform account settings > Domains

- [ ] **Physical mailing address is included in every email**
  CAN-SPAM and CASL require a physical address in every commercial/marketing email. Most platforms will block sending if this is missing. Use your organization's address or a P.O. Box.

- [ ] **Unsubscribe link is present and functional**
  Required by law. Test it. Confirm that unsubscribes are processed promptly and that unsubscribed contacts are not re-added to your list accidentally.

- [ ] **Double opt-in is enabled (recommended)**
  Double opt-in requires new subscribers to confirm their email address before being added to your list. This reduces bounces and spam complaints significantly.

Section 3: List Hygiene

A clean list protects your sender reputation. High bounce rates and spam complaints are among the fastest ways to damage deliverability.

- [ ] **Inactive contacts have been identified**
  Segment contacts who have not opened or clicked any email in the past 12 months. These contacts hurt your engagement metrics and may increase spam complaints.

- [ ] **Re-engagement campaign sent to inactive contacts**
  Before removing inactive contacts, send a re-engagement campaign asking if they still want to hear from you. Remove those who don't respond.

- [ ] **Hard bounces are removed promptly**
  Hard bounces (permanently undeliverable addresses) should be removed immediately. Most platforms do this automatically, but verify your bounce handling settings.

  Tool: Platform > Audience > Manage contacts

- [ ] **No purchased or scraped email lists in use**
  Purchased lists are a fast path to being blacklisted. Every contact on your list should have explicitly opted in to receive emails from your organization.

- [ ] **List is segmented for relevant targeting**
  Sending highly relevant emails to engaged segments improves open rates and reduces spam complaints — both of which improve your sender reputation over time.

Section 4: Domain Reputation Monitoring

- [ ] **Google Postmaster Tools is set up for your domain**
  Google Postmaster Tools gives you direct insight into how Gmail views your sending reputation. It shows your domain reputation score, spam rate, and authentication results. Free — set it up at postmaster.google.com.

  Tool: postmaster.google.com

- [ ] **Domain reputation is "High" or "Medium" in Postmaster Tools**
  Low or Bad reputation means Gmail is actively filtering your emails to spam. Recovery requires sending only to engaged contacts, removing inactive addresses, and giving reputation time to rebuild.

- [ ] **Spam rate is below 0.10% in Postmaster Tools**
  Google recommends keeping spam complaint rate below 0.10%. Above 0.30% will cause significant deliverability issues. Monitor this metric monthly.

- [ ] **Domain is not on any email blacklists**
  Check your domain and sending IP against common blacklists. A listing means ISPs may be blocking your email entirely.

  Tool: MXToolbox.com > Blacklist Check

- [ ] **Sending volume is consistent (no sudden spikes)**
  Suddenly sending 10x your normal volume is a spam signal. If you need to scale up volume (e.g., for a major campaign), warm up gradually over several weeks.

Section 5: Website / Transactional Email

Transactional emails are the automatic emails your website sends — contact form notifications, confirmations, receipts. These are often overlooked but can damage your domain reputation if not properly configured.

- [ ] **Website is not using shared hosting's default mail server**
  Most shared hosting mail servers have poor reputation and no dedicated authentication. Use a dedicated sending service instead.

- [ ] **A dedicated email sending service is configured (SMTP)**
  Recommended options: Amazon SES (very affordable, excellent deliverability), Mailgun, SendGrid, Postmark. Configure your CMS (WordPress, etc.) to route all outgoing email through this service.

  Tool: WordPress: Gravity SMTP, WP Mail SMTP, or FluentSMTP plugin

- [ ] **Sending service is authenticated (SPF/DKIM added to DNS)**
  Your chosen sending service will provide DNS records to add. This authenticates emails sent through their servers as legitimately coming from your domain.

- [ ] **Test emails are landing in inbox (not spam)**
  Send test emails to Gmail, Outlook, and Yahoo accounts. Check both inbox delivery and full email headers to confirm authentication is passing.

  Tool: mail-tester.com — gives you a deliverability score and diagnosis

Audit Summary

Section	Items Checked	Items Passing	Priority
1. DNS Authentication Records	/6		Critical
2. Email Platform Settings	/5		High
3. List Hygiene	/5		High
4. Domain Reputation Monitoring	/5		Medium
5. Website / Transactional Email	/4		Medium
TOTAL	**/25**		

Not sure what to do next?
If you've worked through this worksheet and still have unresolved issues — or if your domain reputation is already damaged — we can help. Mission Tech Advisors works with nonprofits to diagnose and fix email deliverability problems, configure sending infrastructure, and get your communications reaching your donors and supporters reliably.

Schedule a free consultation:
missiontechadvisors.com/contact

Email:
ebooth@missiontechadvisors.com