

The email deliverability checklist for Microsoft 365

Key takeaways

- Email deliverability is whether your mail reaches the inbox instead of the spam folder. This checklist covers five areas: DNS authentication (SPF, DKIM, DMARC, MX), email signature hygiene, sending infrastructure, monitoring, and maintenance.
- Fix DNS authentication first: DMARC checks alignment against SPF and DKIM, so without at least one of them correctly set up, DMARC has nothing to enforce.
- If you deploy email signatures server-side, confirm DKIM is re-signed by Microsoft 365 after the email signature is applied; signing before it breaks authentication.
- Work down the list below, tick what's true today, and treat anything unchecked as your backlog.

1 Is your DNS authentication set up correctly?

- ☐ SPF record published and valid, with no more than 10 DNS lookups.
- ☐ DKIM enabled in Microsoft 365, with at least one active selector.
- ☐ DMARC record published, even at p=none, so you can monitor before you enforce.
- ☐ Every legitimate third-party sender confirmed aligned to your From domain, by SPF or DKIM, before enforcing DMARC.
- ☐ MX records correct and pointing to Exchange Online.
- ☐ If email signatures are deployed server-side, DKIM re-signed by Microsoft 365 after the email signature is applied.

Where Exclaimer fits

Exclaimer's cloud solution applies email signatures inside Microsoft's mail flow. For server-side deployment, your SPF record needs Exclaimer's include mechanism added, with the exact value depending on your region; that's what the SPF item above covers, not a separate step. DKIM and DMARC need no changes on Exclaimer's part: Exclaimer strips the existing DKIM signature on receipt and inserts the email signature, then Microsoft 365 re-applies DKIM before the message goes out, so authentication there keeps passing.

2 Is your email signature hygiene clean?

- ☐ Each image 50KB or less, with contact details in real text rather than baked into one image.
- ☐ Banner and logo images hosted externally over HTTPS, not embedded as base64 in the email signature HTML.
- ☐ Tracking links use full, branded destination URLs, not link shorteners.
- ☐ UTM tags preferred over redirect-based tracking. If you redirect, point the tracking domain at your own with a CNAME.
- ☐ Distinct external domains per email kept modest, and banner and link domains have a positive reputation.

Where Exclaimer fits

Exclaimer manages email signature images and campaign banners centrally, so IT controls exactly which domains ride on every email. Nobody is pasting an oversized logo in by hand or linking a redirect nobody's checked.

3 Is your sending infrastructure ready?

- ☐ Warm-up complete for any new sending domain or IP.
- ☐ Sender reputation baseline established and monitored on an ongoing basis (Google Postmaster Tools for Gmail, Microsoft SNDS for Outlook.com).
- ☐ Bounce rate tracked, and spam complaint rate kept under 0.1%.

4 Are you monitoring the right signals?

- ☐ DMARC aggregate reports reviewed monthly.
- ☐ Inbox placement tested against major providers, including Google, Microsoft, and Yahoo.
- ☐ Microsoft 365 Message Trace used to troubleshoot delivery issues.
- ☐ Authentication-Results header read on a test message first, whenever placement drops.

5 Is your maintenance schedule up to date?

- ☐ SPF lookup count audited quarterly.
- ☐ DKIM keys rotated at least annually.
- ☐ DMARC policy stepped from p=none through p=quarantine to p=reject, each move made only once reports show every legitimate sender aligned.
- ☐ Email signature templates reviewed for deliverability hygiene after any major campaign or branding update.

Where Exclaimer fits

Email signature templates and banners live in one place, so a hygiene fix is a single controlled change across every user and device, not a mailbox-by-mailbox chase.

After the audit

Fix DNS authentication first. The rest of this checklist only pays off once your mail is authenticated. Re-run the full audit after any major change to your senders, sending domains, or email signature templates.

See how Exclaimer keeps email signatures deliverability-safe

Centralize signature and banner management so the hygiene this checklist covers stays consistent, without a manual audit.

Trusted by 80,000+ organizations worldwide

exclaimer.com