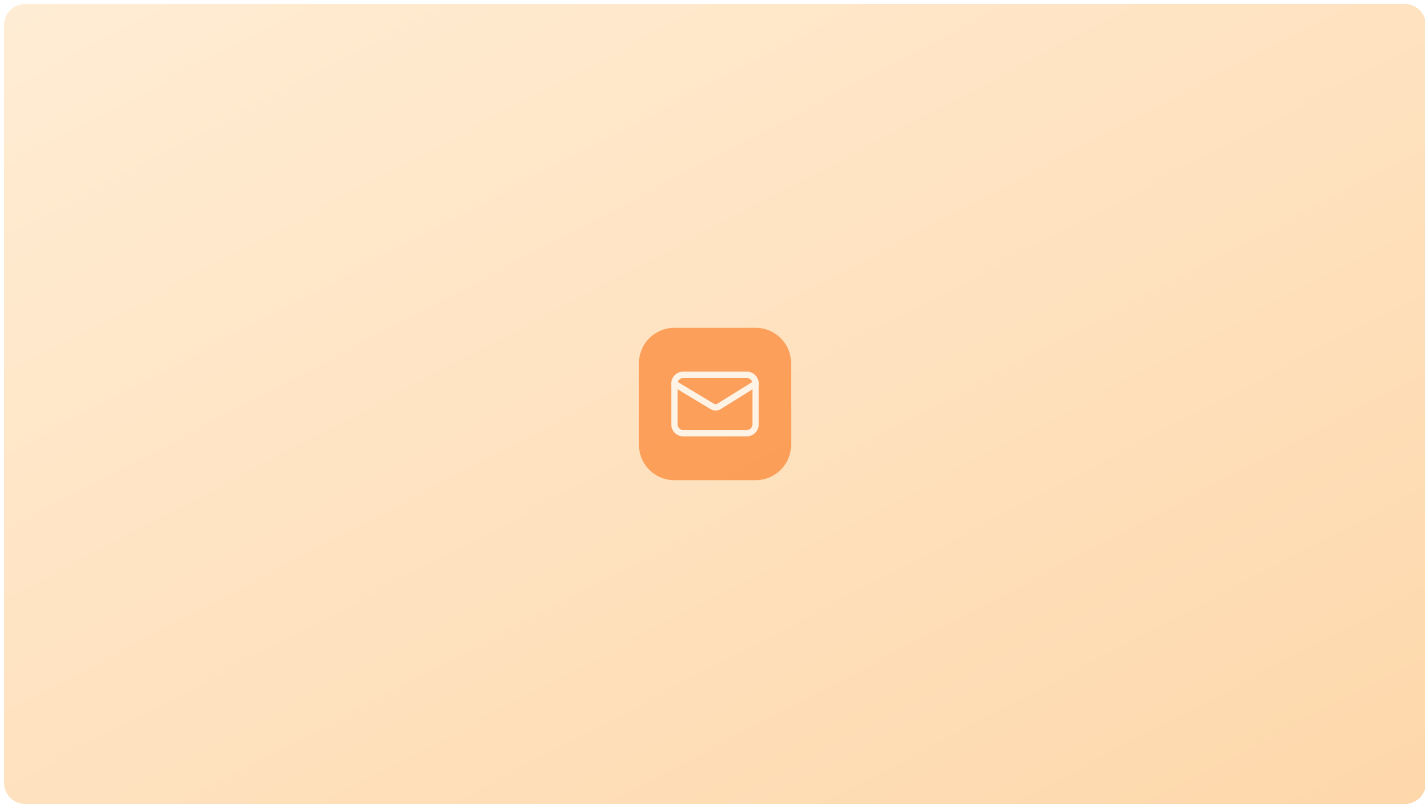
URTRAVELPRO



MARKETING

Sending Domains

Verify your own email domain (DKIM + Return-Path) so campaigns send from your address instead of a shared default. Better deliverability, better trust.

Prepared by Terrance Bortell · May 16, 2026

On this page

A sending domain is the email domain (the part after the @) that your campaigns are sent from. Verifying your own domain (e.g., `youragency.com`) instead of using a shared default dramatically improves deliverability and lets your contacts see emails from `hello@youragency.com` instead of a generic UrTravelPro address.

Why Verify a Sending Domain?

- **Trust** — your contacts see emails from your real domain, not a third-party one
- **Deliverability** — your reputation is your own, not pooled with other senders. Bad behavior by another sender on a shared domain can hurt your inbox placement; with your own domain, you're isolated.
- **Brand consistency** — `noreply@youragency.com` looks professional. `noreply@marketing.urtravelpro.com` does not.
- **Compliance** — modern anti-spam standards (DMARC, BIMI) require domain alignment between the From address and the authenticated domain.

How Verification Works

Marketing uses two DNS-based authentication standards:

- **DKIM** (DomainKeys Identified Mail) — Marketing signs every outbound message with a private key; the matching public key lives in your DNS as a TXT record. Receiving servers verify the signature against your DNS.
- **Return-Path** (a.k.a. envelope-from / MAIL FROM) — bounces and complaints route to a Marketing-managed subdomain of yours so we can process them correctly. Configured via a CNAME record.

Both are added as DNS records at your domain registrar (GoDaddy, Namecheap, Cloudflare, Google Domains, etc.). Marketing gives you the exact records to add and verifies them automatically once propagated.

Step-by-Step

1. Go to **Sending Domains** → **Add Domain**.

2. Enter your domain (e.g., `youragency.com` — just the bare domain, no `www.`).
3. Marketing displays 3 DNS records to add: 1 DKIM TXT, 1 DKIM TXT (second selector), and 1 Return-Path CNAME.
4. Log into your DNS registrar and add each record exactly as shown — copy/paste the host (`name`) and value (`points to` / `content`).
5. Wait for DNS propagation. This usually takes minutes but can take up to 48 hours depending on your registrar.
6. Back in Marketing, click **Verify**. Once all three records are detected, the domain is marked **Verified** and available for sending.

Using a Verified Domain

Once verified, the domain appears in the **From address** dropdown when creating a campaign. You can send from any address at that domain — `hello@`, `support@`, `newsletter@`, `info@youragency.com`. Marketing doesn't require the address to exist as a real inbox (though we recommend it does, so contacts can reply).

> **ADVISOR TIP**
>
> Set up a `replies@` or `hello@` address as a real inbox before sending campaigns from it. Replies that bounce back create a bad experience for engaged contacts who took the time to write to you.

DNS Quick Reference by Registrar

- **Cloudflare** — DNS tab → Records → Add Record. Set Proxy status to "DNS only" (gray cloud) for CNAME records.
- **Namecheap** — Advanced DNS tab → Add New Record.
- **GoDaddy** — DNS Management → Add. Choose the record type, paste host and value.
- **Google Domains** (now Squarespace) — DNS → Manage custom records → Create new record.

Troubleshooting Verification

- **"Records not found"** — DNS may still be propagating. Wait 1-4 hours and re-verify.
- **"DKIM record exists but doesn't match"** — most often a typo in the record value (CRLF, extra spaces, or partial paste). Re-copy the value from Marketing and re-paste.
- **"Return-Path CNAME conflicts"** — your registrar already has a CNAME at that hostname. Delete the conflicting record (usually a default Park or Forwarding entry).

- **Cloudflare-specific** — make sure the proxy status (the orange/gray cloud) is set to "DNS only" gray cloud, not proxied orange cloud. Proxied DNS breaks DKIM.
