# DKIM, SPF, DMARC in Plain English

## Why This Stuff Matters

You can have great offers and smart funnels, but if your emails land in spam, your numbers lie. Deliverability is how you get a fair shot: inbox placement first, persuasion second.

## DNS, Briefly (and Why Your Web & Email Don’t Need the Same Provider)

**DNS (Domain Name System)** is the Internet’s phone book. It translates human-friendly names (like `yourdomain.com`) into the technical details services need (like IP addresses and routing rules). Your *nameservers* host a “zone file” for your domain, which contains individual records.

**Common DNS record types you’ll touch:**

- **A / AAAA:** Point a name to an IP address (A = IPv4, AAAA = IPv6). Example: send web traffic to your web server.
- **CNAME:** Alias one name to another name (no IP). Handy for `www` ? `@` or vendor-hosted subdomains.
- **MX:** Tell the world where to deliver *incoming* email for your domain.
- **TXT:** Free-form text. Used for SPF, DMARC, DKIM (sometimes), site verifications, etc.
- **CAA:** Limit which certificate authorities can issue SSL/TLS certs for your domain (optional but good hygiene).

> **Key idea:** Your *registrar* (where you bought the domain) can be different from your *DNS host* (where your nameservers live), which can be different from your *web host* and your *email provider*. DNS simply “routes” each service to the right place.

### Example: Split Web + Email + Sending Service

Here’s a simple, realistic zone (abbreviated) showing web hosting, Google-style MX, and email authentication records for a sending platform:

Copy

```
; Nameservers are set at your registrar to your DNS host (e.g., ns1.dnsprovider.com,
ns2.dnsprovider.com)

@             A       198.51.100.10           ; Website lives on your web host (IPv4)
```

```
www             CNAME   @                       ; www ? root

; Email routing (incoming mail ? your email provider)
@               MX      1   ASPMX.L.GOOGLE.COM.
@               MX      5   ALT1.ASPMX.L.GOOGLE.COM.
@               MX      5   ALT2.ASPMX.L.GOOGLE.COM.

; SPF (who's allowed to send as you)
@               TXT     "v=spf1 include:_spf.google.com include:mailgun.org ~all"

; DKIM (depends on your provider: TXT or CNAME records they supply)
mail._domainkey         TXT    "v=DKIM1; k=rsa; p=MIIBIjANB..."   ; Example TXT-style DKIM
; or sometimes:
selector1._domainkey    CNAME  selector1.vendor._domainkey.yourdomain.com.

; DMARC policy + reporting
_dmarc          TXT     "v=DMARC1; p=none; rua=mailto:dmarc@yourdomain.com; fo=1"
```

**What this means:**

- Your **website** can live on WebHostCo (A/AAAA records to their IPs).
- Your **email inboxes** can live on a different provider (MX records to Google, Microsoft, Fastmail, etc.).
- Your **email sending tool** (ESP) can sign and authenticate mail via SPF/DKIM/DMARC—also independent of web hosting.

### Practical tips

- **Don't put a CNAME at the root** (`@`)—use A/AAAA (or ALIAS/ANAME if your DNS host supports it).
- **SPF lookup budget:** Keep SPF under ~10 DNS lookups (includes, redirects). Remove old vendors.
- **Alignment matters:** Use a custom sending domain/subdomain (e.g., `mail.yourdomain.com`) so DKIM and From: align.
- **TTL & propagation:** DNS changes are cached. Lower TTL (e.g., 300s) before big moves; expect gradual propagation.
- **Change control:** When you add a new tool that sends as you, update SPF/DKIM *before* your first large send.

If your DNS feels tangled—or you're juggling multiple vendors—use the sequence in this guide to get SPF/DKIM/DMARC right. If inbox placement is still poor after alignment, that's a good time to read about when to hire an email deliverability consultant.

---

## The Big Three: simply explained

- **SPF (Sender Policy Framework):** A DNS record that lists which services are allowed to send mail for your domain (e.g., your ESP, your help desk). Think "authorized senders list."
- **DKIM (DomainKeys Identified Mail):** A cryptographic signature added to each email by your sending platform. Receivers verify the signature using a public key in your DNS. Think "tamper-proof seal."

- **DMARC (Domain-based Message Authentication, Reporting & Conformance):** A policy that tells inboxes what to do if SPF/DKIM don't align with your visible "From:" domain (monitor, quarantine, or reject) and where to send reports. Think "rules + reporting."

# What to fix first: order of operations

1. **Inventory senders:** List everything that sends mail as *you* (ESP, CRM, support desk, billing, marketing tools).
2. **Set/repair SPF:** Add each legitimate sender to your SPF record. Keep it under ~10 DNS lookups to avoid "permerror."
3. **Enable DKIM for each sender:** Most platforms give you one or more DNS entries (CNAME or TXT) to publish. Turn it on, then verify.
4. **Add DMARC at `p=none`:** Start in monitoring mode to get reports without breaking mail. Watch for failures.
5. **Align domains:** Make sure the domain in DKIM and/or SPF *matches* your visible From: domain (or subdomain). Once alignment looks good, tighten DMARC to `quarantine` then `reject`.

# Plain-English examples (edit the placeholders)

### SPF (TXT at your root domain)

Copy

```
v=spf1 include:_spf.your-email-platform.com include:sendgrid.net ip4:203.0.113.25 ~all
```

*Notes:* Use `include:` for each platform. Avoid chains that create more than ~10 DNS lookups. `~all` (softfail) is safer than `-all` while you're auditing.

### DKIM (usually CNAMEs your provider gives you)

Copy

```
selector1._domainkey.yourdomain.com CNAME selector1.yourplatform._domainkey.yourdomain.com
selector2._domainkey.yourdomain.com CNAME selector2.yourplatform._domainkey.yourdomain.com
```

*Notes:* The `selector` name comes from your platform. You don't write the key by hand—publish what they provide and verify inside the platform.

### DMARC (TXT at `_dmarc.yourdomain.com`)

Copy

```
v=DMARC1; p=none; rua=mailto:dmarc@yourdomain.com; ruf=mailto:dmarc@yourdomain.com; fo=1;
sp=none
```

*Notes:* Start with `p=none` to monitor. `rua` = aggregate reports. `ruf` = forensic (some providers limit these). After alignment is clean, move to `p=quarantine` then `p=reject`.

## Alignment: the part most people miss

Inboxes check whether the authenticated domain (from SPF/DKIM) *aligns* with the visible From: domain. If you send as `hello@yourdomain.com` but DKIM signs as `yourplatformmail.com`, that's a mismatch. Fix by using a custom sending domain/subdomain (e.g., `mail.yourdomain.com`) so DKIM and From: live under the same parent domain.

## Common Gotchas and Quick Fixes

- **Too many SPF lookups:** Consolidate vendors; use vendor-recommended includes; remove old tools.
- **Forgot a sender:** Support desk, billing, or a stray plugin still sends as you. Add them to SPF/DKIM or change their from-domain.
- **New vendor, no DNS update:** Whenever you add a sending tool, set up DKIM and update SPF *before* your first big send.
- **DMARC too strict too soon:** Don't jump straight to `reject`. Monitor first, fix alignment, then tighten.
- **Mixing shared and dedicated IPs without warming:** Warm gradually; watch engagement; don't spike volume.

## When to Bring in a Pro

If inboxing is poor across major providers after you follow the sequence above, or if you're prepping a high-stakes launch and can't babysit logs, get help. Here's a straightforward guide on when to hire an email deliverability consultant.

## Quick-Start Checklist:

1. List all services that send mail as your domain.
2. Publish/clean up your SPF record (stay under ~10 lookups).
3. Enable DKIM for every legitimate sender; verify inside each tool.
4. Add DMARC at `_dmarc.yourdomain.com` with `p=none` and a monitored mailbox.
5. Confirm alignment: DKIM/From: domains should match (or be subdomains).
6. Watch DMARC reports; fix failures; then step to `quarantine` ? `reject`.
7. Re-check after vendor changes, domain moves, or DNS edits.

---

# FAQs About SPF, DKIM, and DMARC

### Do I need both SPF and DKIM?

Yes. DMARC relies on at least one aligned pass (SPF or DKIM). Having both gives you redundancy.

### Is a dedicated IP required?

No. Reputation and consistent engagement matter more than IP ownership. Many brands do great on shared pools managed by reputable ESPs.

### How long until results improve?

Often within days to a few weeks, depending on the severity and your sending history. Improvements compound as engagement rises.

Original article: https://tonyherman.com/dkim-spf-dmarc-in-plain-english/
PDF version: https://tonyherman.com/dkim-spf-dmarc-in-plain-english/?apa_pdf=1

# Special Offer for Readers

1,000+ Channels • On-Demand Movies • **5 Devices**

**$69.99/mo (~$2.33/day)**

Try it for a month and see if you like it, then switch.

**Start Your Trial**

Click to learn more about CUE Broadcast

Tip: Get 3 friends of family to sign up and you it for free.