# Email DNS worksheet

Every record a sending domain needs, with the order to add them in, the trap that breaks each one, and the command that proves it landed. Fill this in before the domain sends anything, then keep it.

Domain: _____ Filled by: _____

Mail host (receiving): _____ Sending platform: _____

Registrar / DNS host: _____ Date: _____

## The order

| # | RECORD | WHY IT GOES HERE | DONE |
|---|---|---|---|
| 1 | MX | Receiving comes first. Verification codes, DMARC reports and replies all need somewhere to land. | ☐ |
| 2 | SPF | Names the servers allowed to send for the domain. | ☐ |
| 3 | DKIM | Signs outgoing mail. Publish the key before the first send, not after. | ☐ |
| 4 | DMARC (p=none) | Enforcement published before SPF and DKIM are right quarantines your own mail. | ☐ |
| 5 | Tracking CNAME | Optional. Only if your platform tracks clicks on a hostname of yours. | ☐ |

## The records

### 1. MX

```
Type: MX   Name: @   Priority: _____   Value: _____
Type: MX   Name: @   Priority: _____   Value: _____
TTL: _____   ☐ Previous host's MX records deleted
```

> **Trap.** Old MX records left beside the new ones split your mail between two systems by priority. Half the inbox ends up somewhere nobody is reading.

### 2. SPF

```
Type: TXT   Name: @
"v=spf1 include:_____ include:_____ ~all"
DNS lookups used: _____ of 10   ☐ Confirmed this is the only SPF record on the domain
```

> **Trap.** Two SPF records is a permanent error, not a merge, and receivers treat the error as a failure. Each include, a, mx, exists and redirect costs one of your ten lookups, and providers spend more than one apiece. A single quoted string stops at 255 characters. Publish ~all and let DMARC enforce.

### 3. DKIM

Type: ☐ TXT ☐ CNAME Name: _____._domainkey

Value: _____

Selector recorded: _____ Key length: ☐ 2048 ☐ 1024

> **Trap.** The selector name is arbitrary and only your provider knows it: Google Workspace uses google, Microsoft 365 uses selector1 and selector2, many relays use s1. Write it down or you cannot check the key later. Two senders can sign for one domain at once, on different selectors.

### 4. DMARC

Type: TXT Name: _dmarc

"v=DMARC1; p=none; rua=mailto:_____@_____"

Published: _____ Reports reviewed: _____

Move to p=quarantine: _____ Then p=reject: _____

> **Trap.** Start at p=none. It satisfies Gmail's February 2024 requirement and Microsoft's May 2025 one while you read reports and find the sender you forgot about. The dates on this block are the point: a policy nobody escalates stops nothing.

### 5. Tracking CNAME (optional)

Type: CNAME Name: _____ (link. / email. / mail.)

Value: _____

> **Trap.** Campaign links should resolve on a hostname you own. No shorteners, ever.

## Prove each one landed

| RECORD | COMMAND | HEALTHY OUTPUT | OK |
|---|---|---|---|
| MX | `dig +short MX example.com` | Your mail host's names, with priorities | ☐ |
| SPF | `dig +short TXT example.com` | Exactly one string starting v=spf1 | ☐ |
| DKIM | `dig +short TXT s1._domainkey.example.com` | A long p= value (about 390 characters means 2048-bit) | ☐ |
| DMARC | `dig +short TXT _dmarc.example.com` | v=DMARC1; p=none; rua=... | ☐ |
| CNAME | `dig +short CNAME link.example.com` | Your platform's tracking host | ☐ |

On Windows without dig: `nslookup -type=TXT _dmarc.example.com`. Query a public resolver directly (`dig +short TXT example.com @1.1.1.1`) so you read what the internet sees rather than what your router cached, and remember a replaced record can persist for the length of the old TTL.

## Before the first real send

- ☐ Sent a test to myself and opened the full headers
- ☐ SPF: pass ☐ DKIM: pass ☐ DMARC: pass
- ☐ Scored the message with a free pre-send checker (mail-tester.com or similar): _____ / 10
- ☐ This sheet filed with the date on it

Completed by _____ Date _____