Secuenza

Deliverability guide: SPF, DKIM and DMARC

Whether your emails reach the inbox depends on two things: that providers can check it's really you, and that your mailbox has a good reputation. This guide explains the three records that prove it, how to set them up with the most common providers and which habits protect your reputation.

Why it matters

Gmail, Yahoo and Outlook.com ask anyone who sends often to have **SPF, DKIM and DMARC** on their domain, to let every email be unsubscribed from with one click, and to have hardly anyone mark it as spam. Without those records, your emails will usually end up in spam or not arrive at all.

Secuenza sends from your own mailbox, so it's your email provider that signs (or doesn't sign) each email. What you have to do is publish, in your domain's DNS, the data that confirms it.

Before you start: where your DNS is

Your domain's DNS is managed where you bought it or where you pointed it (the registrar, your hosting, Cloudflare…), which isn't always where your email is. Log in to that panel and look for the DNS zone: that's where you add the records in this guide.

A DNS change takes from a few minutes to a few hours to show. Then go back to **Checks** in Secuenza.

SPF: who may send for your domain

SPF is a **TXT** record at the root of the domain that starts with `v=spf1`, says which servers may send on its behalf and ends with `~all` (others are suspicious) or `-all` (others are rejected).

Provider	What your SPF must include
Microsoft 365	`include:spf.protection.outlook.com`
Google Workspace	`include:_spf.google.com`
IONOS	`include:_spf-eu.ionos.com`
OVHcloud	`include:mx.ovh.com`
Hostinger	`include:_spf.mail.hostinger.com`
Aruba	`include:_spf.aruba.it`
Zoho Mail (EU)	`include:zoho.eu`

For example, with Microsoft 365: `v=spf1 include:spf.protection.outlook.com ~all`.

Three rules worth knowing:

- **There can only be one SPF.** If you already have one (for your website, your invoicing software), don't add another: put the `include`s together in the same record. With two, neither works.
- **No more than 10 lookups.** Every `include` counts, and so do the ones inside it. Go over and servers treat it as broken.
- **Never** `+all`: it would let anyone send in your name.

If your mailbox is a Gmail or Outlook.com address (not on your domain), you don't have to set anything: SPF and signing are the provider's. Those mailboxes do have low limits, and Secuenza respects them.

DKIM: your emails' signature

With DKIM, your provider signs each email with a private key and you publish the public key in DNS, under a name such as `selector._domainkey.yourdomain.com`. That way the recipient knows the email wasn't altered on the way and really comes from your domain.

- **Microsoft 365:** in the Microsoft Defender portal, in the email authentication settings (DKIM), choose your domain. It gives you two **CNAME** records (`selector1` and `selector2`): add them to your DNS and go back to the portal to turn signing on.
- **Google Workspace:** in the Admin console, under Gmail → Authenticate email, generate a **2048-bit** record, add it as a **TXT** record at `google._domainkey` and press "Start

authentication".

- **IONOS, OVHcloud, Hostinger, Aruba, Zoho and most hostings:** look for "DKIM" in the email panel. Many turn it on by themselves if the DNS is also with them; if not, they give you the record to copy.

Secuenza looks for the signature under each provider's usual names. If yours has another name, the **live send test** (Pro) finds it. Use **2048-bit** keys: 1024-bit ones are already considered weak.

DMARC: what to do with what fails

DMARC is a **TXT** record at `_dmarc.yourdomain.com` that tells providers what to do with an email claiming to be from your domain that passes neither SPF nor DKIM, and where to send you reports. To count, the sender's domain must match the domain of SPF or of the DKIM signature ("alignment").

Start by observing:

```
v=DMARC1; p=none; rua=mailto:dmarc@yourdomain.com
```

1. **Two to four weeks on** `p=none` : nothing changes, but you get reports on who sends for your domain. Check that everything legitimate goes out signed (your mailbox, your website, your invoices).
2. **Move up to** `p=quarantine` : whatever fails goes to spam.
3. **And then to** `p=reject` : whatever fails is rejected. It's what best protects your domain from anyone trying to pass themselves off as you.

Reports arrive as XML. There are free services that summarise them; looking at them now and then is enough.

Checking it with Secuenza

In each mailbox's details, **Checks** reviews SPF, DKIM and DMARC, and also mail reception (MX), the server's reverse name, MTA-STS, BIMI and encryption. Each check comes out green, amber or red, with what to set and where. If you already have an SPF, it suggests the complete record with what's missing.

With **Pro**, also:

- **Live send test:** Secuenza sends a real email from your mailbox and tells you what the receiving server sees: signature, SPF, DMARC alignment, encryption and spam check.

- **Blocklists:** it checks whether your server or your domain appear on the lists that filters use.

And the **Safety** section brings together what the brake has stopped, your 30-day figures against their limits and the status of each mailbox: Sending safety explains it.

Reputation: what filters look at

With the records in place, what decides is how you behave:

- **Start slowly.** A new mailbox or domain that suddenly sends hundreds of emails looks like spam. Secuenza's warm-up raises the limit day by day.
- **Respect the limits.** For each provider Secuenza uses a cautious daily and hourly limit, below its maximum, and spreads the sending over your schedule.
- **Make unsubscribing easy.** Every email carries the unsubscribe link and the header that lets Gmail and Outlook show their "Unsubscribe" button. Unsubscribes take effect straight away.
- **Clean lists.** Never buy lists. Bounced emails and inactive contacts are set aside, and the safety brake pauses a campaign if there are too many bounces or unsubscribes, and sending to an email provider where nobody opens your emails.
- **Few complaints.** If more than 2 or 3 in a thousand people mark your emails as spam, filters penalise you. Write only to people who expect your emails.
- **Emails that sound like a person.** Clear text, few links, no link shorteners, images with text around them. Upload images from the editor: those from Drive or Dropbox, or pasted inside the email, often end up in spam. The spam check warns you about what usually counts against you.
- **Get replies.** A reply is the best sign that your email is welcome. Write so that people answer.

If your emails go to spam

1. Open **Checks**: are the three records green?
2. With Pro, run the **live send test** and see what fails on the receiving server.
3. Review the **spam check** of the campaign's emails.
4. Check in **Safety** whether the brake has stopped any email provider, and in **Results**, the unsubscribes and bounces: if they rise, stop and clean the list.
5. Lower the limit for a few days and raise it again slowly.