PAUL PARSONS
DIGITAL MARKETING, AI & MARTECH

GUIDE FREE

EMAIL AUTHENTICATION IN PLAIN ENGLISH

SPF, DKIM and DMARC for people who run a business, not a mail server.

PAULPARSONS.COM.AU
JULY 2026 · V1.0

SPF, DKIM, DMARC.
TEN MINUTES TO CHECK.

01 WHY THIS MATTERS NOW

The major mailbox providers, Google and Yahoo led, Microsoft followed, now require senders, particularly bulk senders, to authenticate their email properly. Fail the checks and your mail lands in spam or gets rejected outright, invoices and proposals included, not just newsletters. The requirements have tightened over recent years and continue to move, so treat the specifics as a snapshot and check current provider documentation when acting. This guide gives you enough to check your own domain and to have an intelligent conversation with whoever fixes it.

02 THE THREE RECORDS, ONE METAPHOR EACH

SPF is the guest list. A public record on your domain listing which services are allowed to send email as you: your email platform, your marketing tool, your CRM. A receiving server checks the list, and a sender not on it looks like a gatecrasher.

DKIM is the tamper-evident seal. Your sending service signs each message cryptographically. The receiver checks the seal, proving the message really came from your domain and was not altered in transit.

DMARC is your standing instruction. A record that tells receivers what to do when a message fails the other two checks, deliver it anyway, quarantine it, or reject it, and where to send you reports about who is sending as your domain. Without DMARC, you have rules but no enforcement and no visibility.

03 THE TEN-MINUTE CHECK

You need your domain name and a free DNS lookup tool (MXToolbox and similar, or Google's Admin Toolbox).

1 **SPF.** Look up the TXT records on your domain. You want exactly one record starting **v=spf1**. Two SPF records is a fault, not double protection, receivers treat it as a failure. Read the record: does it include every service that legitimately sends as you? The email platform, the marketing tool, the CRM, the invoicing software. A service missing from the list will fail.

2 **DKIM.** This lives per sending service, not as one domain record. Open the settings or deliverability page of each platform that sends for you and confirm DKIM shows as verified or enabled for your domain. Any platform showing unverified is sending unsealed mail.

3 **DMARC.** Look up the TXT record at **_dmarc.yourdomain**. If nothing exists, that is your first fix. If it exists, read the **p=** value: **none** means monitor only, **quarantine** means send failures to spam, **reject** means refuse them. Check a **rua=** address is present, that is where the reports go, and reports you never receive help nobody.

04 GETTING TO A SENSIBLE END STATE

The staged path, and the reason nobody sane jumps straight to reject:

1. **Publish DMARC at p=none with a reporting address.** Nothing changes for delivery, you start seeing who sends as your domain, including services you forgot and imposters you did not know about.

2. **Fix what the reports surface.** Add missing legitimate services to SPF, verify DKIM on each platform.

3. **Move to p=quarantine, then p=reject** once the reports show your legitimate mail passing consistently. Tightening before that point sends your own invoices to spam.

Common faults, in the order I meet them: a sending tool added last year and never added to SPF. Two SPF records after a platform migration. DKIM never verified on the marketing platform, the setup email went to someone who left. A DMARC record with no reporting address. And the classic: everything configured on the main domain, nothing on the subdomain the newsletter actually sends from.

When to hand it over: the checks above are safely yours. Changing DNS records is low-risk but unforgiving of typos, if nobody internal is comfortable, this page is the brief to hand your IT support, and the whole job is small.

If you would rather have this done **with** you than **to** you, this is the work I do.

START A CONVERSATION

PAUL PARSONS

CONSULTANT | DIGITAL MARKETING, AI & MARTECH

0403 127 478

pp@paulparsons.com.au

www.paulparsons.com.au

Perth, Western Australia 6111