Business email that lands in the inbox.

SPF, DKIM and DMARC, for a business running **Google Workspace**. Three DNS records decide whether the rest of the internet believes mail from your domain is really from you. **Every Google requirement below is sourced to Google's own current documentation**, checked on the date above, because this is an area where confident advice ages badly.

Who this is for: whoever administers your Google Workspace. The DKIM step in section 04 needs a **super administrator** account for the Google Admin console. SPF in section 04 and all of section 05 need only the ability to **add TXT records** wherever your domain's DNS is managed. Those are often two different places and sometimes two different people. **If neither is you, this is the document to forward.**

01 What each record actually does

SPF	**Lists which servers are allowed to send email using your domain name.** A receiving server looks up the list and checks whether the message came from something on it. *Like giving the post office a list of the couriers permitted to send mail in your company's name. Anyone not on the list is treated as suspect.*
DKIM	**Adds a cryptographic signature to every message you send.** The receiving server checks the signature against a public key published in your DNS, which proves the message really came from your domain and was not altered on the way. *Like a tamper-evident seal on the envelope. Break the seal and it shows.*
DMARC	**Tells receiving servers what to do when a message fails the first two checks, and asks them to report back.** Without it, each receiving server falls back on its own judgement about the From: address your reader actually sees. *Like leaving a standing instruction at the sorting office: if a letter claims to be from us but the list and the seal do not check out, here is what to do with it, and please send me a regular summary of what you saw.*

02 What is required, and what is merely wise

Every sender	Since **1 February 2024**, anyone sending to personal Gmail addresses must have **SPF or DKIM**. Google's wording is "Set up SPF **or** DKIM email authentication for your sending domains". You also need, among others, valid forward and reverse DNS, a TLS connection, RFC 5322 message formatting, and a spam rate under **0.3%**.
5,000+ a day to Gmail	Above that volume the bar rises on all three. Google: "Set up SPF **and** DKIM email authentication for your domain" and "Set up DMARC email authentication for your sending domain. Your DMARC enforcement policy can be set to none." Alignment counts here too: "For direct email, the domain in the sender's From: header must be aligned with either the SPF domain or the DKIM domain".
So, you	If fewer than 5,000 of your daily messages go to Gmail addresses, then on the letter of the rules **DMARC is not required of you**. **Set it up anyway.** The reason is in the next box.

DMARC is not about the phishing that arrives in your inbox. It is about the phishing sent in your name. Gmail screens inbound mail whether you configure anything or not. **What nothing stops by default is somebody else sending email that appears to come from your domain**: a fake invoice with changed bank details, a message to your supplier asking them to update payment records, a note to your own staff that looks like it came from the boss. Those land on **your customers and your colleagues**, carrying your company's name. SPF and DKIM alone say whether a message is authentic. **Neither ties that check to the From: address your customer actually reads.** DMARC does, and it is the record that says what you want done when the check fails. It costs one DNS record, and at the starting setting in section 05 it changes nothing about your own mail.

Only DKIM is configured in the Admin console. SPF and DMARC are not Google settings at all: they are TXT records you add wherever your domain's DNS is managed, which is usually your registrar or your web host. This is a step that sends people hunting the Admin console for a setting that is not there.

03 Check what you have now

Three lookups. Replace `yourdomain.com` with your own domain. On a Mac open Terminal; on Windows open Command Prompt and swap `dig +short TXT` for `nslookup -type=TXT`.

```
# 1. SPF, look for a line containing v=spf1
dig +short TXT yourdomain.com
# 2. DKIM, look for v=DKIM1
dig +short TXT google._domainkey.yourdomain.com
# 3. DMARC, look for v=DMARC1
dig +short TXT _dmarc.yourdomain.com
```

Reading the results:

- ☐ **Nothing came back for lookup 1.** You have no SPF record. Start at section 04.
- ☐ **Lines came back, but none containing `v=spf1`.** Those are usually verification records put there by other services. You still have no SPF. Section 04.
- ☐ **Two or more lines containing `v=spf1`.** Google: "each domain can have only one SPF record that specifies all hosts or email services. If you have multiple SPF records, your email might end up in a recipient's spam folder." Merge them into one.
- ☐ **Nothing came back for lookup 2 or 3.** No DKIM key of your own, and no DMARC. Section 04 step 2, then section 05.

04 Set them up, in this order

Google: "You must turn on SPF and/or DKIM for your domain before you can use DMARC."

Step 1. SPF. At your DNS host, add one TXT record on the root of the domain. If Workspace is your only sender, Google's recommended value is:

```
v=spf1 include:_spf.google.com ~all
```

Google recommends `~all` rather than `-all`. Add every other service that sends as you before moving on, one `include:` each, and mind section 06.

Step 2. DKIM, in the Google Admin console:

1. Sign in at `admin.google.com` as a **super administrator**. Google: "You must be signed in as a super administrator for this task."
2. Open **Menu**, then **Apps**, then **Google Workspace**, then **Gmail**, and click **Authenticate email**.
3. Pick your domain from the **Selected domain** menu.
4. Click **Generate New Record**. On a new tenancy this can fail. Google says you "must wait" 24 to 72 hours after turning on Gmail before the key can be generated.
5. Choose **2048** for key length and leave the prefix selector as `google`. Google: "Longer keys are more secure than shorter keys." Use 1024 only if your DNS provider rejects 2048, and a different prefix if your domain already uses a DKIM key with the `google` prefix.
6. Click **Generate**. Google shows a **DNS Host name (TXT record name)** and a **TXT record value**.
7. At your DNS host, add that TXT record. The host name will look like `google._domainkey`.
8. Go straight back to **Authenticate email**, select the domain again and click **Start authentication**. Once setup is complete and working, the status at the top of the page changes to **Authenticating email with DKIM**. It may not say that yet, see the next step. Google's steps put this straight after the DNS record, with no wait in between, and its troubleshooting page names this click as the fix for a "Not authenticating" error.
9. **Now expect a lag.** Google: it "can take up to 48 hours for DKIM authentication to start working", and the console may keep telling you to update your DNS records for that whole time. Google: "If you've correctly added your DKIM key at your domain provider, you can ignore this message."
10. Check it worked by sending a message to someone on Gmail or Workspace and looking at the `Authentication-Results` header for `dkim=pass`. Google: "You can't verify DKIM is on by sending yourself a test message."

05 The DMARC setting that is easy to get wrong

Step 3, continued from section 04. Wait 48 hours after DKIM, then add DMARC. One TXT record at your DNS host, on `_dmarc.yourdomain.com`. Some hosts append the domain for you, so check the saved record rather than assuming. The `p=` tag is your standing instruction, and it has three values.

p=none	Do nothing, just report. **Start here.**
p=quarantine	Send failures to spam.
p=reject	Refuse failures outright.

> **Do not start at reject, however tempting the advice sounds.** Google's own guidance is: "When you start using DMARC, we recommend setting the policy option (p) to **none**. As you learn how messages from your domain are authenticated by receiving servers, update your policy. Over time, change the receiver policy to quarantine (or reject)." Start at reject before you know every system that sends as you, and the mail you lose is **your own**: the invoicing tool, the booking system, the newsletter. The bounce, if there is one, goes back to whatever sent the message, **not to you**.

A reasonable first record. Send the reports to a mailbox or group you create for them, not a personal address. Google: "We don't recommend using your own email address."

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

They arrive **daily**, as machine-readable XML, one set per receiving provider, which is why they get their own mailbox. Leave the policy at `none` until the reports show every legitimate sender passing. Then move to `quarantine`, and only later to `reject`.

06 The limit that quietly breaks SPF

> **Ten lookups, and nested ones count.** Google: "The SPF specification allows for a maximum of 10 DNS lookups (for example, include, a, mx mechanisms). Complex SPF records that include several third-party services can exceed this limit, causing your SPF record validation to fail." The trap is that **one `include:` can cost five**, because the service you included has includes of its own. A record with five entries can already be at the ceiling. When it tips over, the errors you get "might include warnings that you don't have an SPF record (even if you do have one)", which sends you looking in the wrong place entirely.

Count yours before adding a sixth sender. At the limit, the cheapest fix is usually dropping a service you stopped using.

07 Your website sends mail too

Easy to miss, because it is nobody's job.

- ☐ **Contact form notifications, order receipts, invoices, password resets.** These usually leave from your website or its mail service rather than from Workspace, in which case `include:_spf.google.com` alone does not cover them.
- ☐ **Find out what your site actually sends through**, then add that service to the same single SPF record.
- ☐ **SPF alone is not always enough for DMARC.** DMARC only passes if the domain in the visible From: line matches the domain SPF or DKIM authenticated, which Google calls alignment. A service sending with its own bounce address fails that even when it is in your SPF record. Ask each one to sign with your domain, or to use a bounce address on it. The reports in section 05 will show which sending IPs are failing, which is how you find them.
- ☐ **Send yourself a test from the live contact form**, then open it and check it did not land in spam. This checks delivery, not DKIM. Do it after any DNS change, and again after any hosting move.

> **One honest caveat.** Google notes that "even if SPF is correctly set up for your domain, forwarded messages can still fail SPF". If someone auto-forwards your mail onward, that is usually the explanation, and no DNS change fixes it.

If you would rather not do this yourself

We set up and manage Google Workspace for Singapore businesses, including the DNS side that sits outside the Admin console, and we are an authorised reseller. If you just want a second pair of eyes on what you already have, message us and we will tell you what we would check first. **No obligation, and we will say so if nothing in it stands out.**

info@xsquare.com.sg · **xsquare.com.sg/google-workspace**