USE IT MATE

The Email Deliverability & DMARC Compliance

Author: Jasson Borgueta, Technical Lead — Use IT Mate (Bundaberg & Wide Bay)
support@useitmate.com

The Invisible Leak in Your Business

In early 2024, Google and Yahoo fundamentally changed how the internet handles email.

If your business domain (youragency.com.au) does not have strict backend authentication records configured, major providers now assume you are a spammer or a spoofed hacker.

The Symptoms of a Broken Setup:

- Your invoices and quotes are silently landing in clients' junk folders.
- Your marketing emails (via Mailchimp or ActiveCampaign) are getting heavily penalized.
- Hackers can easily send emails pretending to be admin@youragency.com.au to trick your clients into paying fake invoices.

This guide outlines exactly how to lock down your Microsoft 365 or Google Workspace environment to ensure 100% deliverability and stop spoofing.

The 3 Pillars of Email Security

To comply with modern anti-spam laws, your domain's DNS registry (GoDaddy, Cloudflare, CrazyDomains) requires three specific records to be perfectly aligned.

- SPF (Sender Policy Framework): The guest list. This tells the internet exactly which servers (e.g., Microsoft, your website, your CRM) are legally allowed to send emails on your behalf.

- DKIM (DomainKeys Identified Mail): The digital seal. This encrypts your emails in transit so hackers cannot alter your invoices mid-flight.

- DMARC (Domain-based Message Authentication): The bouncer. This tells Google and Yahoo exactly what to do with emails that fail the first two tests (e.g., "Send them to quarantine" or "Reject them entirely").

The DIY 5-Step Implementation Guide

Warning: Modifying DNS records incorrectly can instantly break your company's ability to send or receive emails. Proceed carefully.

Step 1: Audit Your Sending Software

Before touching anything, write down every piece of software that sends emails on your company's behalf. (e.g., Microsoft 365, Mailchimp, PropertyMe, Xero, VaultRE).

Step 2: Build the SPF "Guest List"

Log into your domain host and locate your DNS settings. Find your existing TXT record for SPF. You must append the specific include: tags for every software you listed in Step 1.

- Example: If you use Microsoft and Mailchimp, your record must look like this: v=spf1 include:spf.protection.outlook.com include:servers.mcsv.net -all

Step 3: Generate and Publish DKIM Keys

Log into your Microsoft 365 Admin Center (or Google Workspace). Navigate to the security routing settings and generate your unique DKIM CNAME records. Copy these two records and publish them in your domain host's DNS dashboard.

Step 4: Deploy the DMARC Safety Net

In your domain's DNS dashboard, create a new TXT record.

- Host/Name: _dmarc
- Value: v=DMARC1; p=quarantine; rua=mailto:admin@yourdomain.com.au;
- Crucial Safety Tip: Never set your policy (p=) to reject immediately, or you risk hard-bouncing your own marketing emails if you made a mistake in Step 2. Always start with quarantine.

Step 5: Verify Global Propagation

Save all records. Wait 1 to 4 hours for the internet to update. Go to mxtoolbox.com/DMARC.aspx, type in your website, and ensure all checks return green.

Need this handled by a professional?

Auditing SPF records across multiple CRMs and generating DKIM keys can be highly technical. If you miss a single software integration, your daily operations will break.

If your team does not have a dedicated Cloud Architect, Use IT Mate deploys this exact security patch for QLD businesses for a flat, one-time fee of $299.

We log into your registry, audit your software, build the records, verify the global propagation, and log out. Zero downtime, zero broken CRMs.

Visit useitmate.com or email us directly (support@useitmate.com) to authorize the fix today.