KOMSTADT

Komstadt Managed Services
enquiry@komstadt.com · +852 2806 8188

GUIDE · EMAIL SECURITY

The three email settings every firm needs

SPF, DKIM and DMARC are three DNS records that stop criminals sending email in your company's name. Using Microsoft 365 or Google Workspace does **not** switch them on for you — someone has to configure them.

1 · SPF — who is allowed to send

A published list of the mail servers permitted to send email for your domain. Receiving servers check it and treat mail from anywhere else as suspect.

Check: is there a single, correct `v=spf1` record that includes every service you send from (Microsoft 365, your CRM, your marketing tool)?

2 · DKIM — proof it wasn't tampered with

A cryptographic signature added to every message. The receiver verifies it against a key in your DNS, proving the mail really came from you and wasn't altered in transit.

Check: is DKIM signing enabled in your mail platform, with the matching keys published in DNS?

3 · DMARC — what to do with fakes, and reporting

Ties SPF and DKIM together and tells receivers what to do with mail that fails: monitor, quarantine, or reject. It also emails you reports of who is sending as your domain.

Check: is there a DMARC record, and is its policy moving from `p=none` toward `p=quarantine` or `p=reject`?

The path to enforced protection

- ✓ Publish one correct SPF record covering every legitimate sender
- ✓ Turn on DKIM signing and publish the keys
- ✓ Start DMARC at p=none and read the reports for a few weeks
- ✓ Fix any legitimate senders that fail, then move DMARC to quarantine, then reject

Not sure where your domain stands? Komstadt will check your SPF, DKIM and DMARC for free and show you exactly what to fix. Email **enquiry@komstadt.com**.

© 2026 Komstadt Systems Limited · komstadt.com

General guidance, not legal or regulatory advice.