MOSEBURY MEDIA

SPF, DKIM and DMARC explained for practices and firms

If your emails reach junk folders, the cause is usually three missing or incorrect records. This guide explains each one.

Why it matters

Appointment confirmations, quotes and client letters are worthless if they land in spam. Large mailbox providers now expect senders to prove that their messages are genuine.

The three records

- SPF lists the services allowed to send email for your domain
- DKIM adds a digital signature that proves a message was not altered
- DMARC tells receiving servers what to do when a message fails those checks, and sends you reports

Common problems

A practice often sends email from several places, such as its mailbox, its booking system and its newsletter tool. If any of them is missing from the records, its messages may be rejected.

What to do

- List every system that sends email using your domain
- Publish an SPF record that includes each one
- Switch on DKIM signing in each system
- Publish a DMARC record, starting in monitoring mode
- Review the reports, then tighten the policy

Related pages

- Hosting, domains and email
- Digital brand launch

Common questions

Do small practices need DMARC?

Yes. It protects your domain from being impersonated and improves the delivery of your own messages.

Where are these records set up?

They are added in the DNS settings for your domain, usually with your domain registrar or hosting provider.

Checklist

- ☐ I have listed every system that sends our email
- ☐ We have a correct SPF record
- ☐ DKIM signing is switched on
- ☐ We have a DMARC record
- ☐ Someone reviews the DMARC reports

Published by Mosebury Media on 27 November 2026 at https://moseburymedia.co.uk/insights/spf-dkim-dmarc-for-practices.html. This guide is general information and is not legal or regulatory advice. Copyright © 2023 Mosebury Media. Contact: hello@moseburymedia.co.uk