CHECKLIST · SOFTWARE & SYSTEMS

SPF, DKIM and DMARC explained: the email settings that help your invoices reach the inbox

Published 6 October 2026. Read the full story, sources and any updates at
digitaladvisors.com.au/journal/email-authentication-spf-dkim-dmarc/

- [ ] **Ask your IT provider or domain host** whether you have SPF, DKIM and DMARC for every domain you send from.
- [ ] **List every service that emails customers as you**, and check it's covered.
- [ ] **Check Microsoft 365 DKIM** is set up for your own domain, not just the onmicrosoft.com one.
- [ ] **Check Google Workspace DKIM** shows as authenticating in the Admin console.
- [ ] **Publish DMARC at p=none with reporting**, then review the reports.
- [ ] **Plan the move to quarantine, then reject**, as the ACSC recommends.
- [ ] **Protect unused domains** with records that say they don't send email.
- [ ] **If you send newsletters**, check your platform handles one-click unsubscribe.

NOTES

General information only, not legal, tax or financial advice. Check the full story and its sources before acting.