CHECKLIST · TECHNOLOGY

DMARC explained: the bouncer checking your café's name at the door

Published 22 October 2026. Read the full story, sources and any updates at
digitaladvisors.com.au/journal/dmarc-explained-cafe-bouncer/

- [ ] **Check whether your domain has a DMARC record.** Ask whoever manages your domain or email, or look for a TXT record at _dmarc.yourdomain.com.au (using your own domain).
- [ ] **List every service that sends email as your business.** Include your mailbox provider, newsletter tool, booking system, invoicing software and website forms.
- [ ] **Make sure each service passes SPF or DKIM using your domain, not its own.** Google recommends setting this up at least 48 hours before adding DMARC.
- [ ] **Publish a DMARC record set to "none" with a reporting address.** Use a dedicated mailbox or a reporting service rather than a staff member's inbox.
- [ ] **Read the reports for at least a week.** Look for genuine services that fail, and fix them before tightening the policy.
- [ ] **Move to "quarantine", then "reject".** Once your own email passes, ask your IT provider to tighten the policy in steps.

NOTES

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