COREWEST
SECURED. MANAGED. TRUSTED.

WA BUSINESS EMAIL SECURITY DATA · OCTOBER 2026

Three in four WA business domains we checked don't tell inboxes to block email faked in their name.

A public, passive check of 7,499 Western Australian business domains, 12 to 14 October 2026 (Perth time). Next update: January 2027.

74.2%
no DMARC policy that asks inboxes to block fakes

40.9%
no valid DMARC record at all

24.9%
enforce DMARC in full (quarantine or reject)

59.1%
run their email on Microsoft 365

DMARC: every domain in exactly one group

GROUP	DOMAINS	SHARE
No valid DMARC record	3,066	40.9%
Monitor only (p=none)	2,488	33.2%
Policy broken or misspelt (e.g. "quarentine")	8	0.1%
Subtotal: don't ask inboxes to block fakes	**5,562**	**74.2%**
Partial enforcement (pct under 100)	70	0.9%
Quarantine	1,161	15.5%
Reject	706	9.4%
Total	**7,499**	**100%**

Enforced in full = quarantine plus reject: 1,867 domains (24.9%). The 70 with partial enforcement are counted on their own.

How we did it

We ran our passive domain check against 8,422 WA business domains. 7,499 gave a complete result and are counted here; we left out 857 that did not finish, 50 that do not exist and 16 with broken DNS. The check reads public DNS records and makes one normal visit to the home page. No logins, no scanning, no access to anyone's systems. We do not publish business names or domains.

Other findings (share of 7,499 domains)

FINDING	SHARE
No SPF record	10.2%
SPF record broken or unhealthy	14.9%
Email on Microsoft 365 (4,431)	59.1%
Email on Google Workspace (963)	12.8%
Email on own server or web host (839)	11.2%
No MTA-STS	93.9%
DNSSEC off	98.1%
No CAA record	97.6%
Website missing basic security headers	68.3%
No privacy policy found on the website	47.7%
HTTPS certificate problem	1.8%

What it means

DMARC is a short public record. It tells other mail systems what to do with email that claims to be from you but isn't. Without it, or set to monitor only, a fake invoice in your name has a better chance of reaching your clients. Whether a fake gets through still depends on the receiving system.

What to do first

1. **Check your own domain.** Free, in your browser: corewest.com.au/check
2. **Fix DMARC first.** If it is missing or set to none, add reporting, watch the reports for a few weeks, then move to quarantine.
3. **Agree a call-back rule** for any change of bank details. Free poster: corewest.com.au/services/invoice-fraud-protection-perth
4. **Get the full picture.** The Free Cyber Risk Snapshot covers 30 public checks and tells you what to fix first.

How to cite

COREWEST, "WA business email security data, October 2026". Public check of 7,499 WA business domains, 12 to 14 October 2026. Published 14 October 2026. https://corewest.com.au/wa-email-security-2026

General information only, not an audit or an assurance of any business's security.