

Is mailguard.com.au legit? TrustSniffer's high-trust assessment: 80/100

mailguard.com.au

Verdict

80

OUT OF 100

HIGH TRUST

mailguard.com.au appears legitimate.

Our checks found nothing pointing to fraud. Ordinary care still applies when you pay or sign in.

Not Scam

Safe for Login

Low Risk

Assessed 2026-08-11 by automated analysis. Classification confidence 75%.

What this site appears to be

MailGuard corporate site describing cloud email security products, features, integrations (Microsoft 365, Google Workspace), support and contact details, free 30-day trial, blog and resources, and company credibility statements (ISO certification).

Evidence status and limitations

- Evidence completeness: UNKNOWN
- The real-world operator identity was not independently verified.
 - Module-level completeness metadata is unavailable for this legacy report.

At a glance

The checks that decide most of this verdict.

Malware engines	None flagged it VirusTotal	CLEAR
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	0 reports AbuseIPDB; shared hosting inflates this count	NOTED
Domain age	25 years old Registered history	CLEAR
Web archive	Archived since 2001 853 snapshots	CLEAR
Certificate	Encrypted connection Issued by Sectigo Public Server Authentication CA OV R36	NOTED

The page as captured

No screenshot is retained for this report.

Key findings

- Automated classification: Not Scam.
- Domain age: more than 10 years (registration continuity).
- Public web-archive history exists since 2001.
- No flags from the reputation services TrustSniffer consulted at assessment time.

Full analysis

Overview

MailGuard is a corporate SaaS website presenting cloud-based email security and phishing-protection services for businesses, with product information, platform integrations, support resources, enterprise channels, and a free-trial pathway.

Scam/Impersonation Risk

No scam, phishing, impersonation, blacklist, or other contradictory signals were observed. The site's stated business model is coherent with a conventional cybersecurity SaaS provider: it presents MailGuard, MailGuard Live, SafeGuard, and ImageGuard for email security, continuity, archiving, and image monitoring, with integrations including Microsoft 365, Google Workspace, Zimbra, and Microsoft Exchange. The homepage also provides ordinary enterprise pathways such as contact, support, partner, and free-trial functions; no sensitive login form, wallet-connect behavior, or cryptocurrency features were identified. Available external reputation checks were clean, and the domain has an established global traffic presence. Evidence:

- The homepage presents a corporate SaaS model for cloud email security, phishing protection, email continuity, archiving, and image monitoring, with no page-level red flags.
- Domain continuity: registered 2001 (~25.24 years old); 853 archive snapshots spanning 2001–2026, covering 26 years tracked.
- External reputation telemetry recorded 0 malicious detections, 0 suspicious detections, and no blacklist or phishing result; the domain is ranked within the global top 1 million traffic set.

Regulatory Verification Notes

The available content is consistent with a commercial cybersecurity software provider rather than a financial-services platform. The About, Terms and Conditions, Privacy Policy, and Contact pathways support a professional corporate presentation, while the site also makes an ISO-certification credibility claim; that claim should be treated as an on-site representation rather than independent certification proof. No financial-services license or registration number is stated, but this is a disclosure and applicability question—not evidence of a scam. Technical records associate the domain with MailGuard Pty Ltd, although the real-world operator identity remains independently unverified. A separate broker-reputation dataset returned no match and provides no adverse regulatory conclusion. Evidence:

- The registration record lists Melbourne IT as registrar and MAILGUARD PTY. LTD. as owner.
- The site's transport encryption uses an OV certificate issued by Sectigo Public Server Authentication CA OV R36, valid to 2026-11-03.

- The homepage and company navigation expose Terms and Conditions, Privacy Policy, About Us, Contact, support, partner, and enterprise-sales pathways.

What to Verify Next

Before credential or payment interactions, an organization should independently match the contracting entity and applicable service terms to the intended MailGuard supplier, confirm any relevant certification or regulatory applicability through authoritative sources, and validate support or sales channels using independently obtained corporate contact details. Contracting teams should also review renewal, cancellation, data-processing, service-level, and payment-protection provisions before committing to a subscription. Evidence:

- The About page provides the appropriate basis for independently corroborating the claimed corporate identity and ISO certification.
- The Terms and Conditions and Privacy Policy pages provide the contractual and data-handling material for procurement review.
- The Contact and support pathways provide channels that can be cross-checked independently before account or payment activity.

Summary Verdict

Available evidence is consistent with an established, apparently legitimate website and supports a high-trust, low-risk posture for ordinary business use. No contradictory indicators were observed, but the evidence does not independently prove the real-world operator identity.

Infrastructure Integrity

The website is protected by Amazon Web Services CDN/WAF infrastructure, with observed traffic terminating at an AWS edge address rather than an exposed origin. This is a meaningful defensive control that reduces direct origin exposure, but it remains a mitigating infrastructure signal rather than proof of organizational legitimacy.

Evidence:

- Served from AS16509 (AMAZON-02 - Amazon.com, Inc., US).
- Observed edge address: 52.62.166.239; no origin candidate was identified.
- TLS certificate subject organization: MailGuard Pty Ltd; validation level: OV; issuer: Sectigo Public Server Authentication CA OV R36; valid to 2026-11-03.

Closing Assessment

Routine site access is proportionate to the available risk posture; credential or payment actions should proceed only after the ordinary independent merchant-identity, contractual, and payment-protection checks have been completed.

Written analysis generated 2026-08-11 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

No rule findings contributed to this verdict.

Identity verification

Status	UNVERIFIED
Identity score	30/100

Identity verification confidence	50%
----------------------------------	-----

- No on-site identity signals detected

Identity verification measures whether the site can be independently connected to a real-world brand or person. It is separate from the classification confidence.

What TrustSniffer observed

First-party facts recorded during the assessment of mailguard.com.au.

- The request stayed on mailguard.com.au. It was not redirected to another domain. CLEAR
- Registration is published under Melbourne IT. CLEAR
- DNS for this domain is served by com.au, across 3 name servers. NOTED
- The earliest public archive of this site is from 2001-05-16. CLEAR
- It is hosted on AMAZON-02, from a server in US. NOTED

Domain intelligence

Registrar	Melbourne IT
Hosting	AMAZON-02 - Amazon.com, Inc., US
Country	US
Server IP	52.62.166.239
Name servers	dns3.mailguard.com.au, dns4.mailguard.com.au, dns2.mailguard.com.au
SSL issuer	Sectigo Public Server Authentication CA OV R36
SSL expiry	2026-11-03
Domain age	25.24 years (continuous registration)
Domain expiry	Not available
Archive first seen	2001-05-16
Archive snapshots	853
Reputation	VirusTotal: 0 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about mailguard.com.au at assessment time. It is a starting point for your own judgement, not a guarantee: a high score means the signals were consistent with a legitimately operated site, a low or critical score means several risk patterns were present.

TrustSniffer assesses a website from the evidence it can collect at a point in time: domain registration and age, hosting and certificate, the content the site served, and third-party reputation feeds. A score is a summary of that evidence, not a guarantee and not a legal finding. There is no human rating and no user review in it. A site can change after it is assessed.

