CYBER
NODE
Your Path to Security

CYBER EXPOSURE SNAPSHOT

EXAMPLE.COM.AU

This report provides an independent, external assessment of publicly visible cyber exposure — the same information an attacker would find during reconnaissance.

Date	March 2026
Target Domain	example.com.au
Prepared by	Cyber Node
Classification	Sample Report

This report is based solely on publicly available information and does not involve the use of credentials or access to internal systems.

Executive Summary

This report presents the findings of an external cyber exposure assessment conducted against **example.com.au**. The assessment was performed using publicly available information only — no credentials were used and no internal systems were accessed. The organisation operates a substantial digital footprint with over 20 subdomains spanning web applications, email marketing platforms, internal tools, and staging environments. Email security foundations are generally well-configured, with SPF, DKIM, and DMARC all in place, and the primary domain's SSL/TLS configuration meets modern standards.

However, several findings require urgent attention. A publicly accessible subdomain is **running PHP 7.2.34, which reached end-of-life in November 2020** and exposes a directory listing of the server's file system. An **admin login panel is publicly accessible** on another subdomain, and a **staging environment reveals a default server configuration page**, both disclosing server technology versions. Additionally, **one staff email address has appeared in a known data breach**, creating a credential-stuffing risk. The **primary website is currently returning a 403 Forbidden error**, meaning the site is inaccessible to the public. While the DMARC policy is set to **quarantine** rather than reject, this represents a reasonable intermediate posture that should be strengthened over time.

OVERALL RISK RATING

HIGH

6 findings require attention — 2 high, 2 medium, 2 low

Key Findings

#	Category	Severity	Finding	Recommendation
1	Exposed Infrastructure	HIGH	A subdomain is serving a **directory index (Index of /)** to the public internet,	Immediately disable directory listing on this server and either upgrade PHP to a currently supported version (8.2 or later)

#	Category	Severity	Finding	Recommendation
			running **PHP 7.2.34** — a version that reached end-of-life in November 2020. This means the server has not received security patches for over five years. Directory listings expose internal file structures, potentially revealing sensitive files, configuration data, or backup archives to anyone who visits the URL.	or decommission the subdomain entirely if it is no longer required. Restrict public access via firewall rules or authentication.
2	Exposed Admin & Staging Panels	HIGH	An **admin login panel is publicly accessible** on one subdomain, and a **staging environment displays a default server page** on another. Both disclose **PHP 8.4** and **LiteSpeed** server technology. Publicly accessible admin panels are a primary target for brute-force and credential-stuffing attacks, while staging environments may contain test data or weaker security controls.	Restrict access to both subdomains by implementing IP allowlisting, VPN-only access, or multi-factor authentication. Remove default server pages from the staging environment and suppress server version headers (X-Powered-By, Server) across all subdomains.
3	Data Breach Exposure	MEDIUM	One staff email address has been identified in at least one known third-party data breach. If this individual has reused their corporate password on the	Immediately reset the password for this account and verify that multi-factor authentication (MFA) is enabled. Conduct a review to ensure no unauthorised access has occurred. Consider implementing a policy requiring

#	Category	Severity	Finding	Recommendation
			compromised external service, attackers could use those credentials to attempt access to organisational systems including email, VPN, or cloud applications.	unique passwords for corporate accounts and periodic breach monitoring for all staff.
4	Website Availability	MEDIUM	The **primary website is returning a 403 Forbidden error**, as are several related subdomains. A 403 response means the server is actively refusing to serve content. This could indicate a misconfiguration, maintenance, or an access control issue. For a consumer-facing brand, an inaccessible website directly impacts customer acquisition and brand credibility.	Investigate the root cause of the 403 errors on the primary website and related subdomains. If the site is undergoing maintenance, ensure a user-friendly holding page is served. Verify that web server access controls and file permissions are correctly configured.
5	Public Email Exposure	LOW	**Ten staff email addresses** are publicly discoverable through external sources, including addresses that follow identifiable naming patterns (firstname@, firstname.lastname@). This volume of exposed addresses increases the organisation's susceptibility to targeted phishing, social engineering,	Where practical, reduce the visibility of individual staff email addresses on public platforms. Consider using generic role-based addresses (e.g., info@, support@) for public-facing communications and implement email security awareness training for all staff whose addresses are exposed.

#	Category	Severity	Finding	Recommendation
			and spam campaigns. Attackers commonly harvest such addresses to craft convincing impersonation emails.	
6	DMARC Policy Strength	LOW	The DMARC policy is currently set to **p=quarantine**, which instructs receiving mail servers to flag suspicious emails rather than reject them outright. While this is a reasonable intermediate posture, it means that spoofed emails impersonating the domain may still be delivered to recipients' spam folders rather than being blocked entirely. The DMARC reporting address is configured to receive aggregate reports, which is positive.	Plan a transition to **p=reject** after reviewing DMARC aggregate reports (rua) to confirm that all legitimate sending sources are properly authenticated via SPF and DKIM. This will provide the strongest protection against domain impersonation.

Positive Findings

	Finding	Detail
✓	**SPF Record Properly Configured**	The SPF record uses a **-all** (hard fail) mechanism, which instructs receiving servers to reject emails from unauthorised sources. Authorised senders including the email provider, support platform, and transactional email service are correctly included.

	Finding	Detail
✓	**DKIM Fully Configured**	Two DKIM selectors are properly configured with 2048-bit RSA keys, providing cryptographic email authentication and integrity verification for all outbound messages.
✓	**DMARC Policy Active with Reporting**	A DMARC policy is in place at quarantine level with aggregate reporting enabled, providing visibility into email authentication results and a meaningful layer of protection against domain spoofing.
✓	**Strong SSL/TLS Configuration**	The primary domain supports only TLS 1.2 and TLS 1.3, with legacy protocols (SSLv2, SSLv3, TLS 1.0, TLS 1.1) all disabled. Cipher suites are modern and strong, including CHACHA20-POLY1305 and AES-GCM. The server is not vulnerable to Heartbleed and supports TLS Fallback SCSV.
✓	**Valid SSL Certificate**	The SSL certificate is current, covers both the apex domain and www subdomain, and uses SHA-256 signing with a 2048-bit RSA key.
✓	**Majority of Staff Accounts Not Breached**	Of the ten discoverable email addresses, nine show no record of involvement in known data breaches, indicating generally good credential hygiene across the organisation.

Infrastructure Overview

Component	Details
Primary Domain	example.com.au — hosted in Australia
DNS Provider	Third-party managed DNS

Cyber Node

Component	Details
Email Provider	Microsoft 365
Email Marketing	Salesforce Marketing Cloud (multiple delivery subdomains)
Transactional Email	Third-party SMTP relay service
Support Platform	Zendesk (included in SPF record)
SSL Certificate	Let’s Encrypt, SHA-256/RSA-2048, valid and current
Primary Web Server	LiteSpeed (hosted in Australia)
Application Servers	LiteSpeed (admin and staging environments); Microsoft IIS (internal application)
CDN/Delivery	Akamai and Amazon CloudFront
Subdomains Observed	23 subdomains identified via certificate transparency and DNS enumeration

Recommended Priority Actions

PRIORITY 1 — IMMEDIATE

Secure or Decommission the Exposed Server

One subdomain is exposing a directory listing on a server running end-of-life PHP 7.2.34, which has not received security patches since 2020. Disable directory listing immediately, then either upgrade the server to a supported PHP version and restrict access, or decommission the subdomain if it is no longer needed. This is the single highest-risk exposure identified.

PRIORITY 2 — IMMEDIATE

Restrict Access to Admin and Staging Environments

The admin panel and staging environment are publicly accessible and disclosing server technology details. Implement IP-based access restrictions, VPN requirements, or multi-factor authentication to prevent unauthorised access. Remove default pages and suppress technology version headers across all non-public subdomains.

PRIORITY 3 — SHORT-TERM

Address Breached Credentials and Resolve Website Availability

Reset the password for the breached account, confirm MFA is active, and audit for any unauthorised access. Separately, investigate and resolve the 403 Forbidden errors on the primary website and related subdomains to restore public access and protect brand reputation.

PRIORITY 4 — ONGOING

Subdomain Hygiene and DMARC Hardening

Conduct a comprehensive review of all 23 observed subdomains to identify and decommission any that are unused. Transition the DMARC policy from quarantine to reject after validating aggregate reports. Establish a quarterly review cycle for subdomain inventory, email authentication, and breach monitoring.

Disclaimer

This is a sample report generated for demonstration purposes. The domain, findings, and infrastructure details shown are illustrative only.

Actual reports are generated from live scan data specific to your organisation’s domain and reflect real external exposure at the time of assessment.