

Is nzpost.co.nz legit? TrustSniffer's high-trust assessment: 80/100

nzpost.co.nz

Verdict

80

OUT OF 100

HIGH TRUST

nzpost.co.nz 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

Official-looking NZ Post site content: navigation for personal and business postal services, tracking, shop, developer APIs, support, and corporate information. Focus on parcel services, tracking tools, retail products and store locations.

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	30 years old Registered history	CLEAR
Web archive	Archived since 1996 1727 snapshots	CLEAR
Certificate	Encrypted connection Issued by Thawte EV RSA CA G2	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 1996.
- No flags from the reputation services TrustSniffer consulted at assessment time.

Full analysis

Overview

NZ Post is a corporate postal and logistics website presenting personal and business services for domestic and international shipping, parcel tracking, courier delivery, retail purchases such as stamps and packaging, customer support, store locations, and developer APIs. Its apparent business model is the provision of postal, parcel, courier, retail, and value-added delivery services through shipping fees, product sales, and business services.

Scam/Impersonation Risk

No contradictions were observed across the site's identity, service presentation, historical continuity, or external reputation signals. The homepage presents a coherent postal-services operating model, includes standard account and tracking functionality, and does not exhibit detected brand-impersonation, phishing, malicious-content, or suspicious-form indicators. Browser telemetry recorded some external requests and posts outside an allowlist, but the same assessment found no cloaking, hidden forms, externally submitted password forms, wallet activity, or other abuse pattern; this is therefore a contextual technical observation rather than evidence of impersonation. The available evidence supports an established, apparently legitimate site, while independently proving the real-world operator identity remains outside the evidence supplied.

EVIDENCE

- The homepage presents consistent NZ Post personal, business, tracking, shop, support, and corporate-service content with no reported red flags.
- The domain was registered in 1997 and is approximately 29.55 years old.
- Historical records contain 1,727 snapshots spanning 1996–2026, covering 31 tracked years.
- External reputation checks recorded 0 malicious detections, 0 suspicious detections, 0 abuse reports, and no blacklist or phishing hit.

Regulatory Verification Notes

The site's apparent postal and logistics business model does not itself establish a regulated financial or other licensed activity. The supplied page evidence references corporate information and support functions, but it does not independently verify the real-world operator identity; any legal-entity or service-authority relationship should therefore be treated as apparent rather than proven. No licensing claim or registration number was identified in the supplied content, which is a transparency item for ordinary verification rather than evidence of a scam. The

domain is registered through CSC Corporate Domains, Inc., and the transport layer uses a known, high-assurance certificate, providing affirmative infrastructure support for the site's established presentation.

EVIDENCE

- The domain registrar is CSC Corporate Domains, Inc.
- The site's TLS certificate was issued by Thawte EV RSA CA G2 with EV validation and is valid through 2026-12-31T23:59:59+00:00.
- The homepage's corporate/service classification and detailed postal-service content are consistent with a mature operating website.
- Available third-party broker context contained no matching adverse association.

What to Verify Next

Before credential or payment interactions, an organization should independently confirm the relevant merchant or service identity, review the applicable terms and return or refund arrangements, and confirm that payment protections are available. Where a regulated service is believed to be involved, the relevant national registry should be checked for the precise legal entity and authorization. Contact and support details should also be confirmed through an independently sourced official channel rather than relying solely on information encountered in an unsolicited message.

EVIDENCE

- The contact and support area is presented as a dedicated site function.
- The corporate information area is available for independent comparison with the legal entity used in any transaction.
- The shop and account areas create distinct points at which payment, credential, and consumer-protection terms should be reviewed.

Summary Verdict

Available evidence is consistent with an established, apparently legitimate website and supports a high-trust, low-risk posture for its stated services. The assessment does not independently prove the real-world operator identity, so legitimacy should be understood as evidence-consistent rather than conclusively verified.

Infrastructure Integrity

The website is protected by CDN/WAF infrastructure, with observed edge addresses hosted by Amazon.com, Inc. on AS16509; no origin candidate was identified in the supplied infrastructure analysis. This protective architecture is a mitigating security measure that reduces direct exposure of the underlying service, but it is not proof of ownership or legitimacy.

Closing Assessment

Normal browsing and ordinary service evaluation are proportionate, but credential or payment actions should follow independent confirmation of the merchant identity, applicable consumer terms, and available payment protections.

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 nzpost.co.nz.

- The request stayed on nzpost.co.nz. It was not redirected to another domain. CLEAR
- Registration is published under CSC Corporate Domains, Inc. CLEAR
- DNS for this domain is served by akam.net, across 6 name servers. NOTED
- The earliest public archive of this site is from 1996-11-12. CLEAR
- It is hosted on AMAZON-02, from a server in US. NOTED

Domain intelligence

Registrar	CSC Corporate Domains, Inc
Hosting	AMAZON-02 - Amazon.com, Inc., US
Country	US
Server IP	76.223.12.173
Name servers	a1-181.akam.net, a18-65.akam.net, a24-67.akam.net, a3-64.akam.net, a5-66.akam.net, a8-67.akam.net
SSL issuer	Thawte EV RSA CA G2
SSL expiry	2026-12-31
Domain age	29.74 years (continuous registration)
Domain expiry	Not available
Archive first seen	1996-11-12
Archive snapshots	1727
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 nzpost.co.nz 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.

This report online: <https://trustsniffer.com/report/nzpost.co.nz> · assessed 2026-08-11