

Is mandela.ac.za legit? TrustSniffer's high-trust assessment: 90/100

mandela.ac.za

Verdict

90

OUT OF 100

HIGH TRUST

mandela.ac.za appears legitimate.

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

Not Scam

Low Risk

Assessed 2026-08-10 by automated analysis. Classification confidence 75%.

What this site appears to be

Official Nelson Mandela University homepage with admissions guidance, news, events, campus information, student/staff portals, emergency contacts, and institutional policies.

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	9.1 years old Registered history	CLEAR
Web archive	Archived since 2017 5000 snapshots	CLEAR
Certificate	Encrypted connection Issued by HARICA OV TLS RSA	NOTED

The page as captured

No screenshot is retained for this report.

Key findings

- Automated classification: Not Scam.
- Domain age: 3 to 10 years (registration continuity).
- Public web-archive history exists since 2017.
- No flags from the reputation services TrustSniffer consulted at assessment time.

Full analysis

Overview

The website presents as the Nelson Mandela University institutional homepage, providing prospective and current students with admissions and study information alongside university news, events, campus resources, student and staff portals, emergency contacts, policies, and donation or engagement options.

Scam/Impersonation Risk

No contradictions were observed. The site's coherent academic-institutional presentation, sustained historical continuity, and clean external threat results are consistent with an established, apparently legitimate university website rather than a phishing or impersonation operation. The real-world operator identity is not independently verified, so the identity conclusion remains evidence-consistent rather than proven. No suspicious contact-channel anomaly was identified in the supplied page findings.

EVIDENCE

- The homepage is classified as a university/institutional site and contains admissions, campus, portal, governance, news, and emergency-support content.
- The domain has an authoritative age of 9.045859 years based on registration continuity.
- Historical records show 5000 snapshots from 2017-07-24 through 2024-01-12, covering 8 years with no suspicious repurposing or semantic drift.
- External checks recorded 0 malicious detections, 0 suspicious detections, 0 abuse reports, and no phishing or impersonation indicators.

Regulatory Verification Notes

The available material is consistent with a public university information service, not a financial or investment platform requiring the type of broker licensing normally associated with trading sites. The pages provide institutional policies, directories, contact information, portals, and governance-oriented content; however, the supplied evidence does not independently establish the operator's legal identity or present a licensing or registration number. That is a transparency and verification point, not evidence of a scam. Transport security and identifiable academic-network hosting provide additional technical support for site continuity, while not independently proving institutional ownership.

EVIDENCE

- The homepage title is “Home - Nelson Mandela University,” with institutional policy, leadership, directory, student, staff, and supplier navigation.
- The site is served from AS2018, TENET (The UNINET Project) - TENET (The UNINET Project), ZA.
- The TLS certificate is issued by HARICA OV TLS RSA at OV validation level and is valid through 2027-02-06.
- The observed business model is public-university information, including study programmes, portals, news, events, engagement, and donations; no financial-services license claim or license number is supplied.

What to Verify Next

Before credential submission or any payment, donation, or application transaction, an organization should independently confirm that the domain is the university's intended official channel through contact details obtained from an offline or separately established institutional source. Any admissions, donation, or payment instructions should be reconciled with the university's published policies and independently confirmed payment-protection arrangements. Where a formal regulatory or education-sector registration is relevant to the specific transaction, that status should be checked with the appropriate official registry.

EVIDENCE

- The captured homepage contains no sensitive form and no untrusted form destination.
- Observed browser behavior detected no hidden forms, password-exfiltration forms, wallet activity, clipboard manipulation, or cloaking.
- The homepage provides institutional emergency contacts, support information, and policy links that can be compared against independently obtained university contact details.

Summary Verdict

The overall posture is high trust and low risk, with the available evidence consistent with an established, apparently legitimate institutional website. No scam, phishing, impersonation, or other contradictory risk signals were identified, although independent operator identity verification remains incomplete.

Infrastructure Integrity

The site resolves to one direct host, with no CDN or WAF detected and a likely origin address visible in the hosting posture. This is a straightforward academic-network deployment rather than an edge-fronted service; it is an infrastructure characteristic, not an indication of malicious activity.

Closing Assessment

Routine informational use is proportionate; independent institutional and payment-protection checks should be completed before credentials or funds are submitted.

Written analysis generated 2026-08-10 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	55/100
Identity verification confidence	60%

- Identity verified on page

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 mandela.ac.za.

- The request stayed on mandela.ac.za. It was not redirected to another domain. CLEAR
- The earliest public archive of this site is from 2017-07-24. CLEAR
- It is hosted on TENET (The UNINET Project), from a server in ZA. NOTED

Domain intelligence

Registrar	Not available
Hosting	TENET (The UNINET Project) - TENET (The UNINET Project), ZA
Country	ZA
Server IP	192.96.15.90
Name servers	Not available
SSL issuer	HARICA OV TLS RSA
SSL expiry	2027-02-06
Domain age	9.05 years (continuous registration)
Domain expiry	Not available
Archive first seen	2017-07-24
Archive snapshots	5000
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 mandela.ac.za 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/mandela.ac.za> · assessed 2026-08-10