

Is nou.edu.ng safe? TrustSniffer's moderate-trust assessment: 65/100

nou.edu.ng

Verdict

65

OUT OF 100

MODERATE TRUST

nou.edu.ng is moderately trusted.

Most signals looked ordinary, and some evidence was missing. Read the checks below before you pay or hand over personal details.

Governance Risk

Assessed 2026-08-13 by automated analysis. Classification confidence 55%.

What this site appears to be

Official-looking homepage for the National Open University of Nigeria (NOUN). Provides contacts, admissions info, faculties, research centres, student services and links to partner resources. No evident malicious forms or high-risk financial solicitations in the provided HTML.

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	Not available No registration record was returned	NOTED
Web archive	Never archived No public history of this site	WATCH
Certificate	Encrypted connection Issued by YE1	NOTED

The page as captured

No screenshot is retained for this report.

Key findings

- Automated classification: Governance Risk.
- No flags from the reputation services TrustSniffer consulted at assessment time.

Full analysis

Overview

The website is the institutional online presence of the National Open University of Nigeria (NOUN), presenting academic programmes, admissions information, faculties, research centres, distance-learning services, student support, news, and study-centre resources. Its apparent purpose is to support university recruitment, administration, learning, and dissemination of institutional information rather than to promote third-party financial products.

Scam/Impersonation Risk

No contradictions were observed across the available pages and technical signals: there are no confirmed phishing, impersonation, blacklist, or malicious-reputation indicators. The homepage presents a coherent university structure, including administration, faculties, admissions, student services, research units, and institutional contacts. Behavioral review identified some inline script patterns for review, but the observed site behavior showed no hidden forms, external password-submission forms, wallet activity, cloaking, or untrusted external posting destinations; this does not amount to evidence of impersonation or credential harvesting.

EVIDENCE

- The homepage identifies NOUN and links to institutional pages covering admissions, faculties, administration, research, student support, and study centres.
- The contact and homepage content publish university-oriented contact and service information, including an institutional email address and telephone contact.
- The behavioral page assessment recorded no hidden forms, no password forms submitted externally, zero wallet-related activity, and no cloaking indicators.
- External reputation checks recorded zero malicious and zero suspicious detections, with no confirmed blacklist or phishing result.

Regulatory Verification Notes

The site's apparent institutional identity is supported by its detailed organisational content, academic structure, and links to Facebook, X, and Instagram. However, the available material does not independently verify the real-world operator's identity, and the pages reviewed do not present a licensing or registration number in the manner expected of a separately regulated financial service; for a university website, the relevant institutional status should therefore be confirmed through the appropriate Nigerian education authority. The absence of a matched broker-reputation record is only contextual and is not a legal or regulatory determination.

EVIDENCE

- The About, Administration, Faculties, Admissions, and Student Support pages describe a structured public-university operating model and named institutional functions.
- The site presents social links to facebook.com, x.com, and instagram.com, consistent with an established institutional communications presence.
- The site's transport encryption uses a DV certificate issued by YE1, valid through 2026-09-24.
- The hosting telemetry identifies AS16509 operated by AMAZON-02 - Amazon.com, Inc., US.

What to Verify Next

Before high-value or sensitive actions, an organisation should confirm the university's current official status and admissions details through an independently obtained government or education-sector source, rather than relying solely on links reached from the website. Any payment, application, or account-support interaction should use contact channels independently confirmed through the institution's published offline or official public communications.

EVIDENCE

- The Admissions, Contact Us, and Student Support pages provide the site-specific channels and workflows requiring independent confirmation.
- The About and Administration pages identify the institutional structure that can be compared with an authoritative education-sector record.
- The homepage links to external partner resources, so the legitimacy and purpose of any partner destination should be checked separately before use.

Summary Verdict

The website has a **moderate-trust posture** and is consistent with an apparently legitimate university information and services platform. Its substantive institutional content and clean observed interaction profile support ordinary informational use, while the available evidence does not independently establish the real-world operator to the standard required for sensitive or high-value reliance.

Infrastructure Integrity

The site is protected by Amazon Web Services CDN/WAF infrastructure, and the analysis observed only an edge address rather than a directly exposed origin. This is a useful exposure-mitigation measure, but it is a defensive hosting characteristic rather than proof of institutional legitimacy.

EVIDENCE

- The infrastructure assessment identified AWS CDN/WAF protection with one observed edge address and no likely origin candidate.
- The observed edge address was 52.30.227.127 in the United States.

Closing Assessment

Routine browsing and institutional information gathering are proportionate uses; sensitive submissions, payments, or consequential account actions should proceed only after the relevant institutional details and transaction channels have been independently confirmed.

Written analysis generated 2026-08-13 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

1 finding contributed to this verdict, raised by registration and ownership.

01 Governance Risk

- The public registration record for this domain is incomplete.

Registration and ownership rule:KF_WHOIS_INCOMPLETE

Identity verification

Status	LIKELY
Identity score	76/100
Identity verification confidence	76%

- Identity verified on page
- Trusted social count=2

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 nou.edu.ng.

- The request stayed on nou.edu.ng. It was not redirected to another domain. CLEAR
- It is hosted on AMAZON-02, from a server in US. NOTED

Domain intelligence

Registrar	Not available
Hosting	AMAZON-02 - Amazon.com, Inc., US
Country	US
Server IP	52.30.227.127
Name servers	Not available
SSL issuer	YE1
SSL expiry	2026-09-24
Domain age	Not available (no registration date was returned)

Domain expiry	Not available
Archive first seen	Not available
Archive snapshots	0
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 nou.edu.ng 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/nou.edu.ng> · assessed 2026-08-13