

Is unilorin.edu.ng legit? TrustSniffer's high-trust assessment: 90/100

unilorin.edu.ng

Verdict

90

OUT OF 100

HIGH TRUST

unilorin.edu.ng 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-looking homepage for the University of Ilorin (UNILORIN). Contains navigation for admissions, academics, research centres, news, contact details, and a contact form. Contact email and phone number are displayed; content focuses on institutional information.

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	22 years old Registered history	CLEAR
Web archive	Archived since 2004 5000 snapshots	CLEAR
Certificate	Encrypted connection Issued by YE1	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 2004.
- No flags from the reputation services TrustSniffer consulted at assessment time.

Full analysis

Overview

What this website presents is the official-looking institutional presence of the University of Ilorin (UNILORIN), offering information on admissions, academic programmes, faculties, research centres, news, student services, library resources, and institutional contact channels as part of a public-university information model.

Scam/Impersonation Risk

No blacklist, phishing, malicious-content, brand-impersonation, or conflicting-identity signals were observed. The homepage content is coherent with a university institution, includes structured navigation across academic and administrative functions, and provides a contact form without a login or sensitive-data submission mechanism. Available evidence is therefore consistent with an established, apparently legitimate website, although the real-world operator identity remains independently unverified.

EVIDENCE

- The homepage identifies the institution as the University of Ilorin and presents admissions, faculties, research centres, news, student affairs, library, and contact functions.
- The homepage analysis found no phishing indicators, brand-impersonation indicators, malicious scripts, hidden forms, wallet activity, or external password forms.
- Domain registration continuity records show registration in 2003, approximately 22.01 years of age.
- Archive records show 5,000 snapshots from 2004-08-06 through 2025-01-11, covering 22 years with a maximum observed gap of 1 year.

Regulatory Verification Notes

The site's apparent institutional purpose and academic presentation are consistent with a public university, and the available reputation evidence is clean. No specific licensing claim, registration number, or regulatory authority disclosure was identified on the reviewed pages; for an educational institution, this is a transparency item requiring contextual confirmation rather than evidence of fraud. The page-level identity claim supports apparent legitimacy but does not independently prove the legal operator.

EVIDENCE

- The homepage is titled “Home - University of Ilorin” and identifies the institution through its academic and administrative navigation.
- The site publishes institutional contact details and a general contact form; no regulated-financial product or sensitive transaction workflow was observed.
- Hosting is on AS16509, AMAZON-02 - Amazon.com, Inc., US.
- The site's TLS certificate is issued by YE1, uses Domain Validation (DV), and is valid to 2026-10-02T12:02:35+00:00.

What to Verify Next

Before credential or payment interactions connected with admissions or other institutional services, an organization should independently confirm the university's official contact channels, verify any applicable educational authorization through the relevant Nigerian institutional or education registry, and review the applicable admissions, fee, refund, and payment-protection terms. Contact details should be corroborated through an independent offline or previously established institutional channel rather than relying solely on the website.

EVIDENCE

- The homepage provides a registrar contact address, telephone number, and contact form for independent channel comparison.
- The admissions and academic navigation provides the relevant context for confirming programme and fee information through an authoritative institutional source.
- The site has no login form or sensitive form on the reviewed homepage, limiting the directly observed credential-collection exposure.

Summary Verdict

The website has a high-trust, low-risk posture, and the evidence is strongly consistent with an established institutional website. Its legitimacy appears credible from the convergence of coherent university content, sustained historical continuity, clean reputation signals, valid transport security, and stable infrastructure, while independent operator verification remains incomplete.

Infrastructure Integrity

The site is protected by AWS CDN/WAF infrastructure, which is a meaningful mitigating control against direct exposure and common delivery-layer abuse. Observed addressing was limited to an AWS edge endpoint, with no origin candidate identified in the supplied infrastructure analysis; this supports infrastructure protection but is not, by itself, proof of institutional legitimacy.

Closing Assessment

Normal informational use is proportionate to the assessed posture; credential or payment activity should proceed after the ordinary independent checks of institutional identity, applicable authorization, terms, and payment protections have been completed.

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 unilorin.edu.ng.

- The request stayed on unilorin.edu.ng. It was not redirected to another domain. CLEAR
- The earliest public archive of this site is from 2004-08-06. 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	99.80.2.193
Name servers	Not available
SSL issuer	YE1
SSL expiry	2026-10-02
Domain age	22.01 years (continuous registration)
Domain expiry	Not available
Archive first seen	2004-08-06
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 unilorin.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/unilorin.edu.ng> · assessed 2026-08-10