

Is univ-lorraine.fr legit? TrustSniffer's high-trust assessment: 100/100

univ-lorraine.fr

Verdict

100

OUT OF 100

HIGH TRUST

univ-lorraine.fr 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 2026-08-13 by automated analysis. Classification confidence 55%.

What this site appears to be

Official homepage of Université de Lorraine with comprehensive information about courses, research, campus life, international programs and student services. Appears to be a legitimate institutional site in French.

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	21 years old Registered history	CLEAR
Web archive	Never archived No public history of this site	WATCH
Certificate	Encrypted connection Issued by GEANT TLS RSA 1	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).
- No flags from the reputation services TrustSniffer consulted at assessment time.

Full analysis

Overview

The website is an institutional university portal for Université de Lorraine, presenting academic information, student resources, research, campus services, and admissions-related content; its apparent purpose is to support education and university administration rather than sell products or solicit investment.

Scam/Impersonation Risk

No scam, phishing, impersonation, or identity contradiction was observed. The homepage content is coherent with a university information portal, contains no commercial or investment solicitation, and the evaluated external reputation signals were clean. Behavioral inspection did identify two suspicious inline scripts, but this limited anomaly was not accompanied by external data submission, hidden forms, credential capture, wallet activity, or cloaking, so it does not outweigh the broader benign evidence. The published contact address ``info@example.come`` is a contact-channel integrity anomaly consistent with a deliverability-breaking typo or possible typosquat, but it is not, by itself, evidence of impersonation.

EVIDENCE

- Domain registration records show registration in 2005; domain age is 21.41 years.
- The homepage is classified as an institutional university page and presents courses, research, campus life, international programs, admissions, and student services.
- Behavioral testing recorded 2 suspicious inline scripts, with 0 external XHR requests, 0 hidden forms, 0 password-external forms, 0 wallet-connect runs, and no cloaking.
- External reputation checks recorded 0 malicious detections, 0 suspicious detections, and no phishing or impersonation contradiction.

Regulatory Verification Notes

The available content consistently presents Université de Lorraine as an academic institution, but the real-world operator identity is not independently verified by the supplied evidence. No licensing claim or registration number was identified in the available site content; for an informational university portal, this is a transparency and applicability point rather than evidence of fraud. The registration and transport-security details are consistent with an established institutional service. No broker-related third-party reputational match was identified.

EVIDENCE

- Registration records list GIP RENATER as registrar.
- The site is served from AS2200, FR-RENATER - Renater, FR.
- The TLS certificate is OV-validated, issued by GEANT TLS RSA 1, with subject organization UNIVERSITÉ DE LORRAINE and validity through 2027-02-08.

What to Verify Next

Before credential or payment interactions, independently confirm that the relevant university service is reached through the institution's official directory or a previously trusted institutional communication channel. Where a transaction, enrollment payment, or other regulated activity is involved, confirm the applicable university authorization, fee terms, refund or withdrawal conditions, and payment-protection arrangements through official administrative contacts. Confirm official support and contact channels independently rather than relying solely on a message or link received unexpectedly.

EVIDENCE

- The homepage contains 0 forms and no sensitive form fields.
- No login form, hidden form, password-external form, or untrusted form destination was detected.
- The homepage links to established social platforms including Facebook, LinkedIn, Instagram, YouTube, and other listed institutional channels.

Summary Verdict

The overall posture is **high trust and low risk**. Available evidence is consistent with an established, apparently legitimate university website, supported by converging institutional, registration, reputation, and transport-security signals. The operator's real-world identity remains likely rather than independently proven, so the site should not be treated as identity-verified solely from its on-page presentation.

Infrastructure Integrity

The site is not CDN- or WAF-fronted and resolves directly to an apparent origin address. This provides less edge-layer shielding than a mainstream CDN deployment, but the direct hosting posture is not itself a trust contradiction and is consistent with the site's institutional hosting context.

Closing Assessment

Normal informational use is proportionate to the assessed posture; credentials or payments should follow the ordinary independent identity, service-term, and payment-protection checks appropriate to the specific university transaction.

Written analysis generated 2026-08-13 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	LIKELY
Identity score	80/100
Identity verification confidence	80%

- Trusted social count=4

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 univ-lorraine.fr.

- The request stayed on univ-lorraine.fr. It was not redirected to another domain. CLEAR
- Registration is published under GIP RENATER. CLEAR
- DNS for this domain is served by ciril.fr, across 2 name servers. NOTED
- The registration is paid up to 2027-06-05. NOTED
- It is hosted on FR-RENATER, from a server in FR. NOTED

Domain intelligence

Registrar	GIP RENATER
Hosting	FR-RENATER - Renater, FR
Country	FR
Server IP	193.54.54.4
Name servers	arcturus.ciril.fr, orion.ciril.fr
SSL issuer	GEANT TLS RSA 1
SSL expiry	2027-02-08
Domain age	21.41 years (continuous registration)
Domain expiry	2027-06-05
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 univ-lorraine.fr 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/univ-lorraine.fr> · assessed 2026-08-13