

Is jstor.org legit? TrustSniffer's high-trust assessment: 100/100

jstor.org

Verdict

100

OUT OF 100

HIGH TRUST

jstor.org appears legitimate.

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

Not Scam

Low Risk

Assessed 2026-08-17 by automated analysis. Classification confidence 55%.

What this site appears to be

JSTOR homepage offering search and access to scholarly content, with account login (including Google/Microsoft) and institutional link options, plus cookie and privacy 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.

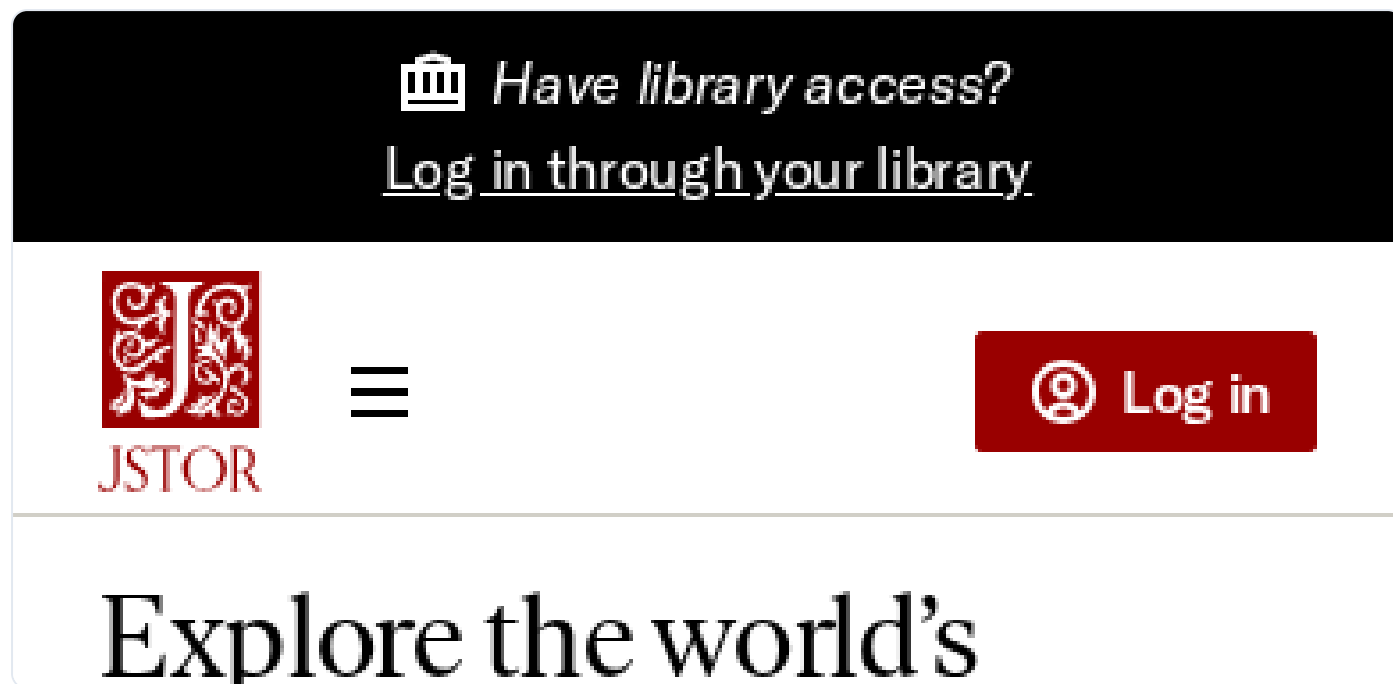
At a glance

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	31 years old Registered history	CLEAR
Web archive	Never archived No public history of this site	WATCH
Certificate	Encrypted connection Issued by GlobalSign Atlas R3 OV TLS CA 2026 Q2	NOTED

The page as captured

<https://www.jstor.org/>



What jstor.org served when TrustSniffer captured it on 2026-08-17. The page may look different now.

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.
- The operator behind the site could not be independently connected to a real-world brand or person.

Full analysis

Overview

JSTOR is an academic content platform that provides visitors with searchable scholarly articles, journals, books, images, and primary sources. Its apparent business model combines institutional access, individual registration, subscriptions, and nonprofit support to enable research and educational use.

Scam/Impersonation Risk

No contradictions were observed. The homepage presents a coherent academic-repository service, and its account functionality is consistent with the stated purpose: users can register, link institutional access, or authenticate through Google and Microsoft. The observed login flow showed no hidden forms, untrusted destinations, wallet activity, or brand-impersonation indicators. External reputation checks found no malicious or suspicious detections, supporting a low scam and impersonation risk assessment.

EVIDENCE

- The homepage provides scholarly search and access functions, institutional linking, registration, and standard account authentication without detected phishing or impersonation indicators.
- Behavioral inspection recorded zero hidden forms, zero password submissions to external forms, zero wallet-provider or wallet-drainer activity, and no cloaking.
- External reputation results recorded 0 malicious detections and 0 suspicious detections; the site held global traffic rank 1091.

Regulatory Verification Notes

The site presents an informational and academic-access model rather than a regulated financial service, so no financial license claim or license number was identified in the reviewed content. The homepage does provide privacy and cookie information and describes institutional and individual access arrangements, but the real-world operator identity is not independently verified by the available evidence. This is an identity-verification limitation rather than an observed contradiction; the registration record uses Network Solutions, LLC, while privacy-protected registrant details are an administrative matter.

EVIDENCE

- The domain registration artifact records creation on 1996-02-16, making the domain 30.52 years old.
- The site's transport encryption uses an OV certificate issued by GlobalSign Atlas R3 OV TLS CA 2026 Q2, valid through 2027-02-01T19:47:36+00:00.
- The homepage identifies scholarly content, institutional access, individual registration, and privacy/cookie information; no regulated financial-service license claim is presented.

What to Verify Next

Before credential or payment interaction, an organization should independently confirm the relevant operator or merchant identity, review the applicable subscription, cancellation, and refund terms, and ensure that payment protections are available. For institutional use, the institution's library or procurement function should confirm that the intended access route and account-linking process are official. Any applicable registration or licensing requirement should be checked against the relevant public registry rather than inferred from the site's presentation.

EVIDENCE

- The homepage offers institutional linking and individual account registration, making independent confirmation of the intended access route an appropriate control.
- The stated commercial model includes subscriptions and institutional licensing, so billing, renewal, cancellation, and refund terms should be reviewed before payment.
- The reviewed content includes privacy and cookie information, which can be checked alongside the applicable account and payment terms.

Summary Verdict

Available evidence supports a high-trust, low-risk posture and is consistent with an established, apparently legitimate website. The classification is strong, while the connection between the website and a specific real-world operator remains unverified; legitimacy should therefore be understood as evidence-consistent rather than proven.

Infrastructure Integrity

The website is protected by Fastly CDN/WAF infrastructure and resolves through AS54113, operated by Fastly, Inc. in the United States. Four observed edge addresses are associated with that network, alongside one potential origin candidate; this architecture mitigates direct exposure of the service infrastructure but is not, by itself, proof of legitimacy.

Closing Assessment

Routine research access is proportionate to the assessed posture, while credentials or payments should be preceded by ordinary independent checks of the contracting entity, applicable terms, and available payment protections.

Written analysis generated 2026-08-17 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	25%

- 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 jstor.org.

- The request stayed on jstor.org. It was not redirected to another domain. CLEAR
- Registration is published under Network Solutions, LLC. CLEAR
- DNS for this domain is served by ithaka.org, across 7 name servers. NOTED
- The registration is paid up to 2031-02-17. CLEAR
- It is hosted on FASTLY, from a server in US. NOTED

Domain intelligence

Registrar	Network Solutions, LLC
Hosting	FASTLY - Fastly, Inc., US

Country	US
Server IP	199.232.172.152
Name servers	usnjpr2ns02.ithaka.org, usmiaa1ns03.ithaka.org, usnjpr2ns04.ithaka.org, usnjpr2ns01.ithaka.org, usnyny1ns05.ithaka.org, usaeaz1ns03.ithaka.org, usaeaz1ns05.ithaka.org
SSL issuer	GlobalSign Atlas R3 OV TLS CA 2026 Q2
SSL expiry	2027-02-01
Domain age	30.52 years (continuous registration)
Domain expiry	2031-02-17
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 jstor.org 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/jstor.org> · assessed 2026-08-17