

Is usc.edu legit? TrustSniffer's high-trust assessment: 100/100

usc.edu

Verdict

100

OUT OF 100

HIGH TRUST

usc.edu appears legitimate.

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

Not Scam

Low Risk

Assessed 2026-08-11 by automated analysis. Classification confidence 70%.

What this site appears to be

Official university website content covering academics, research, admissions, campus life, news, and events. Includes cookie/consent UI and contact/phone information for campuses and services. No financial investment solicitations or credential-harvesting elements detected.

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	41 years old Registered history	CLEAR
Web archive	Archived since 2006 1 snapshot	CLEAR
Certificate	Encrypted connection Issued by YR1	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 2006.
- No flags from the reputation services TrustSniffer consulted at assessment time.

Full analysis

Overview

The website is the official-looking informational presence of the University of Southern California, presenting academic programs, research and innovation, admissions and financial aid, campus life, news, events, and health and medical services. Its apparent purpose is to support higher-education communications, campus navigation, admissions activity, and institutional information rather than provide investment, custodial, or other financial services.

Scam/Impersonation Risk

No contradictions were observed. The homepage presents coherent university and institutional content, with no investment solicitation, cryptocurrency activity, credential-harvesting form, or suspected brand-impersonation element identified. External reputation signals are clean, and the site's strong global traffic footprint is consistent with an established public-facing institution. The available evidence therefore supports a low scam and impersonation risk, while not independently proving the real-world operator identity.

EVIDENCE

- The homepage identifies "University of Southern California" and covers academics, research, admissions, campus life, news, events, and health services; no financial solicitation or credential-harvesting element was detected.
- External checks recorded 0 malicious detections and 0 suspicious detections, with no phishing or other external threat hit.
- Domain registration: 1985-08-20; approximately 41 years old.
- Web archive: 1 snapshot dated 2006-05-12, spanning 2006–2006 with 1 year tracked; this is sparse archival coverage, not evidence of recent domain creation or repurposing.

Regulatory Verification Notes

The site's apparent business model is higher education, supported through tuition, research activity, philanthropy, healthcare services, and auxiliary services rather than regulated financial offerings. The reviewed content does not present a financial-services license or registration number; in this context, that is a scope and disclosure note rather than evidence of deception. Institutional branding, campus and service contact information, privacy notices, and cookie-consent controls provide a coherent public-facing disclosure framework. A separate broker-reputation dataset returned no match, which is contextual reputational support only and not a licensing determination.

EVIDENCE

- The homepage contains institutional branding and a privacy and cookie-consent notice describing necessary, functional, analytics, performance, and advertising cookies.
- The site's published content includes contact and telephone information for campuses and services.
- Served from AS54113 (FASTLY - Fastly, Inc., US).
- TLS certificate issued by YR1 (DV), valid to 2026-09-14.

What to Verify Next

Before any credential or payment interaction, an independent party should confirm that the relevant admissions, student, healthcare, or service channel corresponds to the institution's independently sourced contact details. Any payment should use established payment-protection mechanisms, and account activity should be limited to the service actually required. Where a regulated or licensed service is separately offered outside the reviewed informational scope, its authorization should be confirmed with the relevant official registry.

EVIDENCE

- The homepage is classified as informational and university-focused, with no sensitive form detected.
- The reviewed content includes admissions, financial-aid, campus, and service-navigation areas that can be cross-checked through independently sourced institutional contacts.
- The site provides privacy-notice and consent-management information relevant to account and browsing interactions.

Summary Verdict

The overall posture is **high trust and low risk**, and the available evidence is consistent with an established, apparently legitimate website. The real-world operator identity is not independently verified, so this assessment supports confidence in the site's observed legitimacy without treating that identity connection as proven.

Infrastructure Integrity

The site uses Cloudflare CDN/WAF protection, with observed edge infrastructure associated with Fastly in the United States. Edge delivery and a potential origin candidate were observed; this protective architecture reduces direct exposure of the service infrastructure but is a mitigating control, not proof of institutional legitimacy.

Closing Assessment

Normal informational browsing is proportionate; before submitting credentials or making payments, ordinary independent identity, service-channel, and payment-protection checks should be completed.

Written analysis generated 2026-08-11 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 usc.edu.

- The request stayed on usc.edu. It was not redirected to another domain. [CLEAR](#)
- The registration is paid up to 2027-07-31. [NOTED](#)
- The earliest public archive of this site is from 2006-05-12. [CLEAR](#)
- It is hosted on FASTLY, from a server in US. [NOTED](#)

Domain intelligence

Registrar	Not available
Hosting	FASTLY - Fastly, Inc., US
Country	US
Server IP	2620:12a:8001::3
Name servers	Not available
SSL issuer	YR1
SSL expiry	2026-09-14
Domain age	41.00 years (continuous registration)
Domain expiry	2027-07-31
Archive first seen	2006-05-12
Archive snapshots	1
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 usc.edu 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.

