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

ucsd.edu

Verdict

HIGH TRUST

ucsd.edu 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 70%.

What this site appears to be	Official University of California San Diego homepage content: navigation to admissions, academics, research, events, campus services, contact details and giving. No sign of credential harvesting or financial transaction forms on this page.

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** 2 snapshots	CLEAR
Certificate	**Encrypted connection** Issued by InCommon RSA Server CA 2	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 public University of California San Diego homepage, presenting admissions, academic programs, research, campus services, events, student support, health services, employment, and charitable giving. Its apparent purpose is to provide institutional information and facilitate university-related activities rather than direct commercial sales.

Scam/Impersonation Risk

No phishing, impersonation, blacklist, or other identity contradictions were observed. The homepage presents coherent university content, including admissions, research, campus services, and giving, and the available reputation checks were clean. Interactive testing did detect hidden forms, but there were no password-submission forms, wallet activity, credential-harvesting indicators, or financial transaction forms; this signal therefore does not establish a fraud pattern. The site appears legitimate and established, although the real-world operator identity remains independently unverified.

EVIDENCE

- The homepage is titled “University of California San Diego” and contains institutional navigation for admissions, academics, research, student life, health, employment, and giving.
- Domain registration: 1985-12-09; age 40.7 years; expiration 2028-07-31.
- Web-archive records: 2 snapshots spanning 2006–2007, covering 2 years.
- External reputation checks recorded 0 malicious detections, 0 suspicious detections, and no blacklist hit; traffic rank 1828.

Regulatory Verification Notes

The homepage supports an academic and public-service purpose rather than a regulated financial or commercial offering. No licensing or regulatory registration claim is presented on the supplied homepage; this is a transparency item to clarify only if a particular service or payment activity requires regulatory authorization, and it is not evidence of a scam. The page provides institutional contact and service pathways, while the available evidence is consistent with an established university website. A third-party broker-intelligence comparison produced no match, which is contextual reputation support rather than a legal or licensing determination.

EVIDENCE

- The homepage identifies the institution as University of California San Diego and links to admissions, financial aid, research, health, employment, and charitable giving services.
- Hosted on AS16509 (Amazon.com, Inc., US).
- TLS certificate issued by InCommon RSA Server CA 2, using OV validation, subject organization University of California, San Diego, valid to 2027-04-11.
- Page-authority assessment is in the high band.

What to Verify Next

Before credential or payment interactions, independently confirm that the intended university service and contact channel are reached through an independently sourced institutional route rather than an unsolicited message or advertisement. For donations or other payments, confirm the recipient, payment destination, applicable receipt process, and available payment protections. If a service is represented as requiring professional or regulatory authorization, confirm that authorization with the relevant official registry.

EVIDENCE

- The homepage provides navigation to “Give,” “Apply Now,” admissions, financial aid, and contact-related institutional services.
- The homepage analysis found no login form, sensitive form, untrusted form destination, or credential-harvesting indicator.
- The site’s stated business model is tuition-, grant-, donation-, and public-funding-supported academic activity rather than direct commercial sales.

Summary Verdict

Available evidence supports a high-trust, low-risk posture for an apparently legitimate and established institutional website. No contradictory scam or impersonation signals were identified, but independent connection of the website to the real-world operator has not been verified; that distinction should remain explicit in any formal onboarding or payment decision.

Infrastructure Integrity

The website is protected by a CDN/WAF layer, with observed edge infrastructure hosted by Amazon on AS16509; the origin server was not observable in this analysis. This is a mitigating infrastructure characteristic that reduces direct origin exposure, but it is not by itself proof of legitimacy.

Closing Assessment

Normal informational use is proportionate to the assessed posture; credential or payment interactions should proceed only after the ordinary independent institutional, destination, and payment-protection checks described above.

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	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 ucsd.edu.

- The request stayed on ucsd.edu. It was not redirected to another domain. CLEAR
- The registration is paid up to 2028-07-31. CLEAR
- The earliest public archive of this site is from 2006-05-06. 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	99.83.137.54
Name servers	Not available
SSL issuer	InCommon RSA Server CA 2
SSL expiry	2027-04-11
Domain age	40.70 years (continuous registration)
Domain expiry	2028-07-31
Archive first seen	2006-05-06
Archive snapshots	2
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 ucsd.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.

This report online: https://trustsniffer.com/report/ucsd.edu · assessed 2026-08-13