

Is colorado.edu legit? TrustSniffer's high-trust assessment: 94/100

colorado.edu

Verdict

94

OUT OF 100

HIGH TRUST

colorado.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 2026-08-12 by automated analysis. Classification confidence 55%.

What this site appears to be

Official homepage for the University of Colorado Boulder providing navigation to admissions, academics, research, events, and campus resources. The content is informational and geared toward prospective and current students, faculty, staff, and visitors.

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	40 years old Registered history	CLEAR
Web archive	Never archived No public history of this site	WATCH
Certificate	Encrypted connection Issued by Certainly Intermediate R1	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 University of Colorado Boulder website is an institutional academic portal presenting admissions, academics, research, campus events, visits, and student and campus resources for prospective and current students, faculty, staff, and visitors. Its apparent purpose is public information and university-service delivery rather than direct commercial activity.

Scam/Impersonation Risk

No contradictions were observed: the supplied evidence shows no phishing, impersonation, blacklist, or malicious-reputation indicators. The homepage presents a coherent university identity and informational purpose, supported by established domain tenure and broad institutional social presence. Automated interaction did observe hidden forms across two runs, but no password-external forms, wallet activity, cloaking, or login form was identified; this is treated as a behavioral implementation signal rather than evidence of deception. The homepage also contained no red-flag content.

EVIDENCE

- The domain record shows registration on 1986-06-02 and an age of 40.22 years.
- The homepage is titled "Home | University of Colorado Boulder" and provides navigation for admissions, academics, research, events, visits, and campus resources.
- Behavioral testing recorded hidden forms in 2 of 2 runs, while recording 0 password-external forms, 0 wallet-connect runs, 0 wallet-drainer runs, and no cloaking.
- External reputation checks recorded 0 malicious and 0 suspicious detections, with no blacklist or phishing result.

Regulatory Verification Notes

The homepage identifies the University of Colorado Boulder and operates as an academic and public-information site, not as a financial platform or broker. No licensing claim or registration number is presented in the supplied content; for this institutional use case, that is a disclosure item for ordinary identity and payment verification rather than evidence of a scam. The available identity evidence is consistent with the named institution, but the real-world operator connection remains likely rather than independently verified.

EVIDENCE

- The homepage describes an institutional university function and identifies University of Colorado Boulder as its organization.
- The site links to social profiles on Twitter, Facebook, Bluesky, Instagram, and LinkedIn; four were counted as trusted social signals.
- The site is served from AS54113 (FASTLY - Fastly, Inc., US).
- The transport certificate is issued by Certainly Intermediate R1, uses DV validation, and is valid to 2026-08-24T06:27:29+00:00.

What to Verify Next

Before credential or payment interactions, an organization should confirm the university identity and relevant service details through independently obtained institutional contact information rather than relying solely on links encountered during browsing. Where a transaction involves tuition, donations, applications, or other payment activity, the recipient, payment destination, refund or withdrawal terms, and available payment protections should be checked against official university records.

EVIDENCE

- The homepage provides institutional navigation for admissions, visits, and campus resources that can be used to locate the appropriate official service route.
- The supplied homepage analysis identified one search/newsletter form and no sensitive form destination, supporting a separation between ordinary public browsing and any later credential or payment workflow.

Summary Verdict

Available evidence is consistent with an established, apparently legitimate website with a high-trust, low-risk posture and no observed scam or impersonation contradictions. The classification is strong, while the operator's real-world identity should remain described as likely rather than proven.

Infrastructure Integrity

The site is protected by Fastly CDN/WAF infrastructure, and all observed addresses were CDN edge servers; no origin candidate was identified in the analysis. This provides a meaningful exposure-mitigation layer but is not, by itself, proof of institutional legitimacy.

EVIDENCE

- The infrastructure record identifies Fastly CDN/WAF protection across 8 observed edge addresses and 0 likely origin addresses.

Closing Assessment

Normal informational use is proportionate to the assessment; before submitting credentials or making payments, ordinary independent checks of institutional identity, transaction terms, and payment protection should be completed.

What the analysis found

No rule findings contributed to this verdict.

Identity verification

Status	LIKELY
Identity score	80/100
Identity verification confidence	80%

- Identity verified on page
- 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 colorado.edu.

- The request stayed on colorado.edu. It was not redirected to another domain. CLEAR
- The registration is paid up to 2027-07-31. NOTED
- 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	2a04:4e42:6b::645
Name servers	Not available
SSL issuer	Certainly Intermediate R1
SSL expiry	2026-08-24
Domain age	40.22 years (continuous registration)
Domain expiry	2027-07-31
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 colorado.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/colorado.edu> · assessed 2026-08-12