

Is nps.gov legit? TrustSniffer's high-trust assessment: 100/100

nps.gov

Verdict

100

OUT OF 100

HIGH TRUST

nps.gov appears legitimate.

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

Not Scam

Low Risk

Assessed 2026-08-13 by automated analysis. Classification confidence 70%.

What this site appears to be

Official U.S. National Park Service homepage providing navigation to parks, trip planning, educational resources, events, and ways to get involved. Content is informational and public-facing.

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	29 years old Registered history	CLEAR
Web archive	Archived since 2004 2 snapshots	CLEAR
Certificate	Encrypted connection Issued by DigiCert Global G2 TLS RSA SHA256 2020 CA1	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 2004.
- No flags from the reputation services TrustSniffer consulted at assessment time.

Full analysis

Overview

The website is the official-looking public-service homepage of the U.S. National Park Service, presenting visitors with navigation to national parks, trip planning, events, passes, educational resources, news, volunteering, donations, and other ways to engage with the agency.

Scam/Impersonation Risk

No scam, phishing, impersonation, or other contradictory signals were observed. The homepage presents a coherent U.S. government public-service purpose, uses official government-site messaging, and contains no detected red flags or suspicious interaction patterns. The domain's long registration history, strong global traffic footprint, and clean external reputation are consistent with an established site rather than a newly created impersonation. The apparent institutional identity is supported by the page content, although independent linkage to the real-world operator is not treated as conclusively verified.

EVIDENCE

- The homepage identifies itself as the "U.S. National Park Service" and displays official-government and secure-government-site messaging.
- The domain was registered in 1997 and is approximately 28.88 years old; registrar: get.gov.
- The domain has 2 archive snapshots spanning 2004–2004, with 1 year tracked.
- External reputation checks recorded 0 malicious detections, 0 suspicious detections, and no detected blacklist or phishing contradiction; the site's traffic rank was 1814.

Regulatory Verification Notes

The site presents an informational government-service model rather than a financial, brokerage, or other commercially regulated activity. Its pages describe park information, trip planning, education, events, and public participation, so a financial-services license is not implicated by the stated purpose. The on-page government designation is a strong legitimacy signal, but it should not be treated as independent proof of the real-world operator's identity. No separate broker or financial-services reputational match was identified.

EVIDENCE

- The homepage is categorized as “Government / Public Service” and provides public information and services concerning U.S. national parks.
- The site is served from AS14618, operated by AMAZON-AES — Amazon.com, Inc., US.
- Transport security uses an OV certificate issued by DigiCert Global G2 TLS RSA SHA256 2020 CA1; the certificate is valid to 2026-08-30T23:59:59+00:00.
- The page content contains no login form, sensitive form, untrusted form destination, or detected red-flag item.

What to Verify Next

Before any credential or payment interaction, ordinary independent checks should confirm that the relevant transaction or account flow is reached through an independently obtained official government channel. Where a payment is involved, the applicable terms, refund or return arrangements, and payment-protection options should also be reviewed before completion.

EVIDENCE

- The homepage provides an “An official website of the United States government” disclosure and explains how official government websites can be recognized.
- Observed homepage behavior recorded no wallet connection, wallet-sensitive activity, hidden forms, password-external forms, or suspicious inline scripts.
- The site’s stated purpose is public information and service delivery, not a commercial investment or financial product offering.

Summary Verdict

The overall posture is **high trust and low risk**, with available evidence consistent with an established, apparently legitimate public-service website. No contradictory risk signals were identified, while operator identity remains independently unverified rather than proven.

Infrastructure Integrity

The site is protected by Cloudflare CDN/WAF infrastructure, which mitigates direct exposure of the service environment. All observed addresses were CDN edge addresses, with no origin candidate identified during the infrastructure assessment; this is a protective architecture signal, not independent proof of legitimacy.

Closing Assessment

Normal browsing and ordinary site use are proportionate to the assessed posture, while independent confirmation of the official transaction or credential channel remains appropriate before sensitive actions.

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	30%

- 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 nps.gov.

- The request stayed on nps.gov. It was not redirected to another domain. CLEAR
- Registration is published under get.gov. CLEAR
- DNS for this domain is served by cloudflare.com, across 2 name servers. NOTED
- The registration is paid up to 2027-08-29. NOTED
- The earliest public archive of this site is from 2004-11-01. CLEAR
- It is hosted on AMAZON-AES, from a server in US. NOTED

Domain intelligence

Registrar	get.gov
Hosting	AMAZON-AES - Amazon.com, Inc., US
Country	US
Server IP	2600:9000:20aa:0:1:983:9400:93a1
Name servers	ivan.ns.cloudflare.com, lucy.ns.cloudflare.com
SSL issuer	DigiCert Global G2 TLS RSA SHA256 2020 CA1
SSL expiry	2026-08-30
Domain age	28.88 years (continuous registration)
Domain expiry	2027-08-29
Archive first seen	2004-11-01
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 nps.gov 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/nps.gov> · assessed 2026-08-13