

Is liteblue-usps-gov.com a scam? TrustSniffer's high-risk assessment: 0/100

liteblue-usps-gov.com

Verdict

0

OUT OF 100

CRITICAL RISK

liteblue-usps-gov.com shows high-risk / scam indicators.

This assessment found strong scam indicators. Do not pay, sign in, or share personal details with this site.

Sensitive Interaction Risk

Governance Risk

Assessed 2026-08-21 by automated analysis. Classification confidence 55%.

WHAT THIS SITE APPEARS TO BE

A WordPress blog (Humapk11) with posts focused on online earning, remote jobs, apps, AI and regional guides. Content appears informational; no login, payment flows, or credential collection visible in provided 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	13 flagged it VirusTotal	RISK
Google Safe Browsing	Listed as unsafe Google	RISK
Abuse reports on the host	0 reports AbuseIPDB; shared hosting inflates this count	NOTED
Domain age	2.5 years old Registered history	CLEAR
Web archive	Archived since 2024 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YE2	NOTED

The page as captured

https://liteblue-usps-gov.com/

August 21, 2026

Humapk11

Humapk11, HUMAPK11, humapk 11

MAIN MENU

What liteblue-usps-gov.com served when TrustSniffer captured it on 2026-08-21. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: 1 to 3 years (registration continuity).
- Public web-archive history exists since 2024.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

Fortinet, Google, Kaspersky, Sophos flagged this site in external intelligence checks, indicating elevated compromise/scam exposure that requires immediate caution.

This website presents itself to visitors as “Humapk11,” a WordPress information blog publishing articles on online earning, remote work, applications, artificial intelligence, financing, and regional guides. Its apparent model is ad-supported or affiliate-supported publishing rather than direct financial services, although the domain name uses a USPS-like formulation that is not consistent with the site's visible editorial identity.

Scam/Impersonation Risk

The site carries a clearly elevated security concern because the domain is subject to a confirmed blacklist signal, including a malicious classification by Google Safe Browsing and multiple malicious detections from major security providers. The domain's USPS-like naming, contrasted with the unrelated “Humapk11” blog presentation, creates an identity concern even though page-level analysis did not establish confirmed brand impersonation or a visible phishing form. No confirmed legal-entity identity contradiction was observed, but the external detections are sufficient to make login, credential submission, and financial interaction inappropriate.

The absence of visible login, payment, wallet, or credential-collection mechanisms reduces the observed interaction surface; it does not offset the external threat findings.

EVIDENCE

- The domain is marked malicious by Google Safe Browsing and is listed in external blacklist data.
- Security scanning recorded 13 malicious detections and 1 suspicious detection, with Fortinet, Google, Kaspersky, and Sophos among the flagged providers.
- The domain was registered on 2024-02-11 and is approximately 2.52 years old.
- Archive records show 22 snapshots spanning 2024-04-16 to 2026-03-12, tracked across 3 years.

Regulatory Verification Notes

The visible site includes About Us, Contact Us, Disclaimer, and Privacy Policy pages, but the supplied content does not establish a verifiable operating entity, regulated status, or licensing authority. No license claim or license number is disclosed in the available business-model evidence. This is a material transparency gap for any activity that could be interpreted as employment, financing, or money-making advice, but it is a regulatory-verification issue rather than independent proof of fraud. The site's informational presentation and lack of transactional forms do not provide a basis for treating it as a regulated financial service.

EVIDENCE

- The homepage identifies the site as "Humapk11" and presents WordPress blog content rather than a named regulated institution.
- The available navigation includes About Us, Contact Us, Disclaimer, and Privacy Policy pages; no license authority or registration number is supplied in the reviewed business disclosures.
- The hosting network is AS13335, Cloudflare, Inc. (CLOUDFLARENET - Cloudflare, Inc., US).
- The site's TLS certificate is issued by YE2 at DV validation level and is valid to 2026-10-22T05:47:24+00:00.

What to Verify Next

Before any sensitive interaction, an institution should independently confirm whether the domain has any legitimate connection to the organization suggested by its naming, using an official government or corporate channel rather than contact details supplied by the site. Any employment, financing, monetization, or referral claim should be checked against the named provider's official service pages and, where applicable, the relevant licensing or corporate registry. Browser and endpoint security teams should also treat the external threat warnings as a reason to block or isolate access pending a documented business justification.

EVIDENCE

- The domain naming and the homepage's "Humapk11" identity are materially different from one another and require independent ownership or affiliation confirmation.
- The reviewed homepage contains no login form, sensitive form, hidden form, external password form, wallet connection, or payment flow.
- The site is identified as a WordPress blog using the HitMag theme, with content focused on online earning, remote jobs, applications, AI, financing, and regional guides.

Summary Verdict

The overall posture is **critical and unsuitable for sensitive interaction**. The site has an informational appearance and limited observed transaction surface, but those benign characteristics are outweighed by confirmed external threat contradictions and the absence of independently verified operator identity. Passive viewing does not establish that the site is legitimate or appropriate for trusted business use.

Infrastructure Integrity

The website is protected by Cloudflare CDN/WAF infrastructure, and all observed addresses were CDN edge servers rather than a directly exposed origin. This provides a meaningful mitigation against straightforward origin exposure, but it is only a protective infrastructure signal and cannot counter the site's external reputation findings or independently establish legitimacy.

Closing Assessment

Access should be limited to controlled, passive review, with no account login, credential submission, financial transaction, download, or other sensitive interaction unless the domain's legitimacy has first been established through an independent authoritative channel.

Written analysis generated 2026-08-21 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

2 findings contributed to this verdict, raised by registration and ownership, analysis engine, external reputation.

01 Governance Risk

- The public registration record for this domain is incomplete.

Registration and ownership rule:KF_WHOIS_INCOMPLETE

02 Sensitive Interaction Risk

- The analysis matched a pattern TrustSniffer treats as a direct threat to a visitor.

Analysis engine signal:direct_threat

- An external threat feed lists this domain: either Google Safe Browsing marked it malicious, or a significant number of malware engines flagged it.

External reputation rule:EXT_BLACKLIST_CRITICAL

Identity verification

Status	UNVERIFIED
Identity score	30/100
Identity verification confidence	50%

- 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 liteblue-usps-gov.com.

- The request stayed on liteblue-usps-gov.com. It was not redirected to another domain. CLEAR
- Registration is published under Dynadot Inc. CLEAR
- DNS for this domain is served by cloudflare.com, across 2 name servers. NOTED
- The registration is paid up to 2027-02-11. NOTED
- The earliest public archive of this site is from 2024-04-16. CLEAR
- It is hosted on CLOUDFLARENET, from a server in US. NOTED

Domain intelligence

Registrar	Dynadot Inc
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US
Server IP	2606:4700:3035::6815:4fa8
Name servers	AMBER.NS.CLOUDFLARE.COM, COSMIN.NS.CLOUDFLARE.COM
SSL issuer	YE2
SSL expiry	2026-10-22
Domain age	2.52 years (continuous registration)
Domain expiry	2027-02-11
Archive first seen	2024-04-16
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 13 flagged AbuseIPDB: 0 reports Google Safe Browsing: 1 match

About this assessment

A trust score summarises the evidence TrustSniffer could collect about liteblue-usps-gov.com 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/liteblue-usps-gov.com> · assessed 2026-08-21