

Is xn--yet824cpd.vip a scam? TrustSniffer's high-risk assessment: 0/100

xn--yet824cpd.vip

Verdict

0

OUT OF 100

CRITICAL RISK

xn--yet824cpd.vip 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

GPT summary status=skipped | No usable content for GPT summary (clean/dom/html all empty)

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.

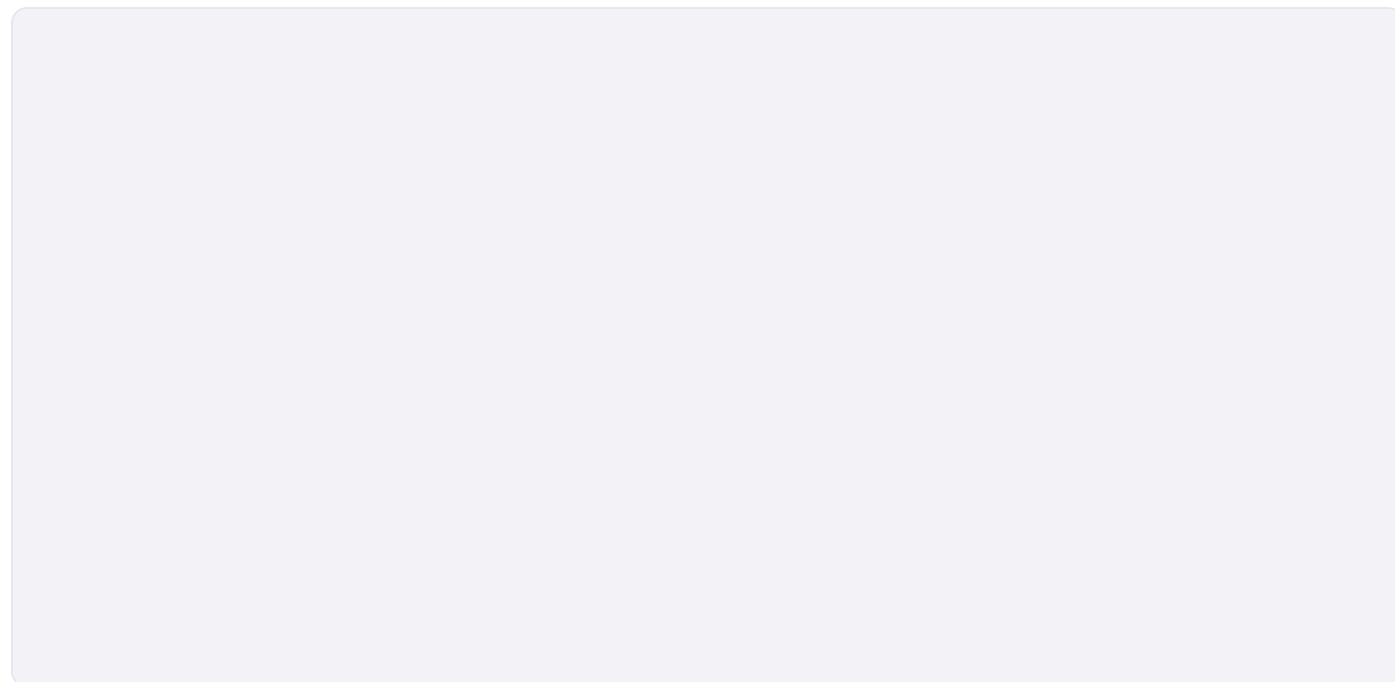
At a glance

The checks that decide most of this verdict.

Malware engines	17 flagged it VirusTotal	RISK
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	0 reports AbuseIPDB; shared hosting inflates this count	NOTED
Domain age	1.2 years old Registered history	CLEAR
Web archive	Archived since 2025 Public history exists	CLEAR
Certificate	Encrypted connection Issued by WE1	NOTED

The page as captured

https://qunekp.walletstore.app/web_home_cn/



What xn--yet824cpd.vip 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 2025.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

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

This website is an online domain whose available page material does not identify a product, operator, or clear business model; its intended purpose therefore cannot be reliably characterized from the supplied website evidence.

Scam/Impersonation Risk

The domain presents a **critical sensitive-interaction risk** because external security-reputation checks identify it as blacklisted and multiple major security providers classify it as malicious or suspicious. This is a material contradiction to ordinary trust expectations, although the available evidence does not establish brand impersonation, conflicting legal identities, or confirmed phishing. The domain is also relatively young, which provides limited operating history in comparison with an established service. Evidence:

- External reputation telemetry recorded 17 malicious and 2 suspicious detections, with Fortinet, Kaspersky, and Sophos among the flagged providers.

- The domain was registered on 2025-06-22 and is approximately 1.16 years old.
- Historical records show first observation on 2025-07-19 and last observation on 2026-03-08, covering 2 years of tracked history.

Regulatory Verification Notes

The real-world operator identity remains unverified, and the available evidence does not establish a clear licensing or regulatory disclosure. This is a verification gap rather than a standalone finding of fraud, but it is significant given the external malicious detections. A valid transport certificate and mainstream hosting infrastructure confirm technical configuration only; they do not establish that the operator is legitimate or authorised.

EVIDENCE

- The site is served through AS13335, CLOUDFLARENET — Cloudflare, Inc., US.
- The transport certificate is issued by WE1, uses Domain Validation (DV), and is valid until 2026-09-22T02:15:54+00:00.
- The available identity-verification status is unknown, with no independently verified connection to a real-world operator.

What to Verify Next

Before any sensitive interaction, an independent source should confirm the legal operator, applicable licence or registration, and the service's official support channels. Credentials, account creation, payments, fund transfers, and other financial actions should remain withheld unless those checks produce authoritative, independently sourced confirmation. Evidence:

- The available website evidence does not provide a sufficiently established basis for independently confirming the operator.
- The regulatory disclosure state is unclear, requiring confirmation through the relevant official registry where regulated activity is claimed.
- The domain is subject to external malicious and blacklist detections, making independent confirmation a prerequisite for sensitive use.

Summary Verdict

The overall posture is critical and unsuitable for sensitive interaction. The available evidence does not support treating the site as trustworthy for login, credential submission, or financial activity.

Infrastructure Integrity

Cloudflare CDN/WAF protection is present and all observed addresses are CDN edge servers rather than identified origin infrastructure. This provides a useful mitigation against direct exposure of the hosting environment, but it is only a protective infrastructure characteristic and does not offset the site's external reputation risk.

EVIDENCE

- CDN/WAF provider: Cloudflare; observed edge addresses: 104.21.56.59 and 172.67.178.197.
- Both observed edge addresses resolve through AS13335; likely origin IP count: 0.
- Hosting provider: CLOUDFLARENET — Cloudflare, Inc., US; registry: ARIN; country: US.

Closing Assessment

Prospective users should restrict activity to passive viewing and avoid sensitive interaction unless independent identity, authorisation, and channel verification has been completed.

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

- Registration details are held behind a privacy service, so no operator is named publicly. This is common and legal, and it also means there is nobody to check.

Registration and ownership rule:KF_WHOIS_PRIVATE

- The registration record withholds contact details for the operator.

Registration and ownership rule:KF_WHOIS_HIDDEN

02 Sensitive Interaction Risk

- The analysis matched a pattern TrustSniffer treats as a direct threat to a visitor.
- An external threat feed lists this domain: either Google Safe Browsing marked it malicious, or a significant number of malware engines flagged it.

Analysis engine signal:direct_threat

External reputation rule:EXT_BLACKLIST_CRITICAL

Identity verification

Status	UNKNOWN
Identity score	50/100
Identity verification confidence	15%

- AI page analysis unavailable (page captured; identity not AI-verified)

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 xn--yet824cpd.vip.

- The request for xn--yet824cpd.vip ended on qunekp.walletstore.app, a different domain. WATCH

- Registration is published under Chengdu west dimension digital technology Co., LTD. CLEAR
- DNS for this domain is served by dnspod.net, across 2 name servers. NOTED
- The registration is paid up to 2027-06-22. NOTED
- The earliest public archive of this site is from 2025-07-19. CLEAR
- It is hosted on CLOUDFLARENET, from a server in US. NOTED

Domain intelligence

Registrar	Chengdu west dimension digital technology Co., LTD
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US
Server IP	172.67.178.197
Name servers	kent.dnspod.net, lee.dnspod.net
SSL issuer	WE1
SSL expiry	2026-09-22
Domain age	1.16 years (continuous registration)
Domain expiry	2027-06-22
Archive first seen	2025-07-19
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 17 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about xn--yet824cpd.vip 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/xn--yet824cpd.vip> · assessed 2026-08-21