

Is 13yxw.com a scam? TrustSniffer's high-risk assessment: 0/100

13yxw.com

Verdict

0

OUT OF 100

CRITICAL RISK

13yxw.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 2026-08-18 by automated analysis. Classification confidence 70%.

What this site appears to be

Chinese-language landing page for a multi-chain crypto wallet named 'tokenim' offering app downloads, key/seed management guidance, and DApp access. Provides marketing claims (user counts, chains supported) but no visible verifiable audits, legal entity, or direct download links to validated stores on the page snapshot.

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	14 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	2.4 years old Registered history	CLEAR
Web archive	Archived since 2013 20 snapshots	CLEAR
Certificate	Encrypted connection Issued by LiteSSL RSA CA 2025	NOTED

The page as captured

<https://13yxw.com/>

404 Not Found

nginx

What 13yxw.com served when TrustSniffer captured it on 2026-08-18. 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 2013.
- 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.

The website is a Chinese-language product landing page for “tokenim,” presenting a multi-chain cryptocurrency wallet with app-download prompts, private-key and seed-phrase management guidance, and access to decentralised applications. Its apparent business model is the distribution of a crypto-wallet application, with possible ancillary exchange and DApp functionality.

Scam/Impersonation Risk

The site presents a high-stakes crypto-wallet proposition while making substantial claims—including support for BTC, ETH, BSC, TRON, Aptos, Polygon, Solana, Cosmos, Polkadot, EOS, and IOST, as well as claims of more than 20 million users, 30 million daily transactions, and availability across more than 200 countries—without visible audit evidence, independently validated app-store destinations, or corroborating corporate information in the captured content. This claim-and-evidence gap is significant because the site instructs users on importing wallets and handling private keys or recovery phrases. No distinct legal-entity identity contradiction or page-level brand impersonation was observed, but independent security assessments produced malicious and suspicious

detections, and the domain is confirmed as blacklisted by external sources. The observed absence of a login form or wallet-drainer behavior does not offset the external reputation findings for a site promoting software and sensitive digital-asset handling.

EVIDENCE

- External security assessment: 14 malicious detections and 3 suspicious detections from 22 evaluated results; three major security providers flagged the domain.
- Homepage: advertised “tokenim” wallet support for multiple named blockchain networks, on-device private-key and seed-phrase storage, wallet import using seed phrases or private keys, and DApp access.
- Domain registration record: registered 2024-03-29 (~2.39 years old) through GoDaddy.com, LLC.
- Web archive: 20 snapshots spanning 2013-07-17 to 2026-05-20, covering 14 tracked years.

Regulatory Verification Notes

The captured site content does not visibly identify a verifiable legal entity, provide a licensing or registration number, or present independent security-audit documentation. Those omissions are regulatory and transparency verification gaps rather than, by themselves, proof of fraud; however, they materially limit the ability to establish who operates the wallet service or what oversight applies to any associated exchange or financial functionality. The available evidence supports an unverified operator identity, while the external blacklist status remains the principal adverse trust signal. No broker-reputation match was identified in the supplied third-party context.

EVIDENCE

- Homepage and navigation: “About,” “Features,” “Tools,” and FAQ content were present, but no verifiable corporate identity, licence, registration number, or audit certificate was visible.
- Hosting telemetry: served from AS54801, ZILLION-NETWORK - Zillion Network Inc., US.
- Transport telemetry: DV TLS certificate issued by LiteSSL RSA CA 2025, valid to 2026-09-23.
- Page authority telemetry: authority classified in the mid band, without any resulting trust reclassification.

What to Verify Next

Before any sensitive interaction, an independent party should confirm the legal operator and any applicable virtual-asset, money-services, or exchange licensing through the relevant official registry. The official application listing should be reached through an independently verified developer account, with the publisher identity, package signature, download provenance, and security-audit claims checked separately from the website. Recovery phrases, private keys, wallet imports, credentials, and funds should not be supplied unless those checks produce reliable and independently corroborated results. Official support channels should also be confirmed through an independent route rather than relying solely on the website.

EVIDENCE

- Homepage capture: app-store labels were displayed, but no direct links to validated official store listings were visible.
- Observed page behavior: two successful runs showed zero external XHR or fetch requests, no hidden forms, no sensitive-form submission, and no wallet-connect or wallet-drainer execution.
- Site metadata: no structured data, canonical declaration, or meta description was detected, limiting independent validation of publisher information.

Summary Verdict

The overall posture is **critical trust risk**, with sensitive interaction risk driven by confirmed external blacklist status and malicious detections. The website's apparent legitimacy and operator identity remain unverified, and the available presentation does not provide a sufficient basis for trusting software distribution or digital-asset handling.

Infrastructure Integrity

The site resolves to one identified origin address hosted by ZILLION-NETWORK - Zillion Network Inc. in the United States, on AS54801, with no CDN or WAF edge layer identified. The valid DV TLS certificate provides transport encryption only and should be treated as a limited technical control, not as evidence of operator legitimacy.

Closing Assessment

The appropriate institutional posture is to restrict activity to passive viewing and prevent downloads, wallet connections, credential submission, or financial transfers until independent identity, application provenance, and regulatory checks are satisfactorily completed.

Written analysis generated 2026-08-18 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 registration record withholds contact details for the operator.
Registration and ownership rule:KF_WHOIS_HIDDEN
- 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

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	25%

- 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 13yxw.com.

- The request stayed on 13yxw.com. It was not redirected to another domain. CLEAR
- Registration is published under GoDaddy.com, LLC. CLEAR
- DNS for this domain is served by domaincontrol.com, across 2 name servers. NOTED
- The registration is paid up to 2027-03-29. NOTED
- The earliest public archive of this site is from 2013-07-17. CLEAR
- It is hosted on ZILLION-NETWORK, from a server in US. NOTED

Domain intelligence

Registrar	GoDaddy.com, LLC
Hosting	ZILLION-NETWORK - Zillion Network Inc., US
Country	US
Server IP	154.39.192.197
Name servers	NS05.DOMAINCONTROL.COM, NS06.DOMAINCONTROL.COM
SSL issuer	LiteSSL RSA CA 2025
SSL expiry	2026-09-23
Domain age	2.39 years (continuous registration)
Domain expiry	2027-03-29
Archive first seen	2013-07-17

Archive snapshots	20
Reputation	VirusTotal: 14 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about 13yxw.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/13yxw.com> · assessed 2026-08-18