

# Is 2366xyx.com a scam? TrustSniffer's high-risk assessment: 0/100

2366xyx.com

## Verdict

0

OUT OF 100

CRITICAL RISK

2366xyx.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 advertising a multi-chain cryptocurrency wallet called 'tp官方安卓最新版本' / TPWallet with feature claims (multi-chain support, on-device key storage, multi-sig, DApp access), download links, user/testimonial snippets and unverified usage statistics. The page reads like promotional marketing and contains guides and articles about wallets and transfers.

## 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<br>VirusTotal                                | RISK  |
| Google Safe Browsing      | Not listed<br>Google                                       | CLEAR |
| Abuse reports on the host | 0 reports<br>AbuseIPDB; shared hosting inflates this count | NOTED |
| Domain age                | 4.7 years old<br>Registered history                        | CLEAR |
| Web archive               | Archived since 2021<br>17 snapshots                        | CLEAR |

## The page as captured

<https://2366xyx.com/>

# 404 Not Found

nginx

What 2366xyx.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: 3 to 10 years (registration continuity).
- Public web-archive history exists since 2021.
- 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 promotional landing page for “TPWallet,” presenting a downloadable multi-chain cryptocurrency wallet with on-device key and seed-phrase storage, multi-signature functionality, DApp access, and links purporting to support major mobile-app platforms.

### Scam/Impersonation Risk

**The site presents a material sensitive-interaction risk.** Its homepage combines a crypto-wallet download proposition with high-stakes security claims, including sole user control of private keys and seed phrases, cold-wallet and multi-signature capabilities, and broad support for assets and networks such as BTC, ETH, BSC, TRON, Aptos, Polygon, Solana, Cosmos, Polkadot, EOS, IOST, and USDT. It also displays unverified counters claiming 2,000,000 users, 3,000,000 daily transactions, coverage across 200 countries and regions, and

50,000,000 in daily transaction volume; the available page evidence does not substantiate these claims. Independent reputation evidence records a confirmed blacklist and multiple malicious detections, including coverage from Fortinet, Kaspersky, and Sophos. No identity contradiction between distinct legal entities was observed, but the reputation findings are sufficient to make credential submission, application installation, wallet connection, or financial activity inappropriate. Evidence:

- The homepage advertises the TPWallet application, download links, multi-chain asset management, on-device key storage, multi-signature protection, and DApp access.
- The homepage displays the stated user, transaction, geographic-coverage, and transaction-volume counters without supporting evidence.
- External reputation telemetry records 17 malicious detections, 0 suspicious detections, and a confirmed blacklist.
- The domain registration record shows creation on 2023-11-13 and a reported age of 2.76 years; archival coverage contains 17 snapshots spanning 2021–2026, with 6 years tracked.

### **Regulatory Verification Notes**

The available landing-page content does not identify a licensing authority, registration number, or clearly named operating entity. That is a regulatory and disclosure gap requiring independent verification, rather than standalone proof of fraud. The site's apparent wallet and digital-asset functionality creates a need to establish which entity operates the service and whether any applicable authorization exists before engagement. Its independently unverified identity further prevents the on-site branding and security assertions from being treated as proof of a real-world operator. Evidence:

- The homepage presents a digital-asset wallet service but contains no stated license claim, license number, or regulatory authority.
- The site's transport encryption is a DV certificate issued by YR1, valid to 2026-09-27T07:31:26+00:00.
- Hosting telemetry identifies AS54801 operated by ZILLION-NETWORK - Zillion Network Inc., US.
- The domain registrar is GoDaddy.com, LLC, with an expiration date of 2026-11-13T19:30:04Z.

### **What to Verify Next**

Any prospective assessment should first obtain the official publisher identity for the application and independently compare it with the publisher shown in the relevant official app-store listing. Applicable digital-asset licensing or registration should be checked directly with the competent registry using the operator's legal name, not links or claims supplied by the site. Contact channels should be confirmed through an independently sourced route, and no credentials, recovery phrases, private keys, payment details, or wallet authorizations should be entered while those checks remain unresolved. Evidence:

- The homepage's high-stakes security and usage claims require confirmation from independently attributable documentation.
- The absence of a stated licensing authority or registration number makes direct registry verification necessary.
- The confirmed external reputation findings require validation of the application publisher and distribution channel before installation.

Summary Verdict

The website has a **critical trust posture** for sensitive interaction. The combination of confirmed external threat detections, an unverified operator identity, and unsupported high-stakes claims means the site should not be treated as an established or dependable service for credentials, wallet access, or financial activity.

Infrastructure Integrity

The site resolves to a single likely origin IP, with no CDN edge or detected WAF vendor providing an additional separation layer. This infrastructure configuration does not itself establish malicious intent, but it offers limited protective mitigation against the reputation concerns identified above.

Closing Assessment

The proportionate course is to refrain from installation and sensitive interaction unless the application publisher, operator identity, applicable authorization, and distribution channel are independently confirmed through trusted sources.

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

- 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.

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 2366xyx.com.

- The request stayed on 2366xyx.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 2026-11-13. NOTED
- The earliest public archive of this site is from 2021-11-23. CLEAR
- It is hosted on ZILLION-NETWORK, from a server in SC. NOTED

## Domain intelligence

|                    |                                                                                 |
|--------------------|---------------------------------------------------------------------------------|
| Registrar          | GoDaddy.com, LLC                                                                |
| Hosting            | ZILLION-NETWORK - Zillion Network Inc., US                                      |
| Country            | SC                                                                              |
| Server IP          | 156.239.182.3                                                                   |
| Name servers       | NS59.DOMAINCONTROL.COM, NS60.DOMAINCONTROL.COM                                  |
| SSL issuer         | YR1                                                                             |
| SSL expiry         | 2026-09-27                                                                      |
| Domain age         | 4.73 years (continuous registration)                                            |
| Domain expiry      | 2026-11-13                                                                      |
| Archive first seen | 2021-11-23                                                                      |
| Archive snapshots  | 17                                                                              |
| 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 2366xyx.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.