

Is 1207f.com a scam? TrustSniffer's high-risk assessment: 0/100

1207f.com

Verdict

0

OUT OF 100

CRITICAL RISK

1207f.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 cryptocurrency wallet app promoting downloads, multi-chain support, security features (on-device key generation, multisig), DApp access, and tutorials. Contains marketing metrics and FAQs but lacks clear verifiable corporate/regulatory disclosures.

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	16 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	4.7 years old Registered history	CLEAR
Web archive	Archived since 2021 15 snapshots	CLEAR
Certificate	Encrypted connection Issued by YR2	NOTED

The page as captured

https://1207f.com/

404 Not Found

nginx

What 1207f.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.

This website is a Chinese-language promotional landing page for a mobile and desktop cryptocurrency wallet application, presenting multi-chain asset management, wallet-security features, decentralized-application access, tutorials, and download options for prospective users.

Scam/Impersonation Risk

The site presents itself as an official cryptocurrency-wallet service, but the available evidence includes a confirmed blacklist status and multiple malicious threat detections, creating a material risk for sensitive interaction. The homepage promotes support for BTC, ETH, BSC, TRON, Aptos, Polygon, Solana, Cosmos, Polkadot, EOS, and IOST; claims that private keys and recovery phrases are generated and stored only on the user's device; and advertises multisignature and cold-wallet capabilities. It also displays highly specific usage figures—2,000,000 users, 3,000,000 daily transactions, 200 countries or regions, and 50,000,000 in daily transaction volume—without supporting corporate or independently verifiable evidence. These claim-evidence inconsistencies, together with the external detections, materially outweigh the absence of observed login forms,

wallet-drainer activity, clipboard hijacking, or suspicious outbound network activity. No separate brand-impersonation or conflicting legal-identity finding was established, but the blacklist and malicious-detection signals are sufficient to make downloads, credentials, wallet access, and financial activity inappropriate.

EVIDENCE

- External reputation checks recorded 16 malicious detections and 1 suspicious detection, including threat identification by three major security vendors; the domain was also present on an external blacklist.
- The homepage displays the unsupported service metrics of 2,000,000 users, 3,000,000 daily transactions, 200 countries or regions, and 50,000,000 in daily transaction volume.
- The domain registration record shows 2023-12-26T19:37:08Z; the registration record reports an age of 2.64 years, while reconciled historical analysis reports a domain age of 4.73 years.
- Historical captures comprise 15 snapshots spanning 2021–2026, with 6 years tracked.

Regulatory Verification Notes

The website's legal and identity presentation is insufficiently clear for a service involving digital-asset custody or wallet distribution. The available page content does not provide a clearly verifiable corporate entity, regulatory status, license number, or licensing authority, and the published claims about security and global adoption are not matched by clear supporting disclosures. This is a regulatory-transparency gap rather than, by itself, proof of fraud; however, in combination with the confirmed external blacklist and malicious detections, it prevents a favorable legitimacy determination. The available third-party broker context produced no matching result, which does not establish authorization or safety.

EVIDENCE

- The homepage and support content describe a wallet, DApp access, and digital-asset services but contain no clear verifiable corporate or regulatory disclosure.
- The site's transport encryption is a DV certificate issued by YR2, valid until 2026-09-27.
- The site is hosted on AS54801, ZILLION-NETWORK – Zillion Network Inc., US; the resolved infrastructure is registered through AFRINIC and geolocated to SC.
- Page analysis identified missing structured metadata and no clear canonical identity information.

What to Verify Next

Before any interaction, an organization should independently identify the application publisher through official app-store records and confirm that the publisher, domain, support channels, and wallet software are controlled by the same legal entity. Any claimed registration, authorization, or custody-related status should be checked directly with the relevant regulator or corporate registry rather than through links or contact details supplied by the site. The application should not be downloaded from this landing page, and no credentials, recovery phrases, private keys, wallet connections, or funds should be provided unless those independent checks resolve the reputation concerns.

EVIDENCE

- The homepage offers App Store and Google Play download prompts but does not establish the publisher's legal identity.
- The site provides wallet-security and DApp-access claims without independently verifiable governance or licensing documentation.
- Independent verification is required for the publisher, corporate entity, regulatory status, and official support channels before sensitive use.

Summary Verdict

The website has a **critical trust posture** and its operator identity remains unverified. Confirmed external blacklist and malicious-detection signals, reinforced by unsupported marketing claims and unclear legal disclosure, make the site unsuitable for sensitive interaction or financial reliance.

Infrastructure Integrity

The site resolves directly to three likely origin IP addresses, with no CDN edge identified and no confirmed CDN/WAF mediation observed. This infrastructure configuration does not independently establish malicious behavior, but it provides no protective infrastructure basis that would offset the external reputation findings.

Closing Assessment

Treat the site as unsuitable for downloads, account access, credential submission, wallet interaction, or financial activity unless independent publisher, corporate, and regulatory checks produce authoritative confirmation.

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 1207f.com.

- The request stayed on 1207f.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 2026-12-26. NOTED
- The earliest public archive of this site is from 2021-11-24. 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	YR2
SSL expiry	2026-09-27
Domain age	4.73 years (continuous registration)
Domain expiry	2026-12-26
Archive first seen	2021-11-24
Archive snapshots	15
Reputation	VirusTotal: 16 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about 1207f.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/1207f.com> · assessed 2026-08-18