

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

gxlaobao.com

Verdict

0

OUT OF 100

CRITICAL RISK

gxlaobao.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

Chinese-language landing site presenting a multi-chain cryptocurrency wallet app ('小狐钱包'), with downloads, security claims (keys stored on-device), support for many chains, FAQs, articles and contact details. The page makes strong product and usage claims but lacks independently verifiable evidence of regulatory status or audits on the page itself.

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	15 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	2.6 years old Registered history	CLEAR
Web archive	Archived since 2012 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YR2	NOTED

The page as captured

<https://gxlaobao.com/>

404 Not Found

nginx

What gxlaobao.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 2012.
- 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 landing page for the “小狐钱包” cryptocurrency wallet application. It promotes wallet downloads, multi-chain asset support, private-key and mnemonic storage on the user’s device, cold-wallet and multisignature features, and related cryptocurrency guides and articles. Its apparent business model is distribution of a digital-asset wallet and potentially associated in-app services or ecosystem referrals.

Scam/Impersonation Risk

The site presents a high-stakes digital-asset service while making expansive, unsupported claims, including being a “globally leading” and “largest” digital-currency wallet, serving nearly 20 million users, operating across more than 200 countries and regions, and processing more than 30 million daily transactions. The homepage also claims that private keys and mnemonics are generated and stored exclusively on the user’s device, but the supplied page content provides no independent audit, publisher evidence, or other substantiation for these security and scale assertions. These claim-to-evidence gaps, combined with opaque value-flow indicators, materially increase the risk associated with downloading or relying on the application. Confirmed blacklist status

and malicious detections from external threat-intelligence sources are direct contradictions; no separate brand-impersonation finding was recorded. Evidence:

- The homepage claims support for BTC, ETH, BSC, TRON, Aptos, Polygon, Solana, Cosmos, Polkadot, EOS and other networks, alongside device-held key and mnemonic claims.
- The homepage displays unsupported scale counters for 200+ countries and regions, 30M+ daily transactions and 20M+ users, and describes the wallet as globally leading and the largest digital-currency wallet.
- External reputation telemetry recorded 15 malicious detections and 1 suspicious detection among 21 evaluated results; blacklist status was reported by two external sources.
- Registration telemetry records creation on 2023-12-27T19:28:35Z and an age of 2.65 years; historical telemetry records 26 archive snapshots, captures in 2015–2026, and 15 years tracked.

Regulatory Verification Notes

The site's apparent operator identity remains unverified, and the available pages do not establish a legal entity, regulatory authority, license number, or independent audit applicable to a service handling digital assets. This is a material disclosure gap for a wallet distribution site, although the absence of a stated license is a verification issue rather than, by itself, proof of fraud. The transport layer provides encryption, but a domain-validated certificate does not validate the operator, application integrity, custody model, or regulatory standing. Evidence:

- The homepage and associated informational content provide product, security and usage claims without citing an applicable regulator, license authority, registration number or independent security audit.
- The site's hosting telemetry identifies AS54801, ZILLION-NETWORK - Zillion Network Inc., US.
- The site's TLS certificate is issued by YR2, uses DV validation, and is valid to 2026-09-27T07:40:40+00:00.

What to Verify Next

Before any installation or sensitive interaction, an independent party should confirm the real-world publisher of the application through an official app-store record or a separately obtained, cryptographically verifiable distribution channel. Any claimed regulatory status should be checked directly with the relevant jurisdictional registry, and the application package, signing identity and published integrity information should be compared with records obtained through an independent route. Contact channels should likewise be confirmed through an offline or independently sourced channel rather than relying solely on the website. Evidence:

- The homepage provides application-download calls to action but the supplied content does not provide independently verifiable publisher or package-signing information.
- The site contains one contact form, with no login form, password form or other sensitive web form identified.
- No external links were identified in the supplied link analysis, limiting direct corroboration from the site itself.

Summary Verdict

The website has a **critical trust posture** driven by confirmed external threat detections and blacklist status, compounded by unsupported high-stakes security and scale claims. Its legitimacy and operator identity are not independently established, so sensitive interaction cannot be treated as acceptable on the available evidence.

Infrastructure Integrity

No CDN or WAF was detected. The site resolves to one likely origin address hosted by ZILLION-NETWORK - Zillion Network Inc., US, on AS54801; this provides a concrete hosting path but no meaningful legitimacy assurance or protective infrastructure benefit.

Closing Assessment

Prospective users should restrict activity to passive viewing and should not download software, authenticate, disclose credentials or conduct financial transactions until the publisher, application integrity and applicable regulatory position have been independently validated.

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.
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 gslaobao.com.

- The request stayed on gslaobao.com. It was not redirected to another domain. CLEAR
- Registration is published under Gname.com Pte. Ltd.. CLEAR
- DNS for this domain is served by share-dns.com, across 2 name servers. NOTED
- The registration is paid up to 2026-12-27. NOTED
- The earliest public archive of this site is from 2012-06-10. CLEAR

- It is hosted on ZILLION-NETWORK, from a server in SC. NOTED

Domain intelligence

Registrar	Gname.com Pte. Ltd.
Hosting	ZILLION-NETWORK - Zillion Network Inc., US
Country	SC
Server IP	156.239.182.3
Name servers	A6.SHARE-DNS.COM, B6.SHARE-DNS.NET
SSL issuer	YR2
SSL expiry	2026-09-27
Domain age	2.65 years (continuous registration)
Domain expiry	2026-12-27
Archive first seen	2012-06-10
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 15 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

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