

Is scyq999.com a scam? TrustSniffer's high-risk assessment: 0/100

scyq999.com

Verdict

0

OUT OF 100

CRITICAL RISK

scyq999.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 called 小狐钱包 with download links, feature marketing, team blurbs, and many how-to articles. The site markets itself as an official wallet and references MetaMask; however, verifiable trust signals (official domains, audit links, clear legal identity) are not present in the captured content.

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	2.3 years old Registered history	CLEAR
Web archive	Archived since 2024 Public history exists	CLEAR
Certificate	Encrypted connection Issued by LiteSSL RSA CA 2025	NOTED

The page as captured

https://scyq999.com/

404 Not Found

nginx

What scyq999.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 2024.
- 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 Chinese-language website presents itself as the official download and information site for 小狐钱包, a multi-chain cryptocurrency wallet offering app installation links, blockchain and token support, decentralized-application access, NFT functions, and educational articles. Its apparent business model is to distribute the wallet application and promote related cryptocurrency usage and services.

Scam/Impersonation Risk

The site presents a **confirmed blacklist and malicious-detection concern**. External security evaluation recorded 17 malicious detections, including flags from Fortinet, Kaspersky, and Sophos, and the domain is listed in an external blacklist. This directly conflicts with the homepage's "official" wallet positioning and its high-stakes claims that the service provides a secure digital-asset environment. The site also references MetaMask without establishing an official relationship, while its claims about broad global use, transaction activity, users, supported tokens, and extensive DApp coverage are not supported by independently verifiable evidence in the captured content. The available evidence does not show a login form, hidden sensitive form, wallet-connection execution,

or wallet-drainer behavior during technical observation; those limited behavioral positives do not resolve the external threat detections or blacklist status.

EVIDENCE

- The homepage identifies 小狐钱包 as an official cryptocurrency-wallet site and provides Google Play and iOS App Store download links.
- The homepage claims support for Bitcoin, Ethereum, BNB Chain, Polygon, Solana, TRON, Avalanche, Fantom, Polkadot, Arbitrum, numerous tokens, DApps, and NFTs, but the captured content provides no audit or independently verifiable security evidence.
- External reputation telemetry records 17 malicious detections, Tier-1 flags from Fortinet, Kaspersky, and Sophos, and an external blacklist hit.
- Technical interaction testing found no login form, hidden form, external password form, wallet-provider detection, wallet-connect execution, or wallet-drainer execution.

Regulatory Verification Notes

The site's legal and accountability disclosures are insufficient for a service involving custody-adjacent cryptocurrency activity and application distribution. The captured About and team content names roles and individuals, including Rachel Bella, Celia Cooper, Terry Cooper, and Michael Moss, but does not establish a verifiable operating legal entity. No license, registration number, licensing authority, or audit link is disclosed in the captured content. Identity verification remains unverified, and the absence of clear legal status is a material transparency gap requiring resolution before any regulated or financial engagement. The domain's registrar and transport security are identifiable, but those technical facts do not establish that the wallet operator is legitimate.

EVIDENCE

- Domain registration telemetry: registered 2024-04-24 (~2.32 years old); registrar: GoDaddy.com, LLC.
- Archive telemetry: 76 archive snapshots spanning 2024–2026 (3 years tracked).
- Hosting telemetry: served from AS54801 (ZILLION-NETWORK – Zillion Network Inc., US).
- TLS telemetry: certificate issued by LiteSSL RSA CA 2025, DV validation, valid to 2026-09-27.

What to Verify Next

Any prospective engagement should first confirm that the application publisher shown in the official Google Play and iOS App Store listings is the same legal entity responsible for the website, using the stores' publisher records rather than links supplied by the site. The relevant financial or virtual-asset regulator should independently confirm whether the operator requires authorization and, if so, whether the named operator is licensed. Application integrity should be checked through official store distribution, cryptographic or vendor-confirmed release information where available, and an independent contact route; credentials, seed phrases, private keys, payment details, and wallet approvals should not be provided while these checks remain unresolved.

EVIDENCE

- The homepage distributes wallet installation links and presents itself as the official source.
- The About and team content provides role descriptions but no verifiable corporate identity or licensing reference.
- The captured site contains no sensitive forms or wallet-connection execution, so the immediate observed page behavior does not itself validate the safety of any downloaded application.

Summary Verdict

The website has a **critical trust posture** and presents material sensitive-interaction risk. Its apparent wallet purpose, unsupported security and scale claims, and confirmed external threat and blacklist signals are not consistent with a site suitable for credentials, software installation, or financial activity. The operator's real-world identity is not independently verified.

Infrastructure Integrity

The site resolves to a single likely origin address rather than a detected CDN edge, with hosting provided by ZILLION-NETWORK – Zillion Network Inc. in the United States on AS54801. No CDN was detected; the available hosting arrangement therefore provides limited infrastructure-based mitigation. The site does use DV TLS issued by LiteSSL RSA CA 2025, which protects transport encryption but does not authenticate the operator or validate the application.

Closing Assessment

Until independent publisher, operator, and regulatory checks produce consistent results, activity should remain limited to passive viewing; downloads, credential submission, wallet authorization, and financial transfers should not be attempted.

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 scyq999.com.

- The request stayed on scyq999.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 2027-04-24. NOTED
- The earliest public archive of this site is from 2024-05-03. 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	154.39.192.198
Name servers	NS33.DOMAINCONTROL.COM, NS34.DOMAINCONTROL.COM
SSL issuer	LiteSSL RSA CA 2025
SSL expiry	2026-09-27
Domain age	2.32 years (continuous registration)
Domain expiry	2027-04-24
Archive first seen	2024-05-03

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 scyq999.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/scyq999.com> · assessed 2026-08-21