

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

gjbfyb.com

Verdict

0

OUT OF 100

CRITICAL RISK

gjbfyb.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 itself as the official TP wallet download page. Claims to support many blockchains and large user numbers, includes blog/FAQ content and contact details (Guangzhou address, phone, an email). Presentation has duplicated blocks and low editorial quality; authenticity of claims and official status is unverified and potentially impersonative.

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	4.6 years old Registered history	CLEAR
Web archive	Archived since 2021 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YR1	NOTED

The page as captured

<https://gjbfb.com/>

404 Not Found

nginx

What gjbfb.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: 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 Chinese-language website is a landing page presenting itself as the official TP wallet download portal. It promotes a downloadable multi-chain cryptocurrency wallet, blockchain-related features, FAQ and blog content, and broad user-adoption claims, with an apparent business model centered on application downloads and related digital-asset services.

Scam/Impersonation Risk

The site presents itself as an official wallet-download destination, but its authenticity and connection to the claimed brand remain unverified. The principal risk contradiction is external threat intelligence: the domain is confirmed as blacklisted and received malicious classifications from multiple security providers, including Fortinet, Kaspersky, and Sophos. The page also contains duplicated content, weak editorial quality, unsupported claims of being a leading or largest digital-asset wallet, and repeated counters claiming service to more than 200 countries, 30M+ daily transactions, and 20M users. These inconsistencies materially weaken the credibility of

the site's official-status claims, although the supplied evidence does not establish a confirmed brand impersonation or identity inconsistency.

EVIDENCE

- The homepage title and landing-page content describe the site as an “official” TP wallet download service and claim support for BTC, ETH, BSC, TRON, Aptos, Polygon, Solana, OKExChain, Polkadot, Kusama, EOS, IOST, and other networks.
- External security telemetry records 17 malicious detections, with Fortinet, Kaspersky, and Sophos among the flagged providers; the domain is also recorded as blacklisted.
- The homepage repeats country, transaction, and user counters and contains duplicated blocks, while the displayed team and editorial material provide no independent substantiation for the scale claims.
- Domain registration telemetry records creation on 2024-04-11, with an age of approximately 2.36 years.

Regulatory Verification Notes

The available site content does not establish a verifiable operating legal entity, licensing basis, or registration number for a digital-asset service. The contact material supplies a Guangzhou address and telephone details, and the homepage names individual team members, but these disclosures do not independently validate the operator or authorize the advertised financial-technology activity. The regulatory position should therefore be treated as unresolved rather than as evidence of a licensed service. Transport encryption is present, but a domain-validation certificate authenticates control of the domain connection, not the legitimacy of the operator.

EVIDENCE

- The homepage and contact material provide a Guangzhou address, telephone details, and named personnel, but no independently verifiable corporate or licensing disclosure is supplied.
- The site's business presentation is centered on a downloadable cryptocurrency wallet and digital-asset management, with no license authority or license number stated.
- Hosting is provided by ZILLION-NETWORK — Zillion Network Inc. through AS54801.
- The site's TLS certificate is issued by YR1, uses DV validation, and is valid until 2026-09-26.

What to Verify Next

Before any sensitive interaction, an organization should obtain the wallet application only through a separately verified official distribution channel and confirm that the domain is published by the genuine wallet operator. Any claimed company, address, and regulatory status should be checked against the relevant corporate and financial-services registries using independently sourced records. Contact channels should be validated through an offline or independently established route rather than relying solely on information presented by the site.

EVIDENCE

- The homepage is categorized as a wallet-download and informational landing page rather than a clearly documented regulated service.
- The site provides one contact form and contact details, but no external links or structured corporate identity evidence were observed.
- The site's legal status, product provenance, and relationship to the claimed wallet brand remain unverified.

Summary Verdict

The website has a **critical trust posture** and presents unacceptable risk for sensitive interaction. The available evidence supports treating its official-status and operational claims as unsubstantiated, with the confirmed external threat reputation outweighing the site's basic technical availability and content presentation.

Infrastructure Integrity

The site resolves directly to a single likely origin IP, with no detected CDN or WAF edge layer. Its hosting is attributed to ZILLION-NETWORK — Zillion Network Inc. through AS54801; this infrastructure provides no protective edge-layer mitigation sufficient to offset the external reputation findings.

Closing Assessment

Prospective users and institutions should restrict activity to non-interactive observation and should not download software, submit credentials, connect wallets, or make financial transfers through the site.

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

- 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 gjbfyb.com.

- The request stayed on gjbfyb.com. It was not redirected to another domain. CLEAR
- Registration is published under West263 International Limited. CLEAR
- DNS for this domain is served by myhostadmin.net, across 6 name servers. NOTED
- The registration is paid up to 2028-04-11. CLEAR
- The earliest public archive of this site is from 2021-12-01. CLEAR
- It is hosted on ZILLION-NETWORK, from a server in SC. NOTED

Domain intelligence

Registrar	West263 International Limited
Hosting	ZILLION-NETWORK - Zillion Network Inc., US
Country	SC
Server IP	156.239.182.2
Name servers	NS1.MYHOSTADMIN.NET, NS2.MYHOSTADMIN.NET, NS3.MYHOSTADMIN.NET, NS4.MYHOSTADMIN.NET, NS5.MYHOSTADMIN.NET, NS6.MYHOSTADMIN.NET
SSL issuer	YR1
SSL expiry	2026-09-26
Domain age	4.59 years (continuous registration)
Domain expiry	2028-04-11
Archive first seen	2021-12-01
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 gjbfyb.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/gjbfyb.com> · assessed 2026-08-21