

Is 126qiyeyou.com a scam? TrustSniffer's high-risk assessment: 0/100

126qiyeyou.com

Verdict

0

OUT OF 100

CRITICAL RISK

126qiyeyou.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

GPT summary status=skipped | No usable content for GPT summary (clean/dom/html all empty)

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	13 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	9.5 years old Registered history	CLEAR
Web archive	Archived since 2023 4 snapshots	CLEAR
Certificate	Encrypted connection Issued by YR1	NOTED

The page as captured

chrome-error://chromewebdata/

What 126qiyeou.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 2023.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

Fortinet, Sophos flagged this site in external intelligence checks, indicating elevated compromise/scam exposure that requires immediate caution.

The website is an internet-facing domain at 126qiyeou.com, but the supplied site material does not establish a clear product, service, corporate operator, or business model; its intended purpose therefore cannot be reliably characterized.

Scam/Impersonation Risk

The site presents a **critical sensitive-interaction risk**. External security assessments identified malicious activity associated with the domain, including 13 malicious detections, and the domain is blacklisted by the cited sources, including Fortinet and Sophos. This is a confirmed reputational threat signal rather than a minor anomaly. Runtime behavior also showed suspicious inline scripting and substantial non-whitelisted external traffic, including outbound requests and posts, which increases concern around interacting with the site. No separate evidence of brand impersonation or conflicting legal identities was supplied, but the confirmed blacklist status is sufficient to make login, credential submission, and financial activity inappropriate.

EVIDENCE

- External reputation assessment recorded 13 malicious detections; Fortinet and Sophos were among the flagged vendors.
- The domain was identified as blacklisted by two cited external sources.
- Homepage runtime behavior recorded 9 external XHR requests and 8 external posts, all classified as non-whitelisted; one suspicious inline script was also observed.
- Domain registration records show registration on 2017-02-28, making the domain approximately 9.47 years old.

Regulatory Verification Notes

The real-world operator identity remains unverified, and the supplied legal and identity material does not establish licensing, authorization, or a verifiable corporate entity. This is a regulatory verification gap, not by itself proof of fraud; however, it must be considered alongside the confirmed external threat findings. The domain uses privacy-protected registration through Xin Net Technology Corporation. A broker-reputation cross-check returned no match, but that result is contextual only and is not a legal or licensing determination.

EVIDENCE

- Web-archive coverage comprises 4 snapshots spanning 2023–2025, across 3 tracked years; this records limited archival coverage rather than the domain's full registration age.
- The domain's registrar is Xin Net Technology Corporation; registrant and organization fields are privacy-protected.
- The site is hosted on AS4811, identified as CHINANET-SHANGHAI-MAN – China Telecom (Group), CN.
- TLS is provided at DV validation level by issuer YR1 and is valid to 2026-09-30T19:01:47+00:00.

What to Verify Next

Before any sensitive interaction, an independent check should confirm whether the operator has the authorization required for the services implied by the site, using the relevant regulator's official registry rather than links or contact details supplied by the domain. The operating entity should also be matched against authoritative corporate records, and contact channels should be confirmed through an independently sourced route. Until those checks are completed, no credentials, financial information, or funds should be submitted.

EVIDENCE

- Licensing and authorization are not established by the supplied legal or identity material.
- The operator's real-world identity is not independently verified.
- Independent confirmation of the official support and contact channels is therefore required before sensitive engagement.

Summary Verdict

The overall posture is **high risk and unsuitable for sensitive interaction**. The convergence of confirmed external malicious detections, blacklisting, and suspicious runtime network behavior outweighs the site's

otherwise functioning transport encryption and established registration age. Apparent legitimacy and operator identity cannot be treated as proven.

Infrastructure Integrity

The domain resolves directly to a single likely origin address, 114.67.107.194, on AS4811 operated by CHINANET-SHANGHAI-MAN – China Telecom (Group), CN. No CDN or WAF vendor was detected, so the hosting arrangement provides no identified edge-layer mitigation; infrastructure identification should be treated as a technical observation, not evidence of legitimacy.

Closing Assessment

Activity should remain limited to non-interactive observation until independent operator, authorization, and contact-channel checks have been completed; login, credential use, and financial transactions should not proceed.

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, behaviour in a sandbox, 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

- The page sent data to a destination TrustSniffer does not recognise.

Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_POSTS

- The page exchanged network traffic with destinations TrustSniffer does not recognise.

Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_TRAFFIC

- A large share of what the page loaded came from other domains.

Behaviour in a sandbox rule:BEHAV_EXTERNAL_RATIO_MODERATE

- The page carried inline scripts written in a style TrustSniffer treats as suspicious.

Behaviour in a sandbox rule:BEHAV_SUSPICIOUS_INLINE_SCRIPTS

- The page made background requests to destinations TrustSniffer does not recognise.

Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_XHR

- 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	UNKNOWN
Identity score	50/100
Identity verification confidence	15%

- AI page analysis unavailable (page captured; identity not AI-verified)

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 126qiye.com.

- The request for 126qiye.com ended on chromewebdata, a different domain. WATCH
- Registration is published under Xin Net Technology Corporation. CLEAR
- DNS for this domain is served by xincache.com, across 2 name servers. NOTED
- The registration is paid up to 2027-02-28. NOTED
- The earliest public archive of this site is from 2023-02-18. CLEAR
- It is hosted on CHINANET-SHANGHAI-MAN, from a server in CN. NOTED

Domain intelligence

Registrar	Xin Net Technology Corporation
Hosting	CHINANET-SHANGHAI-MAN - China Telecom (Group), CN
Country	CN
Server IP	114.67.107.194
Name servers	NS13.XINCACHE.COM, NS14.XINCACHE.COM
SSL issuer	YR1
SSL expiry	2026-09-30
Domain age	9.47 years (continuous registration)
Domain expiry	2027-02-28
Archive first seen	2023-02-18
Archive snapshots	4
Reputation	VirusTotal: 13 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about 126qiye.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/126qiyeyou.com> · assessed 2026-08-18