

Is 0572tv.net a scam? TrustSniffer's high-risk assessment: 0/100

0572tv.net

Verdict

0

OUT OF 100

CRITICAL RISK

0572tv.net 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 news/article page covering a maritime archaeology exhibition, commentary on China–US relations, and tennis match reports. Page indicates JavaScript is required to function.

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.

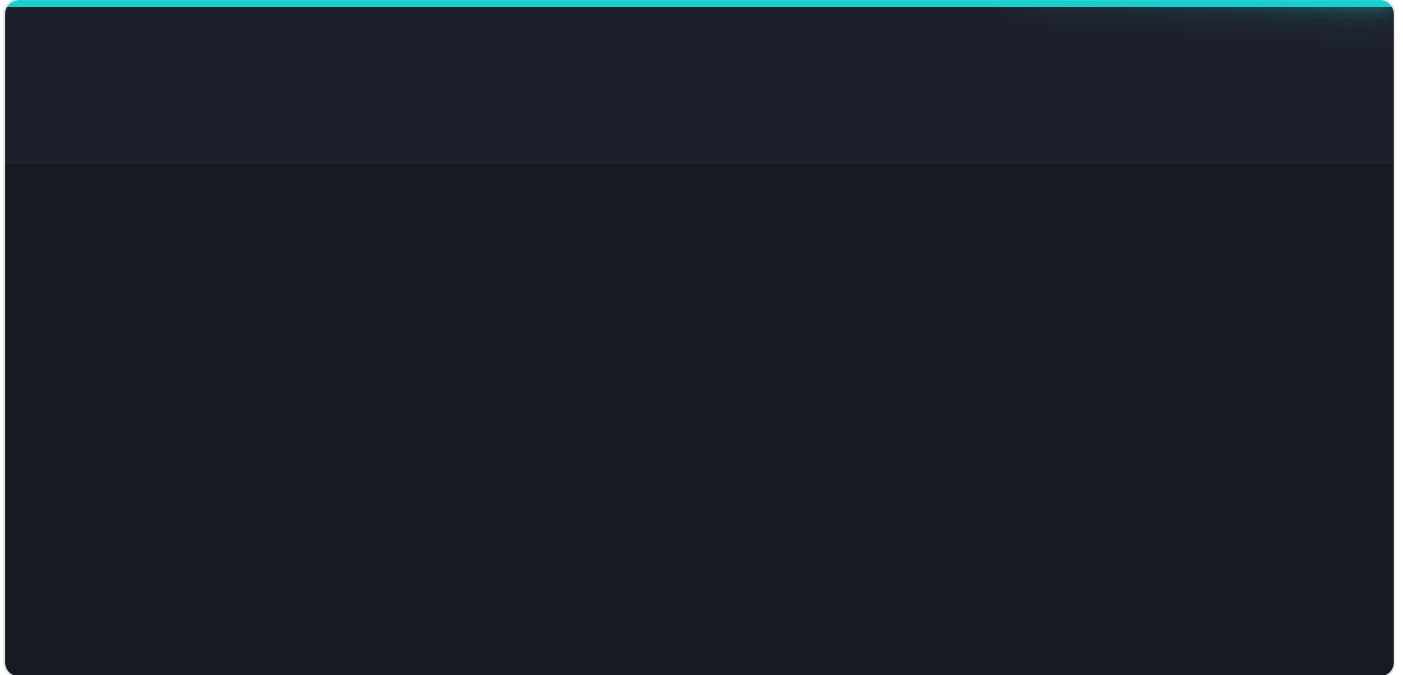
At a glance

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	9 months old Most scam domains are under a year old	WATCH
Web archive	Archived since 2010 97 snapshots	CLEAR
Certificate	Encrypted connection Issued by YE2	NOTED

The page as captured

<https://www.j9t22.com/marketproxypage/888>



What 0572tv.net served when TrustSniffer captured it on 2026-08-18. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: less than 1 year (registration continuity).
- Public web-archive history exists since 2010.
- 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 presents Chinese-language news and article content, including reporting on a maritime archaeology exhibition, China–United States relations, and tennis matches. Its apparent business model is informational publishing, likely supported by advertising or content distribution rather than direct financial services, although the page requires JavaScript to render fully.

Scam/Impersonation Risk

No on-page phishing form, credential collection, brand impersonation, or identity contradiction was observed, and the visible content is consistent with a news/article site. However, this benign presentation is materially outweighed by confirmed external security contradictions: the domain is blacklisted, multiple security services classify it as malicious, and Fortinet and Sophos are among the vendors reporting a threat. Runtime behavior also showed suspicious external network activity and repeated console errors, which further reduces confidence that the visible article content represents the complete risk surface. The site should therefore be treated as unsuitable for sensitive interaction despite the absence of visible login or payment features.

EVIDENCE

- External reputation assessment recorded 17 malicious detections and 1 suspicious detection among 23 evaluated results; Fortinet and Sophos were flagged.
- The domain was marked blacklisted by both VT and an external blacklist source; Google Safe Browsing was recorded as non-malicious.
- The article page contained no forms, no sensitive form fields, and no detected login or phishing indicators.
- Archive records show 97 snapshots spanning 2010–2024, covering 15 tracked years; current registration telemetry records creation on 2025-11-26 and an age of approximately 0.72 years.

Regulatory Verification Notes

The analyzed page presents no financial-service offer and makes no licensing claim. It also does not establish a clearly identifiable real-world operator, so identity remains unverified and the available disclosure position is insufficient for institutional reliance. The absence of a broker-data match is only contextual and does not constitute licensing or regulatory confirmation. The valid transport certificate and identifiable hosting arrangement support technical reachability, not legal legitimacy.

EVIDENCE

- The analyzed homepage/article content is categorized as informational news and records no claimed licence, licence authority, or licence number.
- The site is hosted on AS137951, ASLINE-AS-AP – ASLINE LIMITED, HK.
- The TLS certificate is issued by YE2, uses DV validation, and is valid to 2026-11-10.
- The site's page metadata identifies the title as "j9.live" while the assessed domain is 0572tv.net, a naming inconsistency requiring independent domain and operator confirmation.

What to Verify Next

Before any interaction beyond passive viewing, an institution should confirm through an independently obtained channel that the assessed domain is an authorised publication domain and that the displayed content has a legitimate operator. Any claimed organisation, editorial affiliation, or commercial relationship should be checked against authoritative records rather than relying on the website itself. Security teams should also inspect the domain and its associated infrastructure in a controlled environment before allowing it into enterprise browsing or communication workflows.

EVIDENCE

- The page requires JavaScript and generated 23 external XHR requests, including 14 non-whitelisted requests, during observed execution.
- The same execution generated 10 external POST requests, all classified as non-whitelisted.
- Twelve console errors were recorded across two successful behavioral runs.
- No wallet connection, clipboard hijacking, hidden form, or password-external-form activity was detected during those runs.

Summary Verdict

The overall posture is **critical trust risk**. The site’s apparent news function does not offset the confirmed reputation contradictions, and the real-world operator identity cannot be independently established from the available evidence. It should not be treated as a trusted website for sensitive interaction.

Infrastructure Integrity

The site resolves directly to a single likely origin rather than a detected CDN edge, with no trusted CDN identified. This provides limited infrastructure-layer mitigation and leaves the service dependent on its direct hosting environment; infrastructure characteristics do not counter the reputation findings.

Closing Assessment

Restrict use to passive, read-only viewing, and prohibit credential submission, account access, downloads, or financial activity unless the domain and operator are independently validated through a trusted offline or previously established channel.

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
 - The public registration record for this domain is incomplete.

Registration and ownership rule:KF_WHOIS_INCOMPLETE
- 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 made background requests to destinations TrustSniffer does not recognise.

Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_XHR
 - A large share of what the page loaded came from other domains.

Behaviour in a sandbox rule:BEHAV_EXTERNAL_RATIO_MODERATE
 - The page exchanged network traffic with destinations TrustSniffer does not recognise.

Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_TRAFFIC
 - The page sent data to a destination TrustSniffer does not recognise.

Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_POSTS
 - 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	50%

- 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 0572tv.net.

- The request for 0572tv.net ended on www.j9t22.com, a different domain. WATCH
- Registration is published under Gname 252 Inc. CLEAR
- DNS for this domain is served by dns.com, across 2 name servers. NOTED
- The registration is paid up to 2026-11-26. NOTED
- The earliest public archive of this site is from 2010-12-28. CLEAR
- It is hosted on ASLINE-AS-AP, from a server in ZA. NOTED

Domain intelligence

Registrar	Gname 252 Inc
Hosting	ASLINE-AS-AP - ASLINE LIMITED, HK
Country	ZA
Server IP	168.76.141.60
Name servers	NS1.DNS.COM, NS2.DNS.COM
SSL issuer	YE2
SSL expiry	2026-11-10
Domain age	0.72 years (continuous registration)
Domain expiry	2026-11-26
Archive first seen	2010-12-28
Archive snapshots	97
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 0572tv.net 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/0572tv.net> · assessed 2026-08-18