

Is 3115ff.me a scam? TrustSniffer's high-risk assessment: 0/100

3115ff.me

Verdict

0

OUT OF 100

CRITICAL RISK

3115ff.me 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

Short Chinese-language content with poetry and a brand slogan. No forms, links, or calls-to-action indicating financial services or credential requests.

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	2.2 years old Registered history	CLEAR
Web archive	Archived since 2024 2 snapshots	CLEAR
Certificate	Encrypted connection Issued by WE1	NOTED

The page as captured

https://3115ff.me/86HJM9.html



What 3115ff.me served when TrustSniffer captured it on 2026-08-18. 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

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

3115ff.me presents a short Chinese-language informational page combining a brand slogan with classical poetry. Its apparent purpose is static branding or content publication; the captured page shows no evident financial service, account workflow, payment mechanism, or credential-collection function.

Scam/Impersonation Risk

The site carries a **confirmed external reputation contradiction**: multiple security assessments classified the domain as malicious, and blacklist status was confirmed by more than one source. This materially outweighs the benign appearance of the homepage. The captured page itself contains no login form, sensitive form, explicit phishing request, or detected brand impersonation, but the absence of those features does not reconcile the external malicious detections. The domain’s current operator identity is also not independently verified. No suspicious contact-email anomaly was identified.

EVIDENCE

- External reputation assessment: 15 malicious detections, including a tier-one security-provider detection; blacklist status confirmed by two sources.
- Registration record: registered 2026 (~0.52 years old).
- Web archive: 2 snapshots from 2024-06-01 through 2024-08-19, spanning 1 year tracked; no repurposing was detected, but this historical record does not independently establish the current operator's identity.
- Homepage: 76 characters of Chinese poetry and branding content, with 0 forms and no login or sensitive-form indicators.

Regulatory Verification Notes

The available page does not claim a license or provide a license number, and it does not establish a regulated business identity. This is a regulatory disclosure gap rather than, by itself, proof of fraud; however, in combination with the confirmed external reputation contradiction, the site should not be treated as suitable for regulated or sensitive interactions. The valid transport certificate and identifiable hosting arrangement are technical controls only and do not establish licensing, ownership, or regulatory authorization. No matching broker reputation record was identified in the available third-party context.

EVIDENCE

- Hosting: served from AS13335 (CLOUDFLARENET - Cloudflare, Inc., US).
- TLS certificate: issued by WE1, domain-validated (DV), valid to 2026-11-04.
- Domain registrar: Spaceship, Inc.; expiration recorded as 2027-02-10.
- Homepage: no license claim, license number, or regulated-entity disclosure was identified.

What to Verify Next

Before any sensitive interaction, an independent party should establish the operator's legal identity and confirm any claimed authorization directly with the relevant regulatory registry. Official contact channels should be confirmed through an independently sourced route rather than relying solely on information presented by the site. Until those checks produce a consistent result, access should remain observational and isolated from corporate credentials, payment instruments, and sensitive systems.

EVIDENCE

- Observed behavior: 2 external XHR requests and 2 external POST requests were non-whitelisted during 2 successful runs.
- Observed behavior: 2 console errors were recorded, while no wallet connection, wallet-sensitive action, clipboard write, or hidden form was detected.

Summary Verdict

The overall posture is **critical trust risk**, driven by confirmed external malicious-reputation contradictions and insufficient independent identity assurance. The site's minimal informational presentation does not provide a credible basis for treating sensitive interaction as acceptable.

Infrastructure Integrity

Cloudflare CDN/WAF protection provides a mitigating layer against direct exposure of the hosting environment, but it is not evidence of legitimacy. All observed addresses were CDN edge servers, and no origin candidate was identified, limiting independent assessment of the underlying host.

EVIDENCE

- CDN/WAF: Cloudflare protection identified; 4 edge addresses observed and 0 likely origin addresses identified.
- Network resolution: all observed edge infrastructure mapped to the Cloudflare network in the United States.

Closing Assessment

Sensitive use should be suspended unless independent identity, authorization, and security checks resolve the identified concerns; login, credential submission, and financial transactions should not proceed in the interim.

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
- 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
- A large share of what the page loaded came from other domains.
Behaviour in a sandbox rule:BEHAV_EXTERNAL_RATIO_MODERATE
- 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 confidence25%

- 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 3115ff.me.

- The request stayed on 3115ff.me. It was not redirected to another domain. CLEAR
- Registration is published under Spaceship, Inc.. CLEAR
- The registration is paid up to 2027-02-10. NOTED
- The earliest public archive of this site is from 2024-06-01. CLEAR
- It is hosted on CLOUDFLARENET, from a server in US. NOTED

Domain intelligence

Registrar	Spaceship, Inc.
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US
Server IP	2606:4700:3035::ac43:9b87
Name servers	Not available
SSL issuer	WE1
SSL expiry	2026-11-04
Domain age	2.21 years (continuous registration)
Domain expiry	2027-02-10
Archive first seen	2024-06-01
Archive snapshots	2
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 3115ff.me 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.

