

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

0zhe.com

Verdict

0

OUT OF 100

CRITICAL RISK

Ozhe.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 75%.

What this site appears to be

A Chinese-language overseas community forum (海角社区) focused on user-generated posts. The visible content contains explicit sexual material, including incest and rape-themed titles. The site shows navigation (login/register), rankings, and alternate domain/contact hints for access, but ownership and moderation details are not provided.

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	18 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	3 months old Most scam domains are under a year old	RISK
Web archive	Archived since 2007 506 snapshots	CLEAR
Certificate	Encrypted connection Issued by YE2	NOTED

The page as captured

https://0zhe.com/



What 0zhe.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: less than 1 year (registration continuity).
- Public web-archive history exists since 2007.
- 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.

The website is a Chinese-language user-generated-content forum presenting adult and sexually explicit posts, rankings, login and registration functions, and instructions for reaching alternate domains. Its apparent model is community traffic monetized through advertising, donations, or premium participation rather than a clearly presented conventional purchasing service.

Scam/Impersonation Risk

The site carries a **critical interaction risk** because external security intelligence records confirmed malicious detections and blacklist status across two sources. The page itself contains explicit incest- and rape-themed material, prominent user rankings, and prompts to retain multiple alternate access domains; these features do not independently prove fraud, but they increase the operational and legal-risk context surrounding the service. No distinct legal-entity conflict or confirmed brand impersonation is recorded, so the principal concern is the confirmed external threat reputation rather than a demonstrated identity contradiction. The absence of a login

form in the captured page reduces the observed credential-capture evidence, but does not offset the external detections.

EVIDENCE

- The homepage is titled “海角社区” and displays explicit user-generated posts, sexualized rankings, login/register navigation, and alternate-domain access instructions.
- External reputation assessment recorded 18 malicious detections, including detections from Fortinet, Kaspersky, and Sophos; blacklist status was confirmed by VT and an external blacklist source.
- Archive history records the domain as first seen on 2007-04-23, with an assessed domain age of 19.318275154004105 years.
- The archive contains 506 snapshots spanning 2007–2025, covering 19 tracked years.

Regulatory Verification Notes

The visible forum material does not identify an operating company, provide moderation governance details, or make a licensing claim. Because the observed business model is a user-generated-content forum with no clear commercial purchase flow, the principal regulatory issues are content governance, age controls, lawful-content handling, and operator accountability rather than a demonstrated regulated financial service. No broker match was returned in the available third-party reputational context; that result is contextual only and does not establish licensing or compliance. The site's identity remains unverified independently.

EVIDENCE

- The homepage presents community functions and adult content but no visible corporate operator, moderation policy, license authority, or license number.
- The site's transport encryption uses a DV certificate issued by YE2, valid to 2026-10-23.
- Hosting is provided through AS13335, CLOUDFLARENET — Cloudflare, Inc., US.
- The page-authority signal is in the mid band, which provides limited explanatory context but does not establish legitimacy or regulatory standing.

What to Verify Next

Before any interaction beyond passive viewing, an institution should independently establish the operator's legal identity and confirm that the service has enforceable age-verification, content-moderation, privacy, and complaint procedures. Any proposed use involving registration, credentials, payments, or other sensitive information should be withheld unless the operator and applicable legal obligations are validated through authoritative, offline or independently sourced channels. Security teams should also confirm that endpoint controls continue to block the domain and preserve relevant logs for any attempted access.

EVIDENCE

- The homepage supplies alternate-domain access instructions rather than a clearly documented operator-verification path.
- The visible site provides login and registration navigation, while the captured interaction showed no password form or external password submission.
- The business-model assessment identifies user-generated content potentially supported by advertising, traffic, donations, or premium memberships, with no clear purchase flow.

Summary Verdict

The overall posture is **critical and unsuitable for sensitive interaction**. The available evidence does not independently verify the real-world operator, and confirmed external threat and blacklist signals outweigh the site's stable technical presentation and historical web presence. Passive observation may be distinguished from trust in the service, but the website should not be treated as an approved or reliable destination for sensitive activity.

Infrastructure Integrity

The site is served behind Cloudflare's CDN/WAF, with observed addresses limited to Cloudflare edge infrastructure and no origin candidate identified. This provides a meaningful layer of exposure mitigation, but it is only a protective hosting characteristic and cannot validate the operator or neutralize the external threat findings.

EVIDENCE

- Observed edge addresses: 104.21.29.147, 172.67.149.101, 2606:4700:3030::ac43:9565, and 2606:4700:3035::6815:1d93; all resolve through AS13335.
- The hosting provider is CLOUDFLARENET — Cloudflare, Inc., US, with Cloudflare CDN/WAF protection.
- No likely origin IP candidate was identified in the observed infrastructure.

Closing Assessment

The proportionate institutional action is to maintain a read-only posture and prevent login, credential submission, payment, or other sensitive engagement unless independent operator and security validation materially changes the assessment.

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, 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 Ozhe.com.

- The request stayed on Ozhe.com. It was not redirected to another domain. [CLEAR](#)
- Registration is published under NAMECHEAP INC. [CLEAR](#)
- DNS for this domain is served by cloudflare.com, across 2 name servers. [NOTED](#)
- The registration is paid up to 2027-05-26. [NOTED](#)
- The earliest public archive of this site is from 2007-04-23. [CLEAR](#)
- It is hosted on CLOUDFLARENET, from a server in US. [NOTED](#)

Domain intelligence

Registrar	NAMECHEAP INC
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US
Server IP	2606:4700:3035::6815:1d93

Name servers	DION.NS.CLOUDFLARE.COM, NOLA.NS.CLOUDFLARE.COM
SSL issuer	YE2
SSL expiry	2026-10-23
Domain age	0.23 years (continuous registration)
Domain expiry	2027-05-26
Archive first seen	2007-04-23
Archive snapshots	506
Reputation	VirusTotal: 18 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about 0zhe.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/0zhe.com> · assessed 2026-08-18