

Is 228199.com a scam? TrustSniffer's high-risk assessment: 0/100

228199.com

Verdict

0

OUT OF 100

CRITICAL RISK

228199.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

Short Chinese landing page urging the user to click a button to open a link. Mentions a security check and provides multiple CTAs to click; no service description, contact info, or verifiable claims.

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.

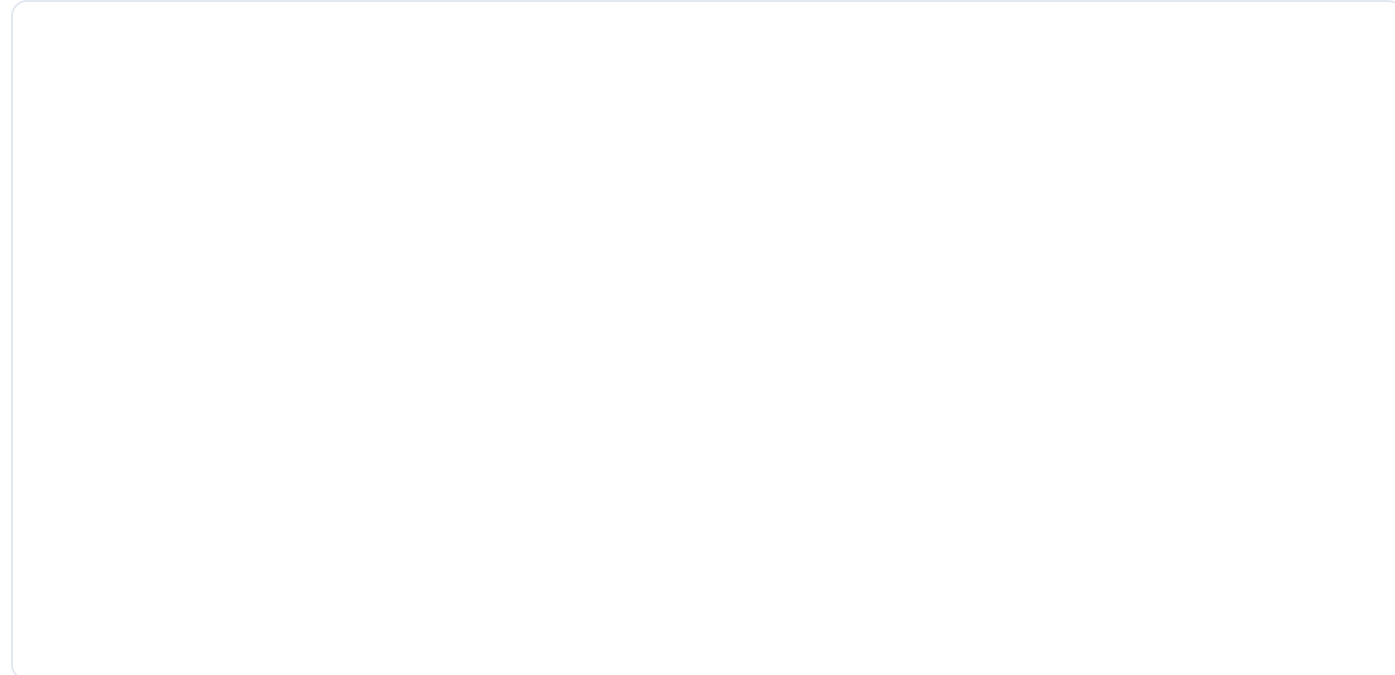
At a glance

The checks that decide most of this verdict.

Malware engines	16 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	6 months old Most scam domains are under a year old	RISK
Web archive	Archived since 2021 9 snapshots	CLEAR
Certificate	Encrypted connection Issued by YE2	NOTED

The page as captured

<https://228199.com/>



What 228199.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 2021.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

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

The website is a minimal Chinese-language click-through landing page at 228199.com that presents a purported security check and repeatedly instructs visitors to click a button to open another link; it does not describe a recognizable product, service, or transparent commercial purpose.

Scam/Impersonation Risk

The site presents a **critical sensitive-interaction risk**. It is blacklisted by multiple external sources, with malicious detections from major security providers including Kaspersky and Sophos. The landing page's "security check" wording, repeated click prompts, and potential redirect behavior create an opaque value flow without explaining the destination or purpose. This is consistent with a click-through or redirect-monetization model rather than a verifiable service, and the available evidence does not establish a legitimate operator identity. The historical archive record also shows captures from 2021–2024 while the current registration record dates from 2026; that provenance discrepancy further limits confidence in continuity, although it is distinct from the confirmed external threat findings.

EVIDENCE

- The homepage contains the Chinese prompts “已通过安全检测” and “点击一下，立即打开,” translated as “security check passed” and “click once to open,” with no substantive service explanation.
- External reputation checks recorded 16 malicious and 1 suspicious detections out of 22 evaluated results; Kaspersky and Sophos were among the flagged vendors, and blacklist status was confirmed by 2 sources.
- Archive records show 9 snapshots from 2021-11-23 through 2024-11-23, covering 4 tracked years.
- The current domain registration record shows creation on 2026-02-20 and an age of 0.49 years.

Regulatory Verification Notes

The available landing page provides no company identity, licensing statement, registration number, terms, privacy disclosure, or contact information. This is a material transparency gap for any site that might seek payment, personal information, or regulated activity, and the operator’s real-world identity remains unverified. No matching broker record was identified in the supplied third-party context; that absence is not a licensing determination. The current certificate and registrar are technical or administrative facts only and do not validate the operator or business model.

EVIDENCE

- The homepage contains no identifiable legal entity, license reference, registration number, or contact channel.
- The domain registrar is GMO Internet Group, Inc. d/b/a Onamae.com.
- The site uses a DV TLS certificate issued by YE2, valid through 2026-09-05.
- Hosting telemetry identifies AS138995, ANTBOX1-AS-AP – Antbox Networks Limited, HK.

What to Verify Next

Any prospective engagement should first identify the final destination behind each button without opening it in a normal authenticated session, and independently confirm that destination through a trusted security process. If the operator claims to provide a regulated service, its legal entity and authorization should be checked directly against the relevant regulator’s register. Contact and ownership details should be confirmed through an independent offline or previously trusted channel before any sensitive interaction. Given the confirmed external threat findings, login, credential submission, payment activity, and financial transactions should not be conducted through this site.

EVIDENCE

- The homepage has no login form or sensitive-data form, but it contains multiple click-through calls to action.
- Browser observation recorded clickbait-CTA and potential-redirect behavior.
- Network observation recorded 7 external XHR requests, including 4 to non-whitelisted destinations.
- The site provides no stated service, transaction terms, or accountable support channel against which a destination could be assessed.

Summary Verdict

The overall posture is critical and unsuitable for sensitive interaction. The evidence converges on a deceptive or unsafe click-through environment with materially weak identity assurance and confirmed external threat indicators; legitimacy is not established.

Infrastructure Integrity

The site is not behind a detected CDN or WAF and resolves through seven likely origin IPs with no identified edge IPs. Hosting is attributed to ANTBOX1-AS-AP – Antbox Networks Limited, HK, and DNS telemetry includes a fast-flux-like heuristic; that heuristic is not conclusive on its own, but the infrastructure provides no meaningful protective mitigation against the stronger page and reputation findings.

EVIDENCE

- Infrastructure resolution identified 7 unique IP addresses, 0 edge IPs, and 7 likely origin candidates.
- The site has no detected CDN, no detected WAF vendor, and no trusted-CDN mitigation.
- DNS telemetry recorded the heuristic flag “fast_flux_like.”
- The resolved infrastructure is registered through AFRINIC in country code SC.

Closing Assessment

The appropriate enterprise disposition is to block or quarantine the domain and investigate any systems or users that followed its prompts; no sensitive interaction should proceed unless an independently verified, legitimate destination is established through separate trusted channels.

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
- Most of what the page loaded came from other domains rather than from this one.
Behaviour in a sandbox rule:BEHAV_EXTERNAL_RATIO_HIGH
- 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 228199.com.

- The request stayed on 228199.com. It was not redirected to another domain. CLEAR
- Registration is published under GMO Internet Group, Inc. d/b/a Onamae.com. CLEAR
- DNS for this domain is served by share-dns.com, across 2 name servers. NOTED
- The registration is paid up to 2027-02-20. NOTED
- The earliest public archive of this site is from 2021-11-23. CLEAR
- It is hosted on ANTBOX1-AS-AP, from a server in SC. NOTED

Domain intelligence

Registrar	GMO Internet Group, Inc. d/b/a Onamae.com
Hosting	ANTBOX1-AS-AP - Antbox Networks Limited, HK
Country	SC
Server IP	45.194.37.69
Name servers	A8.SHARE-DNS.COM, B8.SHARE-DNS.NET
SSL issuer	YE2
SSL expiry	2026-09-05
Domain age	0.49 years (continuous registration)
Domain expiry	2027-02-20
Archive first seen	2021-11-23
Archive snapshots	9
Reputation	VirusTotal: 16 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about 228199.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/228199.com> · assessed 2026-08-18