Is 272586.com a scam? TrustSniffer's high-risk assessment: 0/100

272586.com

Verdict

0
OUT OF 100

CRITICAL RISK

272586.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

Assessed 2026-08-18 by automated analysis. Classification confidence 70%.

What this site appears to be	The page HTML is blank (no head metadata, no body content). No forms, links, or resources detected.

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	**11 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	**2.9 years old** Registered history	CLEAR
Web archive	**Archived since 2023** 16 snapshots	CLEAR
Certificate	**Encrypted connection** Issued by YR1	NOTED

The page as captured

No screenshot is retained for this report.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: 1 to 3 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.

272586.com is an effectively blank web property: the homepage presents no visible text, branding, service description, navigation, forms, or monetization cues, so its intended purpose and business model cannot be determined from the visitor-facing content.

Scam/Impersonation Risk

The site presents a **critical sensitive-interaction risk**. Confirmed blacklist status and multiple malicious detections create a direct contradiction to treating the domain as trustworthy, even though the captured page itself does not display an impersonated brand, login form, or other active phishing interface. The absence of visible content prevents meaningful validation of the operator or any service represented by the domain; it does not reduce the significance of the external threat findings.

EVIDENCE

- External security assessments recorded the domain as blacklisted, with 11 malicious and 2 suspicious detections; Fortinet and Sophos were among the providers flagging it.
- The homepage capture contained no body content, metadata, links, resources, or forms.
- Registration continuity records show the domain was registered in 2024 and is approximately 1.7 years old.
- Web-archive records contain 16 snapshots from 2023-09-11 through 2025-10-05, covering 3 years.

Regulatory Verification Notes

The real-world operator identity remains unverified, and the supplied site content contains no identifiable business description, licensing claim, registration number, or authorization disclosure. This is a material transparency gap for any site that might later solicit credentials, payments, investment, trading activity, or other regulated interactions. The available broker-intelligence comparison produced no match; that result is contextual only and is neither evidence of authorization nor a regulatory clearance.

EVIDENCE

- The captured homepage contains no legal, identity, licensing, or registration disclosures.
- The domain registration record identifies Key-Systems GmbH as registrar and lists creation on 2024-12-05 and expiration on 2026-12-05.
- The site is served through AS24940, HETZNER-AS - Hetzner Online GmbH, DE.
- The transport certificate is DV, issued by YR1, and valid to 2026-10-13.

What to Verify Next

Before any interaction beyond passive inspection, an independent party should establish the responsible legal entity, confirm that any claimed service is authorized in the relevant jurisdiction, and validate the domain through an independently sourced contact or registry route rather than relying on information presented by the site. If the domain later exposes account or payment functionality, those destinations should be assessed separately before use.

EVIDENCE

- No successful behavioral run was recorded across 2 runs, limiting validation of how the site would behave during interaction.
- Observed activity included 4 external XHR requests and 4 external POST requests, while no wallet-connection or sensitive-wallet operation was detected.
- The page contained 0 forms, 0 internal links, and 0 external links.

Summary Verdict

The overall posture is critical and unsuitable for sensitive interaction. The available evidence does not support confidence in the site’s legitimacy, operator identity, or operational purpose, and the confirmed external threat signals outweigh the limited benign technical indicators.

Infrastructure Integrity

Cloudflare CDN/WAF protection is present and is a mitigating infrastructure control, but it should not be treated as proof of legitimacy. All observed addresses were CDN edge addresses, and an origin candidate was not identified in the supplied infrastructure assessment.

EVIDENCE

- Cloudflare was detected as the CDN/WAF provider.
- 10 unique addresses were observed, all classified as edge addresses; likely origin candidates: 0.
- Observed edge addresses included 104.21.46.17, 13.248.169.48, 159.69.186.9, and 159.69.42.212.

Closing Assessment

Prospective users should not log in, submit credentials, or initiate financial activity through the site; any further engagement should remain limited to passive observation until independent security and identity clearance has been obtained.

Written analysis generated 2026-08-18 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

1 finding contributed to this verdict, raised by analysis engine, behaviour in a sandbox, external reputation.

01 Sensitive Interaction Risk

- The analysis matched a pattern TrustSniffer treats as a direct threat to a visitor.
  Analysis engine `signal:direct_threat`
- 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 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 272586.com.

- The request stayed on 272586.com. It was not redirected to another domain. CLEAR
- Registration is published under Key-Systems GmbH. CLEAR
- DNS for this domain is served by ndsplitter.com, across 3 name servers. NOTED
- The registration is paid up to 2026-12-05. NOTED
- The earliest public archive of this site is from 2023-09-11. CLEAR
- It is hosted on HETZNER-AS, from a server in DE. NOTED

Domain intelligence

Registrar	Key-Systems GmbH
Hosting	HETZNER-AS - Hetzner Online GmbH, DE
Country	DE
Server IP	159.69.186.9
Name servers	NS1.NDSPLITTER.COM, NS2.NDSPLITTER.COM, NS3.NDSPLITTER.COM
SSL issuer	YR1
SSL expiry	2026-10-13

Domain age	2.93 years (continuous registration)
Domain expiry	2026-12-05
Archive first seen	2023-09-11
Archive snapshots	16
Reputation	VirusTotal: 11 flagged | AbuseIPDB: 0 reports | Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about 272586.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.