

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

fevertime.com

Verdict

0

OUT OF 100

CRITICAL RISK

fevertime.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 2026-08-21 by automated analysis. Classification confidence 55%.

What this site appears to be

Auto-generated index page showing a directory listing served by LiteSpeed Web Server. Minimal content and no interactive elements or monetization cues.

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.

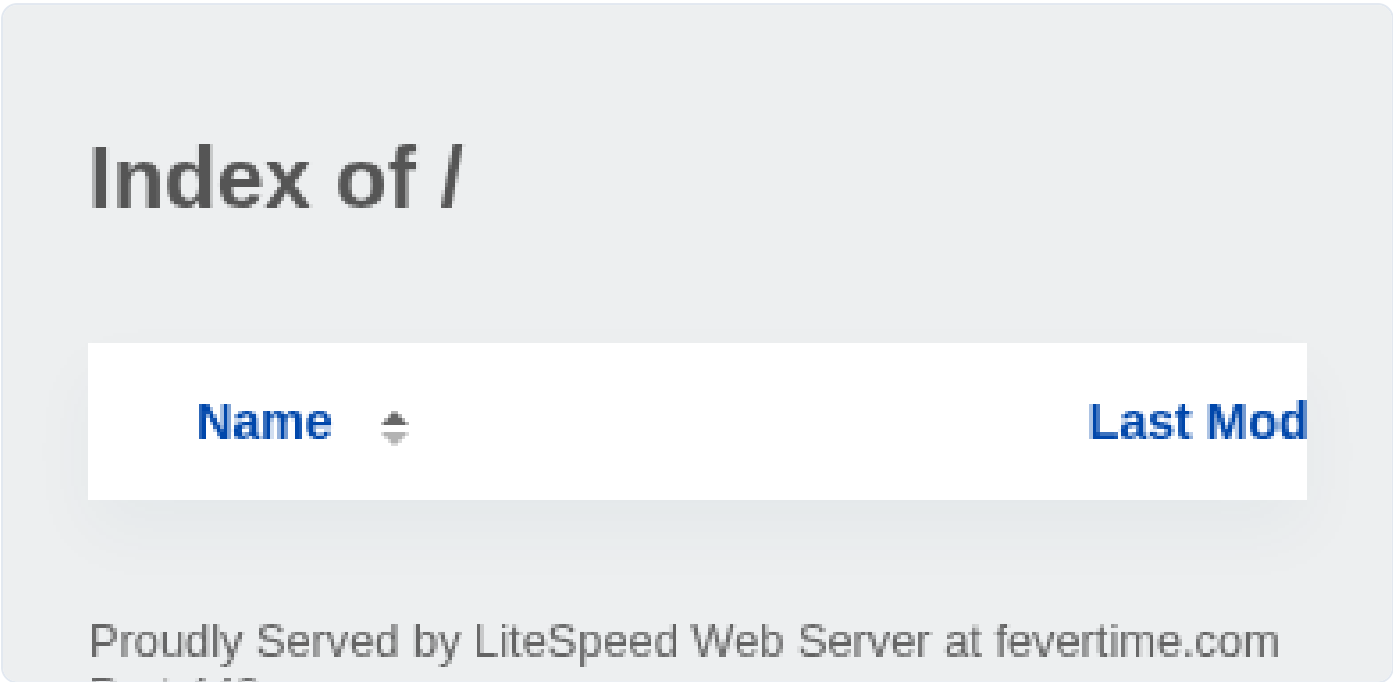
At a glance

The checks that decide most of this verdict.

Malware engines	12 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	12 years old Registered history	CLEAR
Web archive	Archived since 2002 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YR2	NOTED

The page as captured

https://fevertime.com/



What fevertime.com served when TrustSniffer captured it on 2026-08-21. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: more than 10 years (registration continuity).
- Public web-archive history exists since 2002.
- 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.

fevertime.com is an auto-generated public directory listing rather than a developed service website. The homepage presents only an “Index of /” file index and a LiteSpeed Web Server banner, with no visible business proposition, interactive functionality, monetization mechanism, or credential-collection interface.

Scam/Impersonation Risk

Confirmed external threat intelligence identifies the domain as blacklisted, including multiple malicious detections and a tier-one security-vendor detection. This is the decisive contradiction in the assessment and warrants a security-forward posture even though the captured page itself contains no login form, payment request, wallet interaction, or overt malicious script behavior. The absence of a developed service presentation also prevents the directory page from establishing a legitimate purpose or explaining why the domain should be trusted. No conflicting legal identities or brand-impersonation indicators were observed in the supplied page evidence.

EVIDENCE

- The homepage is titled “Index of /” and contains approximately 110 characters of directory-index text rather than an identifiable service presentation.
- External reputation telemetry recorded 12 malicious detections and 1 suspicious detection; the domain was also recorded as blacklisted.
- The observed browser session recorded zero external requests, zero hidden forms, zero wallet-provider interactions, and zero clipboard-write events.

Regulatory Verification Notes

The available material does not establish an independently verified real-world operator. The captured homepage provides no company identity, regulatory status, license number, or governing legal terms, so the site’s regulatory standing cannot be assessed from its own disclosures. This is a material verification gap for any financial or other regulated activity, although it is separate from the confirmed external threat contradiction. The domain’s registration history and valid transport encryption are technical facts, not proof of operator legitimacy.

EVIDENCE

- WHOIS records show registration on 2015-02-20, an age of approximately 11.5 years, and expiry on 2027-02-20 through Name SRS AB.
- Historical archive coverage spans 2002-06-02 through 2025-02-23, representing 24 years tracked.
- The captured homepage discloses no company name, license authority, registration number, or regulated-service terms.

What to Verify Next

Before any sensitive interaction, an independent source should identify the legal operator and confirm that any claimed financial activity is authorized by the relevant jurisdictional regulator. Contact details should be validated through an offline or independently sourced channel rather than relying solely on information presented by the domain. Any file offered through the directory should also be independently verified before download or execution, with endpoint security controls enabled.

EVIDENCE

- The homepage exposes a raw directory listing with downloadable file references rather than a documented business or support process.
- The supplied analysis records the site’s identity-verification status as unverified.
- The supplied regulatory evidence contains no license authority or license number to validate.

Summary Verdict

The overall posture is **critical trust risk**. The confirmed blacklist and malicious-detection signals outweigh the limited benign observations from the static directory page and establish that sensitive interaction is not supported by the available evidence.

Infrastructure Integrity

The domain resolves directly to CYBERCON - CYBERCON, INC. in the Netherlands-associated hosting path, with no detected CDN or WAF layer and a visible origin endpoint. Direct hosting does not itself establish maliciousness, but it provides no protective infrastructure-based mitigation for the reputation concern.

EVIDENCE

- Served from AS7393 (CYBERCON - CYBERCON, INC., US), resolving to 5.172.176.24.
- No CDN was detected; one IP was identified as both the resolved endpoint and likely origin.
- TLS uses a DV certificate issued by YR2, valid to 2026-11-10.

Closing Assessment

Sensitive actions, credential submission, financial activity, and execution of files from the directory should be withheld unless the operator, purpose, and requested activity are independently established through trusted channels.

Written analysis generated 2026-08-21 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, 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
- 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 fevertime.com.

- The request stayed on fevertime.com. It was not redirected to another domain. CLEAR
- Registration is published under Name SRS AB. CLEAR
- DNS for this domain is served by hostek.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 2002-06-02. CLEAR
- It is hosted on CYBERCON, from a server in NL. NOTED

Domain intelligence

Registrar	Name SRS AB
Hosting	CYBERCON - CYBERCON, INC., US
Country	NL
Server IP	5.172.176.24
Name servers	NS3.HOSTEK.COM, NS4.HOSTEK.COM
SSL issuer	YR2
SSL expiry	2026-11-10
Domain age	11.50 years (continuous registration)
Domain expiry	2027-02-20
Archive first seen	2002-06-02
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 12 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about fevertime.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/fevertime.com> · assessed 2026-08-21