

Is 123candle.com a scam? TrustSniffer's high-risk assessment: 0/100

123candle.com

Verdict

0

OUT OF 100

CRITICAL RISK

123candle.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

This page is a standard webserver 'Index of /' directory listing showing folders like cgi-bin/ and wp-content/, and files such as wp-cli.yml. No forms, login prompts, or monetization present.

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	17 years old Registered history	CLEAR
Web archive	Archived since 2011 33 snapshots	CLEAR
Certificate	Encrypted connection Issued by YR2	NOTED

The page as captured

https://123candle.com/

Index of /

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
cgi-bin/	2022-09-27 15:14	-	
wp-cli.yml	2020-09-15 10:36	30	
wp-content/	2025-10-07 05:46	-	

What 123candle.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: more than 10 years (registration continuity).
- Public web-archive history exists since 2011.
- 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.

123candle.com currently presents a raw webserver “Index of /” directory rather than a functioning business website. The homepage exposes folders such as `cgi-bin/` and `wp-content/`, alongside a `wp-cli.yml` file, and provides no visible product, service, monetization, login, or other clear business purpose.

Scam/Impersonation Risk

The principal risk is a confirmed external reputation contradiction: the domain is blacklisted by external security sources, with multiple malicious detections recorded. This is materially more significant than the homepage’s otherwise limited interaction surface. No brand impersonation or conflicting legal-entity identity was observed in the supplied page content, and the directory listing itself contains no phishing form or credential prompt; however, those benign page characteristics do not offset the external threat detections. The site should therefore be treated as unsuitable for login, credential submission, financial activity, or other sensitive interaction.

EVIDENCE

- External reputation telemetry recorded 11 malicious detections and a blacklist hit for the domain; three named security engines contributed to the threat signal.
- The homepage is a directory listing titled "Index of /," exposing `cgi-bin/`, `wp-content/`, and `wp-cli.yml`, with zero forms and no login prompt.
- Behavioral inspection recorded 0 external XHR requests, 0 wallet-connection runs, 0 hidden forms, and 0 suspicious inline scripts across 2 successful runs.

Regulatory Verification Notes

The site does not present an identifiable operating business, terms, licensing statement, registration number, or regulated-service disclosure on the observed homepage. This is a substantive transparency gap for any prospective financial or regulated use, although the absence of a license claim is not independently a finding of fraud. Identity verification remains unresolved: the available material does not independently connect the domain to a real-world operator. Technical continuity and transport security provide limited context but do not establish legitimacy, particularly in light of the blacklist result. No matching broker signal was identified in the supplied third-party context.

EVIDENCE

- Domain registration telemetry: registered 2009-12-28 (~16.65 years old), with expiry recorded as 2026-12-28; registrar: Bluehost Inc.
- Archive telemetry: 33 snapshots spanning 2011-01-28 to 2025-02-22, covering 15 tracked years.
- The site is served from AS31898, ORACLE-BMC-31898 – Oracle Corporation, US.
- TLS telemetry: certificate issued by YR2 at DV validation level, valid to 2026-11-04.

What to Verify Next

Before any engagement, an institution should independently establish whether the domain is intentionally associated with a known organisation and confirm the operator through an official, offline contact route. Any claimed financial, investment, brokerage, or other regulated activity should be checked directly against the relevant regulator's current registry, using the legal entity and jurisdiction rather than relying on the website. Given the confirmed external threat signal, sensitive interaction should remain suspended unless the domain is cleared through formal security review.

EVIDENCE

- The homepage supplies no business description, operator identity, legal terms, licensing information, or service-specific disclosures.
- The observed site state is an exposed server directory rather than a completed customer-facing service.
- Independent security checks produced a blacklist result despite the absence of active forms or monetization on the captured page.

Summary Verdict

The overall posture is critical risk, driven by confirmed external threat detections and the unresolved connection between the domain and a legitimate real-world operator. The limited and technically exposed presentation does not provide a credible basis for sensitive engagement.

Infrastructure Integrity

The site is not shown behind a detected CDN or WAF and resolves through a single hosting address, so no meaningful edge-layer mitigation is evident. The hosting arrangement is a conventional Oracle-hosted environment; infrastructure identification and valid transport encryption should be treated only as technical characteristics, not as evidence that the site or its operator is legitimate.

Closing Assessment

Account access, credential submission, financial transactions, downloads, and other sensitive actions should not proceed unless independent operator validation and formal security clearance are completed.

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

 - 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
 - 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 123candle.com.

- The request stayed on 123candle.com. It was not redirected to another domain. CLEAR
- Registration is published under Bluehost Inc.. CLEAR
- DNS for this domain is served by bluehost.com, across 2 name servers. NOTED
- The registration is paid up to 2026-12-28. NOTED
- The earliest public archive of this site is from 2011-01-28. CLEAR
- It is hosted on ORACLE-BMC-31898, from a server in US. NOTED

Domain intelligence

Registrar	Bluehost Inc.
Hosting	ORACLE-BMC-31898 - Oracle Corporation, US
Country	US
Server IP	162.241.218.31
Name servers	NS1.BLUEHOST.COM, NS2.BLUEHOST.COM
SSL issuer	YR2
SSL expiry	2026-11-04
Domain age	16.65 years (continuous registration)
Domain expiry	2026-12-28
Archive first seen	2011-01-28
Archive snapshots	33
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 123candle.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/123candle.com> · assessed 2026-08-18