

Is elshadaenterprises.co.ke a scam? TrustSniffer's high-risk assessment: 0/100

elshadaenterprises.co.ke

Verdict

0

OUT OF 100

CRITICAL RISK

elshadaenterprises.co.ke 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 2026-08-21 by automated analysis. Classification confidence 55%.

What this site appears to be

A simple directory index page (Index of /) served by LiteSpeed Web Server for elshadaenterprises.co.ke. Shows file listing headers and server signature; no interactive elements 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.

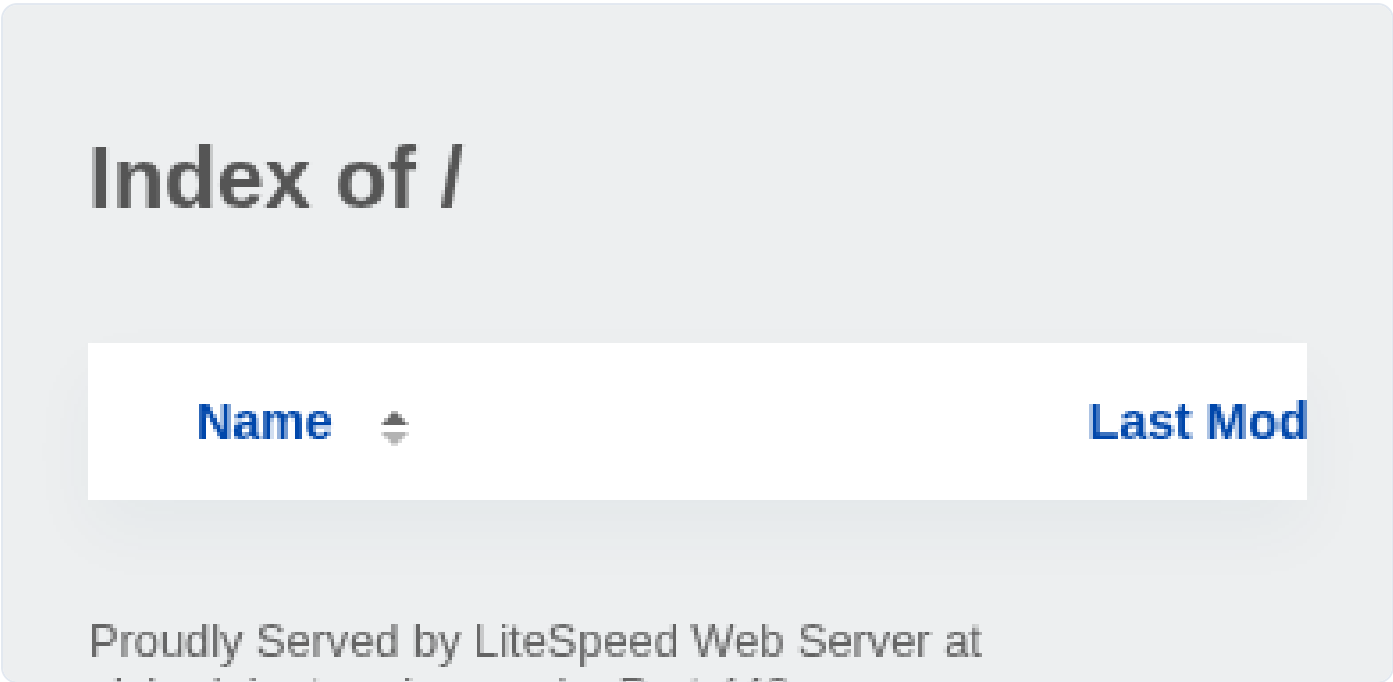
At a glance

The checks that decide most of this verdict.

Malware engines	17 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	5.9 years old Registered history	CLEAR
Web archive	Archived since 2021 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YR2	NOTED

The page as captured

https://elshadaienterprises.co.ke/



What elshadaienterprises.co.ke served when TrustSniffer captured it on 2026-08-21. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: 3 to 10 years (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

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

This website is a bare directory-index page for elshadaienterprises.co.ke, displaying a file-listing header and a LiteSpeed Web Server signature rather than a developed corporate, commercial, or user-service experience. Its apparent function is to expose files from a default web root; no visible account, payment, or transaction purpose is presented.

Scam/Impersonation Risk

Confirmed contradictory reputation signals are present. The domain is blacklisted, and multiple external security detections classify it as malicious or suspicious. Although the observed page contains no login form, payment flow, brand impersonation, or other active user-interaction mechanism, that limited page content does not offset the external reputation evidence. Sensitive interaction with the domain should therefore be treated as unsafe, particularly where credentials, downloads, or financial information could be involved.

EVIDENCE

- External reputation checks recorded 17 malicious detections and 1 suspicious detection.
- The domain was identified on a confirmed blacklist, with blacklist status supported by two external sources.
- The homepage is titled "Index of /" and exposes a directory listing with no forms or transaction controls.

Regulatory Verification Notes

The observed site does not provide a meaningful legal, corporate, or licensing disclosure. Its content is too limited to establish the identity of an operating entity or to determine whether any regulated activity is being conducted. Identity verification remains unconfirmed, and the absence of substantive business disclosures is a material transparency gap rather than independent proof of unlawful conduct. The domain's registration through Webcom Kenya Limited is an administrative fact and does not establish the operator's legitimacy.

EVIDENCE

- The homepage contains only the headings "Index of /," "Name," "Last Modified," and "Size," with no legal-entity or licensing statement.
- The domain was registered in 2020 and is approximately 5.88 years old.
- The domain registrar is Webcom Kenya Limited.
- The transport certificate is DV, issued by YR2, and valid through 2026-10-31.

What to Verify Next

Before any sensitive interaction, an organization should establish the intended operator through an independently obtained contact route and confirm that the requested domain is officially associated with that entity. Any files exposed by the directory should be treated as untrusted until independently validated, and endpoint protection should inspect them before access or execution. If the domain is presented as supporting a regulated service, the claimed entity and authorization should be checked directly with the relevant regulator.

EVIDENCE

- The observed page provides no operator profile, business description, or official contact mechanism.
- The page contains no login, credential-capture, payment, or transaction form through which a legitimate service relationship could be established.

Summary Verdict

The overall posture is **critical trust risk**, driven by confirmed external blacklist status and malicious detections combined with an unverified operating identity and materially insufficient site substance. The website should not be treated as a trustworthy destination for sensitive interaction or as an established business portal.

Infrastructure Integrity

The site resolves directly to one likely origin address hosted by LiquidNet US LLC in the United States, using AS14555, with no CDN or WAF identified. This direct hosting arrangement provides no observed edge-

protection mitigation, while the valid DV certificate confirms encrypted transport only and does not validate the operator or content.

Closing Assessment

Prospective users and organizations should refrain from login, credential submission, financial activity, or downloading site-hosted files unless the domain's ownership and purpose have first been independently confirmed through trusted channels.

Written analysis generated 2026-08-21 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 elshadaienterprises.co.ke.

- The request stayed on elshadaienterprises.co.ke. It was not redirected to another domain.

CLEAR
- Registration is published under Webcom Kenya Limited.

CLEAR
- DNS for this domain is served by webcomke.com, across 4 name servers.

NOTED
- The registration is paid up to 2026-10-02.

NOTED
- The earliest public archive of this site is from 2021-12-01.

CLEAR
- It is hosted on LIQUIDNETLTD1, from a server in US.

NOTED

Domain intelligence

Registrar	Webcom Kenya Limited
Hosting	LIQUIDNETLTD1 - LiquidNet US LLC, US
Country	US
Server IP	162.210.99.158
Name servers	dns1.webcomke.com, dns2.webcomke.com, dns4.webcomke.com, dns3.webcomke.com
SSL issuer	YR2
SSL expiry	2026-10-31
Domain age	5.88 years (continuous registration)
Domain expiry	2026-10-02
Archive first seen	2021-12-01
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 17 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about elshadaienterprises.co.ke 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/elshadaienterprises.co.ke> · assessed 2026-08-21