

Is africangulf.ly a scam? TrustSniffer's high-risk assessment: 5/100

africangulf.ly

Verdict

5

OUT OF 100

CRITICAL RISK

africangulf.ly 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 50%.

What this site appears to be

A standard webserver directory index exposing site files and WordPress artifacts. No sign-in forms, monetization, or investment features. Potential operational risk due to exposed configuration/backups but not directly phishing.

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	None flagged it VirusTotal	CLEAR
Google Safe Browsing	Listed as unsafe Google	RISK
Abuse reports on the host	0 reports AbuseIPDB; shared hosting inflates this count	NOTED
Domain age	4.9 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://africangulf.ly/

Index of /			
Name	Last modified	Size	Description
Thumbs.db	2012-09-05 16:33	23K	

What africangulf.ly 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

Overview

The website currently presents a public directory index rather than a developed business service. Visitors are shown exposed web-server files and WordPress artifacts, including administrative, configuration, archive, and login-related files; no visible monetization, registration, investment, or transaction flow is presented on the captured page.

Scam/Impersonation Risk

Confirmed external threat detections materially outweigh the otherwise limited and apparently informational page content. The domain is blacklisted, including a malicious Google Safe Browsing detection associated with social-engineering activity. The captured homepage does not display an overt phishing form or brand impersonation, and no conflicting legal-entity names were observed; however, behavioral testing recorded two password forms configured for external posting, while the directory listing exposes files such as `wp-config.php` and `ww.zip`. That combination creates a significant risk for sensitive interaction and potential exposure of site or user data, even though the visible page itself is not an active commercial or investment interface.

EVIDENCE

- The domain was flagged as malicious by Google Safe Browsing and appears in an external blacklist.
- The domain was registered on 2021-09-21 and is approximately 4.92 years old, according to the registration record.
- The homepage is titled "Index of /" and exposes WordPress files, including `wp-config.php`, `wp-login.php`, and `ww.zip`.
- Behavioral testing recorded 2 password forms and 2 password forms posting externally, despite no visible login form in the captured directory view.

Regulatory Verification Notes

The captured content does not identify a business purpose, legal entity, licensing authority, registration number, or regulated service. This is a material disclosure gap for any prospective engagement, although the page is primarily a file index rather than a declared financial or commercial service. The registration record names Zakaria M Alnfati and lists LTT local (loc) as registrar, but those details do not independently verify that person as the real-world operator. A valid domain-validated certificate provides transport encryption only; it does not establish legal identity, authorization, or regulatory standing. No matching broker signal was identified in the supplied third-party context.

EVIDENCE

- The homepage contains no visible company, licensing, or regulatory disclosure and presents only a directory index.
- The registration record lists Zakaria M Alnfati as the owner and LTT local (loc) as registrar.
- The TLS certificate is issued by YR2, uses DV validation, and is valid to 2026-10-18T01:45:56+00:00.

What to Verify Next

Before any engagement, an organization should confirm the operator's legal identity and any claimed authorization through the relevant corporate or financial-services registry using independently obtained contact details. Technical review should establish why directory indexing is enabled, whether exposed WordPress and archive files remain accessible, and where the recorded external password submissions are sent. Any internal investigation should preserve the observed files and network behavior for incident-response review rather than treating the visible directory page as a complete representation of the site.

EVIDENCE

- The captured page exposes 26 internal file or directory links and one external link.
- The page contains no forms in the visible DOM, while behavioral testing separately identified externally posting password forms.
- The site's visible metadata includes no meta description, structured data, or canonical declaration.

Summary Verdict

The overall posture is critical and unsuitable for sensitive interaction. The available evidence does not establish a verified operating identity, and confirmed external threat detections create a substantial basis for treating the

site as hostile or compromised rather than as a dependable business destination.

Infrastructure Integrity

The site resolves directly to one likely origin IP, with no detected CDN or WAF and no edge-IP layer identified. This provides no meaningful protective separation between the public service and its origin infrastructure; the hosting environment is associated with a Libyan telecommunications provider.

EVIDENCE

- Hosted on AS21003, General Post and Telecommunication Company (GPTC), Libya.
- The resolved IP address is 62.240.36.36.
- CDN detected: false; WAF or trusted CDN vendors detected: none; likely origin IP count: 1.

Closing Assessment

Sensitive actions should not be performed through this site. Any required investigation should remain controlled, non-interactive, and subject to independent identity, authorization, and technical remediation checks before engagement is reconsidered.

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, 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
- 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 africangulf.ly.

- The request stayed on africangulf.ly. It was not redirected to another domain. CLEAR
- Registration is published under LTT local (loc). CLEAR
- DNS for this domain is served by ltdns.net, across 2 name servers. NOTED
- The registration is paid up to 2026-09-21. NOTED
- The earliest public archive of this site is from 2021-11-24. CLEAR
- It is hosted on General Post and Telecommunication Company (GPTC), from a server in LY. NOTED

Domain intelligence

Registrar	LTT local (loc)
Hosting	General Post and Telecommunication Company (GPTC) - General Post and Telecommunication Company (GPTC), LY
Country	LY
Server IP	62.240.36.36
Name servers	dns3.ltdns.net, dns2.ltdns.net
SSL issuer	YR2
SSL expiry	2026-10-18
Domain age	4.92 years (continuous registration)
Domain expiry	2026-09-21
Archive first seen	2021-11-24
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 0 flagged AbuseIPDB: 0 reports Google Safe Browsing: 1 match

About this assessment

A trust score summarises the evidence TrustSniffer could collect about africangulf.ly 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.

