

Is activegrp.co.za a scam? TrustSniffer's high-risk assessment: 5/100

activegrp.co.za

Verdict

5

OUT OF 100

CRITICAL RISK

activegrp.co.za 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 2026-09-24 by automated analysis. Classification confidence 55%.

What this site appears to be

Company site for Active Group providing waterproofing, fire protection, insulation, floor coverings and jointing services. Includes contact information and a physical location in Centurion. Appears to be a small to mid-sized local contractor brochure site.

Compromised host notice

A threat-intelligence feed listed a file on activegrp.co.za as hosting scam content (last seen 2026-09-24). TrustSniffer's evidence indicates that the site itself was compromised: the listing concerns a file placed on it by someone else, and the site's owner is most likely a victim, not the actor.

Until the file is removed, downloading anything from this site is not safe. If you run this site, remove the listed file, update the site software and its plugins, change its passwords and review it for other unauthorized changes.

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

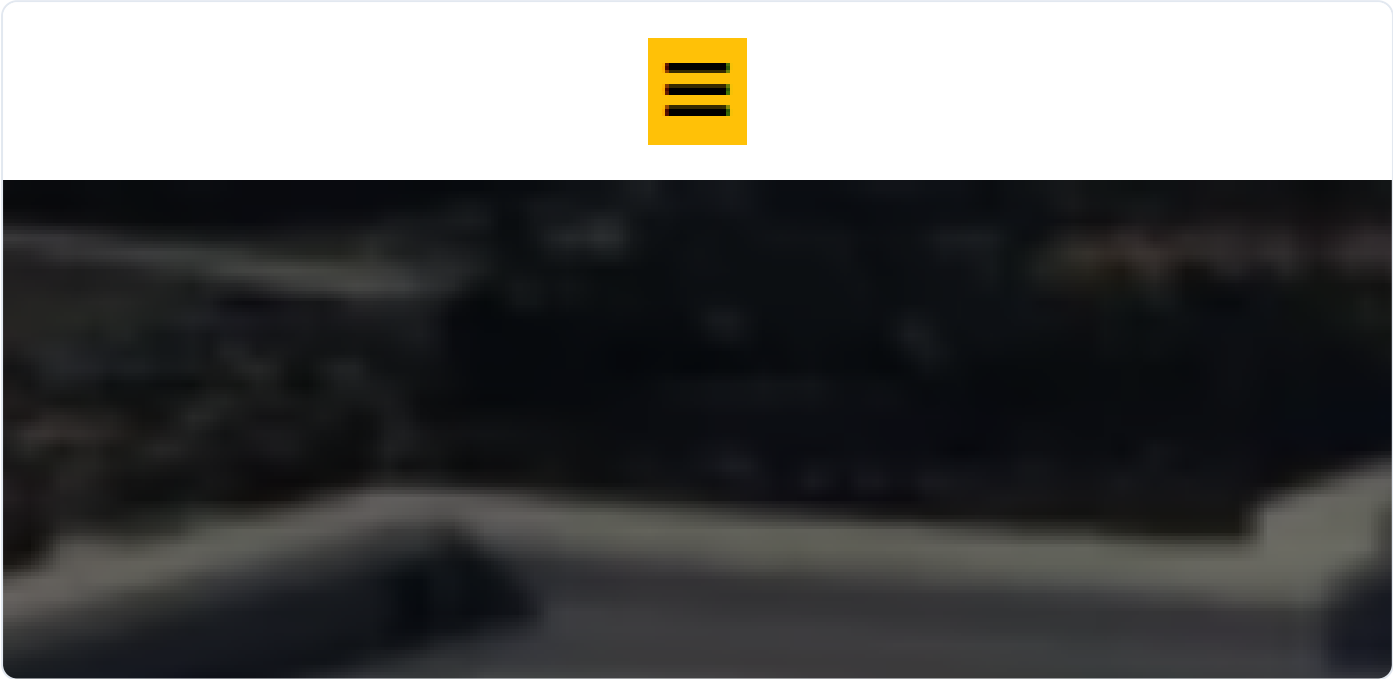
The checks that decide most of this verdict.

Malware engines	3 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	5.6 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://activegrp.co.za/



What activegrp.co.za served when TrustSniffer captured it on 2026-09-24. 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 flagged this site in external intelligence checks, indicating elevated compromise/scam exposure that requires immediate caution.

This website presents Active Group as a local construction-services contractor offering waterproofing, fire protection, insulation, floor coverings, construction jointing, maintenance, and related material-installation services for commercial, industrial, residential, and institutional buildings.

Scam/Impersonation Risk

The site's visible content is a conventional contractor brochure and does not itself present a login form, payment workflow, cryptocurrency feature, or other obvious abuse mechanism. However, that benign presentation is outweighed by confirmed external blacklisting and multiple malicious or suspicious detections, including a detection by Fortinet. The available evidence therefore supports a **critical sensitive-interaction risk** despite the site's ordinary construction-services content. No conflicting legal-entity names or direct brand-impersonation indicators are present in the supplied pages, but the site's apparent business purpose does not offset the external threat findings.

EVIDENCE

- Homepage and services content describe waterproofing, fire protection, insulation, floor coverings, and construction jointing rather than an online account or financial-service workflow.
- External reputation checks recorded 3 malicious and 2 suspicious detections, with Fortinet identified among the flagged vendors.
- The domain is recorded as registered on 2021-03-04, with an age of 5.56 years.
- Historical records cover 4 years, from 2021-11-24 through 2024-10-08.

Regulatory Verification Notes

The site identifies itself as Active Group and describes a legitimate-looking construction-services model, but the available evidence does not independently verify the real-world operator. No licence, registration number, or formal corporate disclosure is identified in the supplied business pages; this is a transparency and verification gap rather than, by itself, proof of fraud. The operator identity should therefore remain treated as unverified, and the external blacklist signal should be considered materially more significant than the site's professional presentation.

EVIDENCE

- The services page describes waterproofing, fire protection, insulation, floor coverings, and jointing work, including use of bituminous, polyurethane, acrylic, and epoxy materials.
- The supplied business content does not state a licence number, registration number, or licensing authority.
- The site is served on AS37611 by AFRIHOST SP (PTY) LTD - AFRIHOST SP (PTY) LTD, ZA.
- Transport encryption uses a DV certificate issued by YR2, valid to 2026-10-29.

What to Verify Next

Before any sensitive engagement, an independent party should confirm that the Active Group named on the site is the same entity responsible for the stated Centurion operations, obtain applicable contractor or trade-registration details directly from the relevant authority, and validate contact details through an offline or independently sourced channel. Any proposed quotation, deposit, document exchange, or remote-access request should be checked against independently obtained company records before acceptance.

EVIDENCE

- The contact material provides a physical location in Centurion that can be independently checked.
- The homepage identifies the business as “Active Group – Built with SitePad,” but the supplied content does not independently establish the legal operator.
- The site was observed without a login form, sensitive form, hidden form, or external password-submission destination.

Summary Verdict

The overall posture is **critical risk for sensitive interaction**. The site may resemble a genuine small contractor brochure, but the confirmed blacklist status and external malicious detections prevent the available evidence from supporting normal trust in credential, financial, or other sensitive engagement. Operator identity remains unverified.

Infrastructure Integrity

The site resolves directly to a likely origin address rather than through a detected CDN or WAF layer. This provides no meaningful protective separation between the public service and the hosting environment; infrastructure characteristics should therefore be treated as neutral to cautionary rather than as evidence of legitimacy.

Closing Assessment

The appropriate posture is read-only observation until the operator, business standing, and any proposed transaction are independently validated through authoritative records and offline contact channels.

Written analysis generated 2026-09-24 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

- 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 activegrp.co.za.

- The request stayed on activegrp.co.za. It was not redirected to another domain. CLEAR
- Registration is published under Afrihost. CLEAR
- DNS for this domain is served by co.za, across 4 name servers. NOTED
- The registration is paid up to 2027-03-04. NOTED
- The earliest public archive of this site is from 2021-11-24. CLEAR
- It is hosted on AFRIHOST SP (PTY) LTD, from a server in ZA. NOTED

Domain intelligence

Registrar	Afrihost
Hosting	AFRIHOST SP (PTY) LTD - AFRIHOST SP (PTY) LTD, ZA
Country	ZA
Server IP	154.0.175.57
Name servers	ns.dns1.co.za, ns.dns2.co.za, ns.otherdns.net, ns.otherdns.com
SSL issuer	YR2
SSL expiry	2026-10-29
Domain age	5.56 years (continuous registration)
Domain expiry	2027-03-04
Archive first seen	2021-11-24
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 3 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about activegrp.co.za 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/activegrp.co.za> · assessed 2026-09-24