

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

akfa.gr

Verdict

0

OUT OF 100

CRITICAL RISK

akfa.gr 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 75%.

What this site appears to be

Small Greek ecommerce site (akfa.gr) listing three products (lawnmower heads and blade) with prices and standard WooCommerce storefront elements. No forms requesting sensitive credentials or financial transfers on this page.

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	13 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	9.1 years old Registered history	CLEAR
Web archive	Archived since 2017 569 snapshots	CLEAR
Certificate	Encrypted connection Issued by YE2	NOTED

The page as captured

https://akfa.gr/

akfa.gr

☰ Menu

What akfa.gr 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 2017.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

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

akfa.gr is a small Greek-language online retail storefront presenting three garden-equipment replacement products—two lawnmower heads and a blade—through a conventional WooCommerce shop, with product prices, cart functionality, checkout, and account access indicating a direct-sale ecommerce model.

Scam/Impersonation Risk

The site presents a **critical sensitive-interaction risk** because external security intelligence records a confirmed blacklist hit, including 13 malicious detections and one suspicious detection, with Fortinet and Sophos among the flagged providers. This is a material contradiction to the otherwise ordinary storefront presentation and warrants treating login, credential submission, checkout, and financial activity as unsafe. The behavioral review also detected two hidden forms in both observed runs, although the visible shop page contained no login form or visible request for sensitive information. The evidence does not establish brand impersonation or conflicting legal identities, but the external detections are sufficient to support a clearly cautionary assessment.

EVIDENCE

- The homepage/shop page lists three physical garden-equipment products with prices and cart/checkout functions.
- Behavioral inspection detected hidden forms in 2 of 2 runs, with 0 external posts and 0 password forms directed externally.
- External reputation assessment recorded 13 malicious detections, 1 suspicious detection, and blacklist status from VT and EXTERNAL_BLACKLIST.

Regulatory Verification Notes

The available legal and identity disclosures are unclear, and the operator could not be independently connected to a verified real-world entity from the supplied evidence. The site does not present a licensing authority or license number; for a physical-goods retailer this is a transparency and business-verification issue rather than independent proof of misconduct. The ordinary WooCommerce presentation, long registration continuity, sustained archival record, and valid transport encryption provide contextual legitimacy signals, but they do not offset the external security detections or establish operator identity. The certificate is domain-validated only, so it confirms encrypted transport rather than legal ownership.

EVIDENCE

- Domain age is 9.122518822724162 years; archive history contains 569 snapshots spanning 2017-07-06 to 2026-06-12, with 10 years tracked.
- The homepage uses WordPress, Storefront, and WooCommerce; no license authority or license number is presented in the supplied site content.
- The site is hosted by AS-HOSTINGER — Hostinger International Limited, CY, on AS47583; the observed hosting country is DE.
- TLS uses issuer YE2 with DV validation and is valid to 2026-10-04T02:13:20+00:00.

What to Verify Next

Before any transaction or account interaction, an institution should independently confirm that the business exists, that the seller's legal name and address correspond to an authoritative business record, and that the relevant payment route provides chargeback or equivalent purchaser protection. Any required business registration or consumer-commerce authorization should be checked directly with the applicable Greek registry or authority. Security teams should also validate the blacklist detections and obtain a current disposition before permitting the domain in enterprise environments.

EVIDENCE

- The site's visible shop page contains three products but does not, in the supplied content, establish the operator's independently verified legal identity.
- The visible page has no sensitive form, while behavioral inspection separately detected hidden forms in both runs.
- The site's stated transaction model is direct ecommerce sales through cart and checkout.

Summary Verdict

The overall posture is critical and unsuitable for sensitive interaction. The storefront's conventional appearance and historical continuity do not overcome the converging external threat indicators that drive the assessment, while operator identity remains unverified.

Infrastructure Integrity

The site is protected by a CDN/WAF layer, with observed edge infrastructure including 162.55.161.171 on AS24940 and two potential origin candidates. This provides a mitigating reduction in direct exposure but is not evidence of legitimacy; the infrastructure also shows some fragmentation between edge and hosting components.

Closing Assessment

Enterprise controls should restrict the domain to passive observation until the external detections are independently resolved and the seller's identity and transaction safeguards are 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

1 finding contributed to this verdict, raised by analysis engine, behaviour in a sandbox, 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
 - The page contained a form a visitor cannot see.
Behaviour in a sandbox rule:BEHAV_HIDDEN_FORMS
 - 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 akfa.gr.

- The request stayed on akfa.gr. It was not redirected to another domain.

CLEAR

- The earliest public archive of this site is from 2017-07-06. CLEAR
- It is hosted on AS-HOSTINGER, from a server in DE. NOTED

Domain intelligence

Registrar	Not available
Hosting	AS-HOSTINGER - Hostinger International Limited, CY
Country	DE
Server IP	2a02:4780:27:1145:0:21a8:679e:4
Name servers	Not available
SSL issuer	YE2
SSL expiry	2026-10-04
Domain age	9.12 years (continuous registration)
Domain expiry	Not available
Archive first seen	2017-07-06
Archive snapshots	569
Reputation	VirusTotal: 13 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

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