

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

geoxsecurity.ro

Verdict

5

OUT OF 100

CRITICAL RISK

geoxsecurity.ro 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 2026-09-22 by automated analysis. Classification confidence 55%.

What this site appears to be

Website for a private security company (Geox/Panthar themed template) describing services, company history, contact info, and testimonials. No forms or financial/investment flows detected.

Compromised host notice

A threat-intelligence feed listed a file on geoxsecurity.ro as distributing malware (last seen 2026-09-01). 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

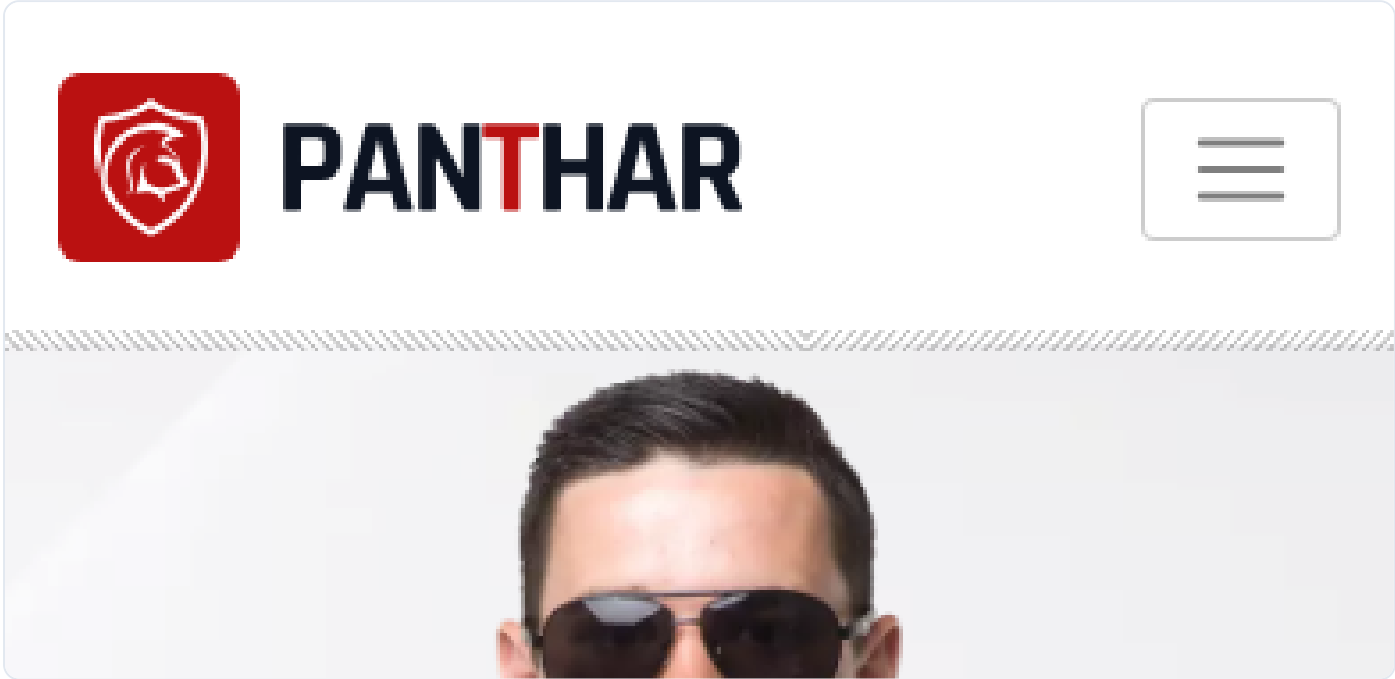
The checks that decide most of this verdict.

Malware engines	5 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	2.5 years old Registered history	CLEAR
Web archive	Archived since 2024 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YR1	NOTED

The page as captured

https://www.geoxsecurity.ro/



What geoxsecurity.ro served when TrustSniffer captured it on 2026-09-22. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: 1 to 3 years (registration continuity).
- Public web-archive history exists since 2024.
- 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.

The website presents itself as Geox Security, a private security-services company offering bank, personal, office, surveillance, and consulting services through contact-led quotations and service engagements. Its content is corporate and service-oriented, with no on-site payment, investment solicitation, login form, or credential-collection workflow identified.

Scam/Impersonation Risk

The site has a **critical interaction risk** because external threat intelligence recorded confirmed blacklist status, including multiple malicious detections. This materially outweighs the otherwise ordinary service-company presentation and the absence of on-site financial or credential-harvesting functions. The homepage also combines Geox Security branding with American Panthar Security recruitment copy, a Bali address, and references to expansion in Colorado, creating uncertainty about the commercial presentation without establishing a confirmed identity contradiction. The contact page contains the address “info@example.come,” a contact-channel integrity anomaly consistent with a deliverability-breaking typo or possible typosquat. No separate confirmed impersonation or phishing page was established in the supplied content.

EVIDENCE

- The domain's registration record shows creation on 2024-03-12 and an age of 2.53 years.
- External reputation telemetry records 5 malicious and 1 suspicious detections, with confirmed blacklist status from two sources.
- The homepage presents Geox Security, American Panthar Security, a Bali address, and Colorado expansion language in the same corporate presentation.
- The contact information includes “info@example.come.”

Regulatory Verification Notes

The website describes private security services but does not claim a license, identify a licensing authority, or provide a license number in the available business content. This is a regulatory-disclosure gap rather than independent proof of fraud. Operator identity is only apparently connected to a real-world business, and the mixed branding and jurisdictional references make independent confirmation of the contracting entity and service jurisdiction particularly important. No matching broker-reputation record was identified in the supplied third-party context.

EVIDENCE

- The homepage and service content describe bank, personal, office, and surveillance security services without a stated license authority or registration number.
- The About and contact-oriented content provides business descriptions and contact routes but does not establish a verified legal entity.
- The site's transport encryption uses a DV certificate issued by YR1, valid through 2026-11-28.

What to Verify Next

Before any sensitive engagement, independently confirm the contracting entity, physical operating address, and authority to provide security services with the relevant corporate and licensing registries. Confirm official contact channels through an independently sourced telephone number or other offline route, and require a contract that identifies the legal counterparty, liability terms, insurance, jurisdiction, and payment beneficiary. Sensitive credentials, access details, and financial information should not be submitted unless those checks produce a consistent result.

EVIDENCE

- The site's displayed branding, address, and geographic references require reconciliation against an independent business record.
- No license authority or license number is stated in the available service and company content.
- The site provides a quote/contact-led model rather than an on-site payment flow, making the contracting documentation and payment beneficiary central verification points.

Summary Verdict

The website should be treated as an untrusted and high-risk destination for sensitive interaction. Its service-oriented appearance does not overcome the confirmed external reputation contradictions, and the available evidence does not support ordinary login, credential submission, or financial engagement.

Infrastructure Integrity

The site resolves directly to infrastructure operated by ROMARG SRL in Romania, with no trusted CDN or WAF layer identified and one likely origin address exposed. This provides limited infrastructure mitigation; the hosting arrangement and a valid DV TLS certificate establish technical reachability and encrypted transport, but neither is evidence of operator legitimacy.

EVIDENCE

- Hosted on AS205275, ROMARG - ROMARG SRL, RO.
- The resolved address is 89.42.218.217 in Romania, with 1 unique IP, 0 edge IPs, and 1 likely origin IP.
- TLS is DV validation, issued by YR1, valid to 2026-11-28T11:50:12+00:00.

Closing Assessment

The proportionate course is to restrict activity to passive review while independently validating the business, licensing position, and contracting entity through authoritative records before considering any operational engagement.

Written analysis generated 2026-09-22 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
- The page rewrote itself after it was interacted with, so what a visitor first sees is not what they end up on.
Behaviour in a sandbox rule:BEHAV_DOM_DIFF_AFTER_INTERACTION
- 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	LIKELY
Identity score	80/100
Identity verification confidence	80%

- Trusted social count=4

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 geoxsecurity.ro.

- The request stayed on geoxsecurity.ro. It was not redirected to another domain. CLEAR
- Registration is published under Romarg SRL. CLEAR
- DNS for this domain is served by romarg.com, across 4 name servers. NOTED
- The earliest public archive of this site is from 2024-08-28. CLEAR
- It is hosted on ROMARG, from a server in RO. NOTED

Domain intelligence

Registrar	Romarg SRL
Hosting	ROMARG - ROMARG SRL, RO
Country	RO
Server IP	89.42.218.217
Name servers	ns1.romarg.com, ns2.romarg.com, ns3.romarg.com, ns4.romarg.com
SSL issuer	YR1
SSL expiry	2026-11-28
Domain age	2.53 years (continuous registration)
Domain expiry	Not available

Archive first seen	2024-08-28
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 5 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about geoxsecurity.ro 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/geoxsecurity.ro> · assessed 2026-09-22