

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

coolairesgroup.com

Verdict

5

OUT OF 100

CRITICAL RISK

coolairesgroup.com 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 2026-09-17 by automated analysis. Classification confidence 55%.

What this site appears to be

Cool Aires Group S.A. (Panamá) — provides residential and commercial air conditioning maintenance, repair and installation services and sells related electrical/HVAC parts. Contact info and product listings are present; typical local business site.

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	15 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 Sectigo Public Server Authentication CA DV R36	NOTED

The page as captured

<https://coolairesgroup.com/>



What coolairesgroup.com served when TrustSniffer captured it on 2026-09-17. 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, Sophos flagged this site in external intelligence checks, indicating elevated compromise/scam exposure that requires immediate caution.

Cool Aires Group is a Panamá-focused local HVAC services and ecommerce website presenting residential and commercial air-conditioning maintenance, repair, installation, ducting, authorized-brand services, and sales of related parts and accessories. Its apparent business model is to generate revenue through service engagements and direct product sales.

Scam/Impersonation Risk

The site's visible content is consistent with a conventional HVAC company and does not show a login form, credential-harvesting form, wallet functionality, or explicit brand impersonation. However, this benign presentation is outweighed by confirmed external blacklist status and multiple malicious detections, creating a material risk that the domain, hosting environment, or associated content has been classified as harmful. No conflicting legal-entity names were observed across the supplied content, but the independently verified identity of the operator remains unresolved. The site should therefore be treated as unsuitable for credential submission, financial transactions, or other sensitive interaction. Evidence:

- External reputation telemetry records 15 malicious and 3 suspicious detections among 23 evaluated results, with a confirmed blacklist status.
- The homepage presents a local HVAC business rather than a security-sensitive service and contains no login form or hidden sensitive form.
- Domain registration records show creation on 2024-03-14, with an age of approximately 2.51 years.

Regulatory Verification Notes

The site identifies itself as Cool Aires Group S.A. in Panamá and describes HVAC services, but the supplied pages do not present a license number, regulatory authorization, or independently verifiable corporate-registration reference. This is a material disclosure gap for confirming the operating entity and any obligations associated with commercial sales or authorized-brand claims; it is not, by itself, proof of fraud. The available evidence does not independently verify the named entity, and the site's transport certificate establishes encrypted transmission rather than legal identity or authorization. Evidence:

- The homepage and company-description content identify Cool Aires Group S.A. and describe the business as Panamá-based.
- No license authority or license number is stated in the supplied business-model and page-disclosure evidence.
- The domain is registered through GoDaddy.com, LLC.
- TLS uses a DV certificate issued by Sectigo Public Server Authentication CA DV R36, valid through 2026-12-24.

What to Verify Next

Before any engagement, the claimed company name should be checked against Panamá's applicable corporate and commercial registries, and any authorized-brand representation should be confirmed directly with the named manufacturers. Contact details should be validated through an independently sourced business channel rather than relying solely on the website. Any purchase should use a payment method with meaningful dispute protection, and sensitive information should not be submitted until the external blacklist issue and operator identity have been independently resolved. Evidence:

- The contact area provides a contact form and live-chat function, creating channels that can be tested against independently sourced business information.
- The site offers direct product sales, so merchant identity, refund terms, fulfilment arrangements, and payment protections require confirmation before purchase.
- The supplied evidence contains no independently verified registration or licensing reference for the claimed entity.

Summary Verdict

The overall posture is **critical trust risk**. Although the site presents a plausible local-business profile and lacks several common page-level phishing mechanisms, confirmed external malicious and blacklist signals create a decisive contradiction that prevents the domain from being treated as trustworthy for sensitive interaction.

Infrastructure Integrity

The site resolves directly to a single origin address, with no detected CDN or WAF edge layer and no origin-masking arrangement. This provides limited infrastructure mitigation: the hosting environment is identifiable as

AS46606, Unified Layer, US, and the absence of an edge protection layer means the technical infrastructure does not offset the external reputation findings. Evidence:

- Hosted on AS46606, Unified Layer, US.
- The resolved server address is 162.215.121.104 in the US.
- TLS validation is DV; the certificate issuer is Sectigo Public Server Authentication CA DV R36 and its stated expiry is 2026-12-24.
- Infrastructure telemetry reports one unique IP, zero edge IPs, and one likely origin IP.

Closing Assessment

The proportionate action is to restrict activity to passive viewing while independently validating the operator, business registration, and any proposed transaction through trusted external channels; credentials, payment details, and other sensitive information should not be provided in the interim.

Written analysis generated 2026-09-17 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 registration record withholds contact details for the operator.
Registration and ownership rule:KF_WHOIS_HIDDEN
 - Registration details are held behind a privacy service, so no operator is named publicly. This is common and legal, and it also means there is nobody to check.
Registration and ownership rule:KF_WHOIS_PRIVATE
- 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	25%

- 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 coolairesgroup.com.

- The request stayed on coolairesgroup.com. It was not redirected to another domain. CLEAR
- Registration is published under GoDaddy.com, LLC. CLEAR
- DNS for this domain is served by site5.com, across 2 name servers. NOTED
- The registration is paid up to 2027-03-14. NOTED
- The earliest public archive of this site is from 2024-04-18. CLEAR
- It is hosted on UNIFIEDLAYER-AS-1, from a server in US. NOTED

Domain intelligence

Registrar	GoDaddy.com, LLC
Hosting	UNIFIEDLAYER-AS-1 - Unified Layer, US
Country	US
Server IP	162.215.121.104
Name servers	DNS.SITE5.COM, DNS2.SITE5.COM
SSL issuer	Sectigo Public Server Authentication CA DV R36
SSL expiry	2026-12-24
Domain age	2.51 years (continuous registration)
Domain expiry	2027-03-14
Archive first seen	2024-04-18
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 15 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about coolairesgroup.com 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.