

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

securitydirectapp.com

Verdict

5

OUT OF 100

CRITICAL RISK

securitydirectapp.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

Assessed 2026-08-21 by automated analysis. Classification confidence 50%.

What this site appears to be

Page states the domain is managed by OutThink, offering cybersecurity training and phishing simulations for organizations; content explicitly for educational security awareness.

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	2.4 years old Registered history	CLEAR
Web archive	Never archived No public history of this site	WATCH
Certificate	Encrypted connection Issued by Amazon RSA 2048 M01	NOTED

The page as captured

<https://securitydirectapp.com/>

This domain is managed by OutThink, a cybersecurity company who operate cybersecurity training, phishing simulations, and detection and analysis of human risk at organizations around the world.

Phishing simulations are managed by our customers, to educate their employees on what to look out for and to protect themselves from phishing attacks.

The content of this website is purely for educational security awareness purposes.

What securitydirectapp.com served when TrustSniffer captured it on 2026-08-21. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: 1 to 3 years (registration continuity).
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.
- The operator behind the site could not be independently connected to a real-world brand or person.

Full analysis

Overview

securitydirectapp.com presents an informational cybersecurity-awareness service focused on organizational training and phishing simulations, with an apparent enterprise business model based on security education and related professional services.

Scam/Impersonation Risk

The site's educational presentation contains no observed brand-impersonation indicators, credential-collection form, or other page-level fraud markers. However, this benign presentation is contradicted by confirmed external threat detections: the domain is marked malicious by Google Safe Browsing and is also present on an external blacklist, with the associated detection identifying social-engineering activity. These findings create a material risk for sensitive interaction despite the site's stated security-awareness purpose.

EVIDENCE

- The homepage presents educational security-awareness content and describes cybersecurity training and phishing simulations.
- Google Safe Browsing reports the domain as malicious, and a separate external blacklist records the domain.
- The page analysis found no login form, hidden form, or suspicious brand-impersonation indicator on the captured homepage.

Regulatory Verification Notes

The available content represents the site as managed by OutThink, but that connection to a real-world operator is not independently verified. No licensing claim or registration number is presented; for a cybersecurity-training service, the applicable licensing requirement is not established by the supplied evidence, but the omission limits formal due-diligence confirmation. Technical legitimacy signals are present—including Amazon Registrar registration and valid domain-validated TLS—but they do not resolve the external threat detections or establish operator identity.

EVIDENCE

- Domain registration: 2024-03-15T07:57:15Z; age 2.44 years; registrar Amazon Registrar, Inc.
- Served from AS16509 (AMAZON-02 - Amazon.com, Inc., US).
- TLS certificate issued by Amazon RSA 2048 M01, validation level DV, valid to 2027-02-15T23:59:59+00:00.

What to Verify Next

Before any sensitive engagement, an organization should independently confirm that the domain is an authorized OutThink property through a previously known corporate channel or an offline business contact. Any proposed commercial relationship should also be validated through independently sourced contracting details, payment instructions, and corporate documentation rather than information supplied solely by this domain. If access is unavoidable for investigation, it should remain limited to passive review until the external detections have been formally explained and cleared.

EVIDENCE

- The homepage returned HTTP status 200 in 2 of 2 successful behavioral runs.
- Behavioral testing recorded 0 external XHR requests, 0 external POST requests, 0 wallet-connection runs, and 0 hidden forms.
- No sensitive form destination was detected during page analysis.

Summary Verdict

The overall posture is critical and unsuitable for sensitive interaction. The site's professional-looking educational content and valid transport security are outweighed by confirmed external threat detections, while the operator connection remains unverified.

Infrastructure Integrity

The website is protected by AWS CDN/WAF infrastructure. All three observed addresses—52.49.167.160, 54.154.92.77, and 54.72.172.242—resolve to AS16509 Amazon edge infrastructure, and no origin candidate was observed; this provides a mitigating layer against direct origin exposure but is not evidence of legitimacy.

Closing Assessment

The domain should be treated as read-only intelligence until its operator relationship and external threat status are independently resolved; login, credential submission, and financial activity should not proceed beforehand.

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, 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
- 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 securitydirectapp.com.

- The request stayed on securitydirectapp.com. It was not redirected to another domain. CLEAR
- Registration is published under Amazon Registrar, Inc.. CLEAR
- DNS for this domain is served by awsdns-15.com, across 4 name servers. NOTED
- The registration is paid up to 2027-03-15. NOTED
- It is hosted on AMAZON-02, from a server in US. NOTED

Domain intelligence

Registrar	Amazon Registrar, Inc.
Hosting	AMAZON-02 - Amazon.com, Inc., US

Country	US
Server IP	54.72.172.242
Name servers	NS-122.AWSDNS-15.COM, NS-1524.AWSDNS-62.ORG, NS-1871.AWSDNS-41.CO.UK, NS-778.AWSDNS-33.NET
SSL issuer	Amazon RSA 2048 M01
SSL expiry	2027-02-15
Domain age	2.44 years (continuous registration)
Domain expiry	2027-03-15
Archive first seen	Not available
Archive snapshots	0
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 securitydirectapp.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.

This report online: <https://trustsniffer.com/report/securitydirectapp.com> · assessed 2026-08-21