

Is guardtrack.co.uk a scam? TrustSniffer's high-risk assessment: 0/100

guardtrack.co.uk

Verdict

0

OUT OF 100

CRITICAL RISK

guardtrack.co.uk 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 2026-08-21 by automated analysis. Classification confidence 55%.

What this site appears to be

A bare login page titled 'GUARDTRACK | Login' requesting email and password with no explanatory content, contact info, or verifiable business details. Treated as a login-only unknown resource and potentially risky.

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	6 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	1.2 years old Registered history	CLEAR
Web archive	Archived since 2018 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YR1	NOTED

The page as captured

https://www.guardtrack.co.uk/user/signin

GuardTrack

Email

Enter Your Email

What guardtrack.co.uk 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).
- Public web-archive history exists since 2018.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

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

This website is a single-purpose login portal titled "GUARDTRACK | Login," presenting only email and password fields, a login control, a "Remember me" option, and password-recovery text; its apparent purpose is to authenticate users to an otherwise unidentified service.

Scam/Impersonation Risk

The site presents a **critical sensitive-interaction risk**. External security intelligence recorded malicious detections and confirmed blacklist placement across two external sources, while the page itself is a credential-collection interface with no service explanation, company identity, contact information, or other context. The combination of a login-only presentation, a prompt-injection indicator, and adverse external detections is materially inconsistent with treating the portal as a trusted authentication endpoint. No conflicting legal-entity names or confirmed brand impersonation were identified in the supplied evidence, but those absences do not offset the confirmed external warnings.

EVIDENCE

- Login page: Requests an email address and password while providing no explanatory service content, business identity, or contact details.
- Login page: Contains the red flags “LOGIN_PAGE_ONLY_NO_CONTEXT” and “prompt_injection_attempt.”
- External reputation telemetry: 6 malicious detections were recorded among 11 effective evaluations; blacklist status was confirmed by 2 sources.
- Domain and archive telemetry: Registered in 2024 (~1.16 years old; 423 days); 7 archive snapshots spanning 2018–2026, with 9 years tracked.

Regulatory Verification Notes

The available identity evidence is insufficient to independently connect the portal to a verified real-world operator. The login page does not disclose a company name, licensing basis, registration number, governing jurisdiction, or accountable business contact, leaving the service’s legal and regulatory status unclear. This is a verification gap rather than a standalone determination of fraud; however, in combination with the external threat findings, it substantially limits the basis for relying on the portal for regulated or financially sensitive activity. No matching broker signal was identified in the supplied third-party contextual dataset, which is neither a licensing confirmation nor a clearance.

EVIDENCE

- Login page: No visible company, licensing, registration, jurisdiction, terms, privacy, or contact disclosure.
- Hosting telemetry: Served from AS14061 (DigitalOcean, LLC, US).
- Transport security telemetry: TLS certificate issued by YR1, domain-validated (DV), valid to 2026-10-29.
- Authority telemetry: Page-authority assessment was in the low band.

What to Verify Next

Before any interaction, an institution should identify the service through an independently obtained official source rather than relying on the portal’s page title or login flow. The purported operator, business registration, applicable license, and official domain should be confirmed through the relevant corporate or regulatory registry. Any password-recovery or support process should be validated through a separately sourced channel, and credential reuse should be ruled out if interaction has already occurred.

EVIDENCE

- Independent registry check: Required to establish the operator’s legal identity and any applicable authorization.
- Official-domain confirmation: Required through a separately sourced corporate or service channel.
- Account-security review: Appropriate where credentials may already have been entered or reused.
- Contact-channel validation: Should be completed through an independently obtained official route.

Summary Verdict

The overall posture is critical, with the available evidence supporting a conclusion that the portal is not suitable for sensitive interaction. Its real-world operator remains unverified, and the convergence of page-level deficiencies with confirmed external threat findings prevents a defensible trust determination.

Infrastructure Integrity

CDN/WAF protection is present and is a mitigating infrastructure control only. The observed edge address was 138.68.170.39, and the origin server was not observable in this analysis; this configuration can reduce direct exposure but does not establish the legitimacy of the service or neutralize the external reputation risk.

EVIDENCE

- Network infrastructure: One observed edge IP, 138.68.170.39, associated with AS14061 and DigitalOcean, LLC.
- CDN/WAF posture: CDN/WAF protection was detected; no likely origin IP candidate was observed.
- Transport encryption: The site used a valid DV TLS certificate issued by YR1, expiring on 2026-10-29.

Closing Assessment

Prospective users should not submit credentials or financial information to the portal, and any required engagement should wait until the operator and service have been independently authenticated through authoritative channels.

Written analysis generated 2026-08-21 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

2 findings contributed to this verdict, raised by page content, analysis engine, external reputation.

01 Governance Risk

- The page presents a sign-in form, and the operator behind it could not be independently verified.
Page content rule:PAGE_TYPE_LOGIN_UNVERIFIED

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	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 guardtrack.co.uk.

- The request stayed on guardtrack.co.uk. It was not redirected to another domain. CLEAR
- The earliest public archive of this site is from 2018-01-07. CLEAR
- It is hosted on DIGITALOCEAN-ASN, from a server in US. NOTED

Domain intelligence

Registrar	Not available
Hosting	DIGITALOCEAN-ASN - DigitalOcean, LLC, US
Country	US
Server IP	138.68.170.39
Name servers	Not available
SSL issuer	YR1
SSL expiry	2026-10-29
Domain age	1.16 years (continuous registration)
Domain expiry	Not available
Archive first seen	2018-01-07
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 6 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about guardtrack.co.uk 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.