

Is windowsdiagnostics.st safe? TrustSniffer's low-trust assessment: 25/100

windowsdiagnostics.st

Verdict

25

OUT OF 100

LOW TRUST

windowsdiagnostics.st is low-trust and potentially risky.

Several risk patterns were present. Do not send money or personal details until you have verified this business another way.

Sensitive Interaction Risk

Governance Risk

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

What this site appears to be

A minimal 'Not Found' response with no links, forms, or substantive content. Likely a 404 page or missing resource.

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	3 flagged it VirusTotal	RISK
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	3% confidence AbuseIPDB, 4 reports; shared hosting inflates reports	CLEAR
Domain age	4 months old Most scam domains are under a year old	RISK
Web archive	Never archived No public history of this site	WATCH
Certificate	Encrypted connection Issued by YR1	NOTED

The page as captured

https://windowsdiagnostics.st/

Pretty-print ☐

```
{"detail": "Not Found"}
```

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

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: less than 1 year (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

Security Alert

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

The website at windowsdiagnostics.st currently presents only a minimal “Not Found” response, with no visible product, service, commercial activity, navigation, or substantive explanation of its purpose.

Scam/Impersonation Risk

The site presents a **high-risk interaction profile** because external security assessments recorded a confirmed blacklist status, including three malicious and two suspicious detections. These signals are materially stronger than the benign characteristics of the captured page and warrant treating the domain as potentially unsafe for sensitive activity. No conflicting legal-entity names or observed brand-impersonation indicators were identified, but the confirmed blacklist status remains a direct contradiction to a trustworthy posture.

EVIDENCE

- The homepage returned a 404-style “Not Found” response containing only a short error message, with no links, forms, or substantive content.
- External reputation checks recorded 3 malicious detections and 2 suspicious detections for the domain.
- The domain was recorded on 2 blacklist sources; the associated IP also had 4 abuse reports attributed to shared CDN infrastructure.

Regulatory Verification Notes

The captured site does not provide a usable business identity, legal information, licensing statement, or registration number. This is a significant verification gap rather than independent proof of fraud, but it prevents the operator, business purpose, and any regulatory status from being established from the website itself. The available evidence does not independently verify the real-world operator. The domain is registered through ST Registry and is very recently established, while its transport security is technically valid but uses domain validation only; neither characteristic establishes legitimacy.

EVIDENCE

- Domain registration: 2026, approximately 0.31 years old; registrar: ST Registry.
- The site's TLS certificate is issued by YR1, uses DV validation, and is valid to 2026-11-24.
- The captured site contains no visible company, licensing, or regulatory disclosure.

What to Verify Next

Before any sensitive interaction, an independent party should confirm the domain's operator through an authoritative corporate or regulatory registry and verify that any claimed service is authorised for the relevant jurisdiction. Official contact channels should be confirmed through an independent, offline route rather than relying solely on information presented by the domain. No credentials, payment details, or other sensitive information should be submitted unless those checks produce a consistent, independently corroborated identity.

EVIDENCE

- The captured homepage provides no company identity or service description from which authorisation could be assessed.
- No login form, payment form, wallet connection, or other sensitive interaction was observed during the available page and behaviour checks.
- The page's observed behaviour included no external requests or wallet activity across 2 successful runs, but this limited technical observation does not resolve the domain's external reputation findings.

Summary Verdict

The website has a low-trust posture with elevated risk for sensitive interaction. Its apparent legitimacy and operator identity are not independently established, and the confirmed external security contradictions outweigh the limited benign signals available from the sparse capture. The appropriate classification is sensitive-interaction risk rather than a trustworthy service endpoint.

Infrastructure Integrity

The site is protected by Cloudflare CDN/WAF infrastructure, with the observed edge route on AS57724 operated by DDOS-GUARD - DDOS-GUARD LTD in Russia. The edge protection is a mitigating security control that can reduce direct exposure of the underlying service, but it does not establish the legitimacy of the website or offset the external reputation concerns.

Closing Assessment

The domain should be treated as unsuitable for credentials, financial activity, or other sensitive interaction unless independent identity, authorisation, and channel checks are completed successfully.

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, 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
 - 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

Signals weighed against the site

- AbuseIPDB: 4 reports on hosting IP 185.178.208.163 (DDOS-GUARD LTD, Content Delivery Network), 3% confidence. The reports are attributed to shared infrastructure, not specifically to this website.

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 windowsdiagnostics.st.

- The request stayed on windowsdiagnostics.st. It was not redirected to another domain. CLEAR

- Registration is published under ST Registry. CLEAR
- DNS for this domain is served by cloudflare.com, across 2 name servers. NOTED
- The registration is paid up to 2027-05-31. NOTED
- It is hosted on DDOS-GUARD, from a server in RU. NOTED

Domain intelligence

Registrar	ST Registry
Hosting	DDOS-GUARD - DDOS-GUARD LTD, RU
Country	RU
Server IP	185.178.208.163
Name servers	dante.ns.cloudflare.com, vivienne.ns.cloudflare.com
SSL issuer	YR1
SSL expiry	2026-11-24
Domain age	0.31 years (continuous registration)
Domain expiry	2027-05-31
Archive first seen	Not available
Archive snapshots	0
Reputation	VirusTotal: 3 flagged AbuseIPDB: 3% confidence, 4 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about windowsdiagnostics.st 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.