

Is dialhost.com.br legit? TrustSniffer's high-trust assessment: 99/100

dialhost.com.br

Verdict

99

OUT OF 100

HIGH TRUST

dialhost.com.br appears legitimate.

Our checks found nothing pointing to fraud. Ordinary care still applies when you pay or sign in.

Not Scam

Low Risk

Assessed 2026-08-17 by automated analysis. Classification confidence 55%.

What this site appears to be

Corporate website for DialHost offering hosting plans (shared, cloud, ASP.NET), site builder, SSL certificates, email marketing and dedicated servers. Contains login forms for control panel and webmail and a newsletter signup; contact/address and company registration (CNPJ) are present.

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.

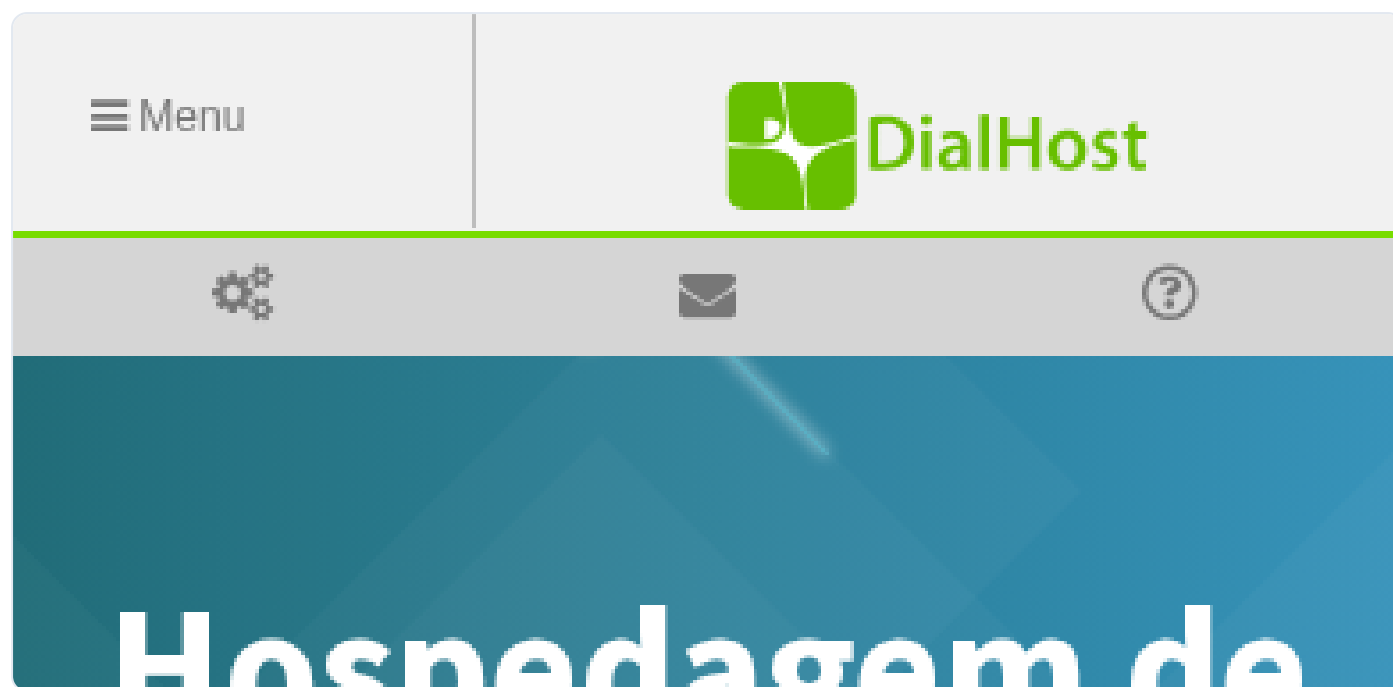
At a glance

The checks that decide most of this verdict.

Malware engines	None flagged it VirusTotal	CLEAR
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	0 reports AbuseIPDB; shared hosting inflates this count	NOTED
Domain age	24 years old Registered history	CLEAR
Web archive	Never archived No public history of this site	WATCH
Certificate	Encrypted connection Issued by Sectigo Public Server Authentication CA DV R36	NOTED

The page as captured

https://www.dialhost.com.br/



What dialhost.com.br served when TrustSniffer captured it on 2026-08-17. The page may look different now.

Key findings

- Automated classification: Not Scam.
- Domain age: more than 10 years (registration continuity).
- No flags from the reputation services TrustSniffer consulted at assessment time.

Full analysis

Overview

This is the DialHost corporate website, presenting commercial web-hosting and cloud services including shared hosting, ASP.NET hosting, dedicated servers, site creation, SSL certificates, email marketing, domain registration, and managed infrastructure for business and personal web projects.

Scam/Impersonation Risk

No contradictions were observed: there are no confirmed phishing, impersonation, malware, or blacklist indicators in the supplied evidence. The homepage contains ordinary control-panel and webmail login forms, but testing found no hidden forms, external password submissions, wallet-drainer behavior, cloaking, or suspicious scripts. The site's coherent hosting-service content, established social presence, and clean external reputation are consistent with an apparently legitimate established website rather than an impersonation operation.

EVIDENCE

- The homepage identifies DialHost as a hosting and cloud-services provider and exposes standard control-panel, webmail, and newsletter forms without an untrusted submission destination.
- Interactive testing recorded 0 hidden forms, 0 external password forms, 0 wallet-connect runs, 0 wallet-drainer runs, 0 clipboard-hijack events, and no cloaking.
- External reputation checks recorded 0 malicious detections, 0 suspicious detections, no Google Safe Browsing malicious finding, and no blacklist match; the site has a traffic rank of 40461 and is within the global top 1 million.

Regulatory Verification Notes

The website presents contact and address information together with a company registration identifier, which supports basic commercial disclosure. It does not claim or display a financial-services license or registration, but the stated hosting and infrastructure-services model does not itself imply financial regulation. Available evidence is consistent with an established, apparently legitimate business; however, the real-world operator identity remains likely rather than independently verified. No adverse broker-reputation match was identified.

EVIDENCE

- The site's corporate and contact content includes an address and company registration identifier.
- The domain was registered on 2002-07-18T15:56:40Z and is 24.1 years old, with registration expiration on 2033-07-18T15:56:40Z.
- The site is served from AS262448, identified as AS262448 - DIALHOST INTERNET EIRELI, BR.
- The TLS certificate uses DV validation, is issued by Sectigo Public Server Authentication CA DV R36, and is valid to 2026-11-26T23:59:59+00:00.

What to Verify Next

Before credential or payment interactions, independently match the corporate registration and contact details against the relevant business registry, review the applicable service, cancellation, and refund terms, and confirm that payment protections are available. Contact channels should be reached through the site's official navigation or an independently sourced business record rather than through an unsolicited message.

EVIDENCE

- The corporate and contact sections provide the registration and address details that should be independently matched.
- The service offering and recurring-subscription model make cancellation, renewal, refund, and billing terms material checks before purchase.
- The control-panel and webmail entry points should be reached through the official site navigation before any credentials are submitted.

Summary Verdict

The overall posture is high trust and low risk, with strong evidence consistent with an established, apparently legitimate website. No scam or impersonation contradictions were identified, although the operator's real-world

identity is not independently proven by the available evidence.

Infrastructure Integrity

The supplied infrastructure evidence does not confirm a trusted CDN or WAF layer, nor an origin-obscuring posture. This is a neutral infrastructure limitation rather than an indication of malicious activity; the site's identified hosting and valid TLS remain mitigating technical signals.

Closing Assessment

Routine evaluation of the service is proportionate, while ordinary independent merchant-identity, service-term, and payment-protection checks should precede credential submission or payment.

Written analysis generated 2026-08-17 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

No rule findings contributed to this verdict.

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 dialhost.com.br.

- The request stayed on dialhost.com.br. It was not redirected to another domain. CLEAR
- DNS for this domain is served by com.br, across 4 name servers. NOTED
- The registration is paid up to 2033-07-18. CLEAR
- It is hosted on AS262448, from a server in BR. NOTED

Domain intelligence

Registrar	Not available
Hosting	AS262448 - DIALHOST INTERNET EIRELI, BR
Country	BR
Server IP	177.52.162.89
Name servers	ns1.dialhost.com.br, ns2.dialhost.com.br, ns3.dialhost.com.br, ns4.dialhost.com.br
SSL issuer	Sectigo Public Server Authentication CA DV R36
SSL expiry	2026-11-26

Domain age	24.10 years (continuous registration)
Domain expiry	2033-07-18
Archive first seen	Not available
Archive snapshots	0
Reputation	VirusTotal: 0 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about dialhost.com.br 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/dialhost.com.br> · assessed 2026-08-17