

Is d-a-g.ru a scam? TrustSniffer's high-risk assessment: 0/100

d-a-g.ru

Verdict

0

OUT OF 100

CRITICAL RISK

d-a-g.ru 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 2026-08-20 by automated analysis. Classification confidence 50%.

What this site appears to be

phpMyAdmin login page showing a username/password prompt, language selector and an HTTPS mismatch warning. No marketing, contact or explanatory content 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.

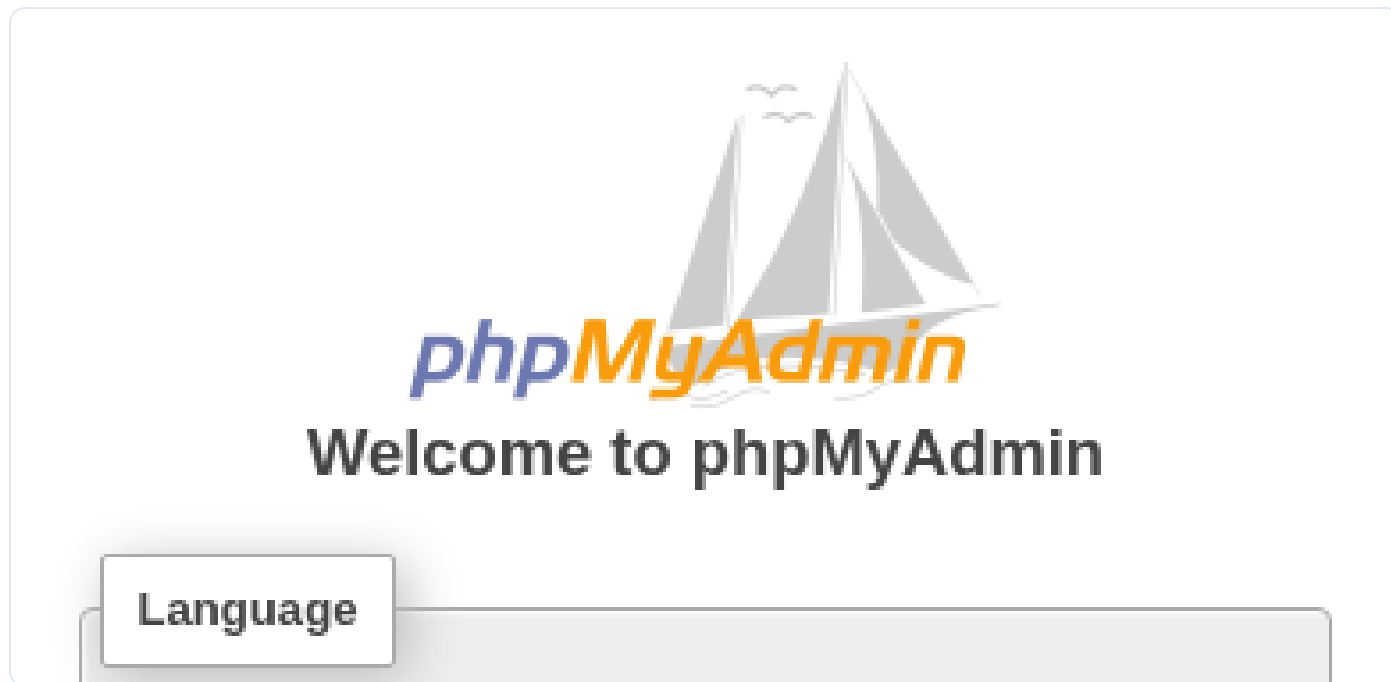
At a glance

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	2.9 years old Registered history	CLEAR
Web archive	Archived since 2013 Public history exists	CLEAR
Certificate	Encrypted connection Issued by WE1	NOTED

The page as captured

https://d-a-g.ru/



What d-a-g.ru served when TrustSniffer captured it on 2026-08-20. 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 2013.
- No flags from the reputation services TrustSniffer consulted at assessment time.

Full analysis

Overview

The website is a phpMyAdmin database-administration interface that presents a username-and-password login, language selection, and a server HTTPS-configuration warning, but provides no explanatory, commercial, contact, or organizational context. Its apparent purpose is to provide access to a web-based database management console rather than a public-facing business service.

Scam/Impersonation Risk

No confirmed blacklist, phishing, or identity contradiction was observed. The principal concern is **sensitive-interaction risk**: the only substantive page is an administrative login that requests credentials without explaining who operates the console, why access is required, or how the host relates to an expected organization. An automated brand-similarity signal associated the page with “g.page,” but the direct page assessment did not identify a suspected brand impersonation, so this remains an uncorroborated indicator rather than a confirmed impersonation finding. The page also warns of an HTTPS mismatch between the server and client configuration, which increases the importance of treating the login prompt as untrusted until the host is independently confirmed.

EVIDENCE

- The homepage is titled “phpMyAdmin” and contains one login form requesting a username and password, with no surrounding business or operator explanation.
- The homepage displays a warning that HTTPS is mismatched between the server and client and that the condition may create a security risk.
- The page-level assessment records the red flag “LOGIN_PAGE_ONLY_NO_CONTEXT” and classifies the page as “Login-only / Unknown.”
- The domain was registered on 2023-09-22 and is approximately 2.91 years old; the available archive record spans 2013-04-04 to 2025-08-10 across 13 years.

Regulatory Verification Notes

The available content does not expose legal, ownership, licensing, or governance information, and there is no public-facing service description against which a regulatory authorization could be assessed. This is a material verification gap for any organization considering the host as an operational access point, although it is not, by itself, evidence of a scam. The domain is registered through DOMAINSHOP-RU, while the transport certificate is domain-validated rather than an organizational identity certificate. External reputation checks did not record blacklist or abuse reports, but coverage was partial and does not resolve the site’s unverified operator identity.

EVIDENCE

- The homepage contains no company name, legal notice, terms page, contact information, license number, or regulatory disclosure; it consists of the phpMyAdmin console.
- Domain registration data identifies DOMAINSHOP-RU as registrar, with creation date 2023-09-22T16:11:43Z and expiry date 2026-09-22T16:11:43Z.
- The site is served through AS13335, identified as CLOUDFLARENET - Cloudflare, Inc., US.
- The TLS certificate uses issuer WE1, has DV validation, and is valid to 2026-11-08T00:28:32+00:00.

What to Verify Next

The intended owner of the database console should confirm the hostname through an independent, pre-existing administrative channel rather than through the page itself. The certificate and HTTPS configuration should be checked after the host is confirmed, with the server-side and client-side scheme configuration corrected before any authentication attempt. Credentials should not be entered unless the host is positively mapped to an authorized environment; any access request should be validated with the relevant system owner or security team.

EVIDENCE

- The homepage presents a single sensitive login form with no external or internal explanatory links.
- The page explicitly reports an HTTPS mismatch and identifies it as a possible security risk.
- Behavioral testing recorded no hidden forms, no external password form destination, and no wallet or clipboard-hijacking activity; these observations do not establish operator legitimacy.
- The page returned successfully during two recorded test runs, but stable delivery does not validate the purpose or authorization of the login endpoint.

Summary Verdict

The site has a **critical trust posture** for sensitive interaction because its operator identity and governance context are unverified and its public presentation is limited to an unexplained administrative credential prompt. No confirmed contradiction or blacklist finding was observed, but the available evidence is insufficient to support normal login, credential submission, or financial use.

Infrastructure Integrity

The site is protected by Cloudflare CDN/WAF infrastructure and resolves through Cloudflare edge addresses, including 104.21.45.185 and 172.67.218.65 on AS13335. This provides a mitigating layer against direct exposure and can improve delivery resilience, but it does not establish that the underlying database console is authorized or legitimately operated.

Closing Assessment

Treat the endpoint as an unverified administrative access surface and use it only after independent confirmation of ownership, purpose, and authorization; absent that confirmation, sensitive interaction should not proceed.

Written analysis generated 2026-08-20 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, registration and ownership, analysis engine.

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
- 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
- The page asks visitors for sensitive information.
Page content rule:PAGE_FORM_SENSITIVE
- The page presents itself as a brand TrustSniffer confirmed it does not belong to.
Page content rule:PAGE_BRAND_IMPERSONATION_CONFIRMED

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 d-a-g.ru.

- The request stayed on d-a-g.ru. It was not redirected to another domain. CLEAR
- Registration is published under DOMAINSHOP-RU. CLEAR
- DNS for this domain is served by com., across 2 name servers. NOTED
- The registration is paid up to 2026-09-22. NOTED
- The earliest public archive of this site is from 2013-04-04. CLEAR
- It is hosted on CLOUDFLARENET, from a server in US. NOTED

Domain intelligence

Registrar	DOMAINSHOP-RU
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US
Server IP	2606:4700:3036::ac43:da41
Name servers	apollo.ns.cloudflare.com., fay.ns.cloudflare.com.
SSL issuer	WE1
SSL expiry	2026-11-08
Domain age	2.91 years (continuous registration)
Domain expiry	2026-09-22
Archive first seen	2013-04-04
Archive snapshots	Not counted (archive lookup incomplete)
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 d-a-g.ru 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.