

Is **douvagroup.com** a scam? TrustSniffer's high-risk assessment: **0/100**

douvagroup.com

Verdict

0

OUT OF 100

CRITICAL RISK

douvagroup.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 2026-08-20 by automated analysis. Classification confidence 55%.

What this site appears to be

Default landing page for an Indonesian hosting provider (IDwebhost). Contains onboarding text advising user to customize site, brief steps for making a website, promotional mentions for free domain and hosting promo, and a contact phone number. No forms or explicit calls to submit sensitive credentials visible.

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.

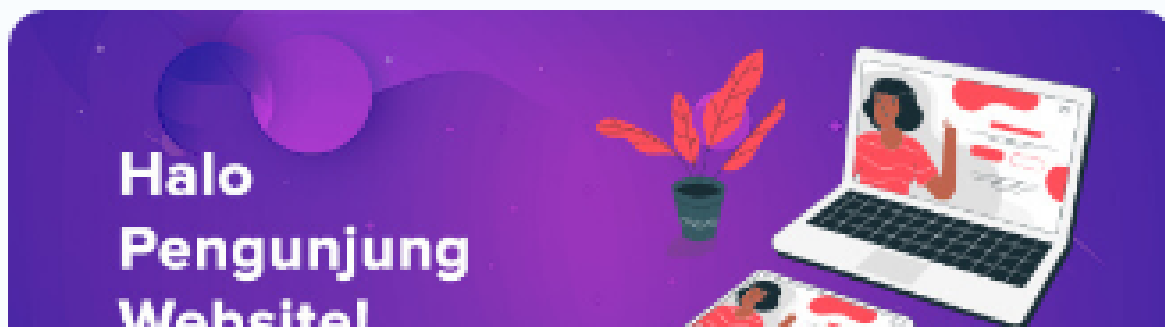
At a glance

The checks that decide most of this verdict.

Malware engines	7 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	13 years old Registered history	CLEAR
Web archive	Archived since 2013 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YR1	NOTED

The page as captured

<https://douvagroup.com/>



What douvagroup.com served when TrustSniffer captured it on 2026-08-20. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: more than 10 years (registration continuity).
- Public web-archive history exists since 2013.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

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

This website is a default Indonesian hosting-provider landing page branded IDwebhost, presenting account activation text, basic website-building guidance, domain and hosting promotions, and a telephone contact channel; its apparent business model is the sale of hosting, domain-registration, and related services.

Scam/Impersonation Risk

The site has a **critical sensitive-interaction risk posture** because independent external reputation checks recorded malicious detections and a confirmed blacklist listing. This is materially more significant than the benign appearance of the homepage: the page shows no login form, credential-harvesting form, wallet connection, or explicit sensitive-data request, and no brand impersonation or conflicting legal-entity identity was observed, but those content-level observations do not offset the external threat findings. The website's apparent age and historical presence establish continuity of the domain, not the safety of current interaction or the legitimacy of the present content.

EVIDENCE

- External reputation checks recorded 7 malicious detections among 12 effective detections and a confirmed blacklist listing.
- The domain registration record shows creation on 2013-06-30T17:25:44Z and an age of 13.15 years.
- Historical records show 71 snapshots spanning 2013–2025, covering 13 years of tracked presence.

Regulatory Verification Notes

The registration record identifies PT Douva Afalla International and lists GKG.Net, Inc. as registrar, while the homepage presents itself as an IDwebhost hosting service. The available identity connection remains unverified, and the landing page is a generic activation or placeholder page rather than a developed corporate or service disclosure page. No licensing claim, licensing authority, or license number is presented in the supplied site content; this is a verification gap, not by itself proof of misconduct. The domain's transport security is present, but domain-validated encryption confirms an encrypted connection rather than the operator's legal identity or regulatory standing. The available broker-intelligence dataset contains no match.

EVIDENCE

- The homepage title and body identify "IDwebhost" and promote hosting and domain services, while the registration record names PT Douva Afalla International.
- The domain is registered through GKG.Net, Inc.; its registration expires on 2027-06-30T17:25:44Z.
- The site is served on AS45324 by GMEDIA-AS-ID - Global Media Teknologi, PT, ID.
- TLS is issued by YR1 at DV validation level and is valid to 2026-10-11T00:00:37+00:00.

What to Verify Next

Before any sensitive interaction, an organization should independently confirm that the intended service operator is the same entity named in the registration record and that the IDwebhost branding is authorized for this domain. Any claimed hosting or domain-registration service should be validated through an independently sourced official support channel, and any applicable licensing or business-registration status should be checked with the relevant Indonesian registry or authority. Credentials, payment details, and other sensitive information should not be submitted until those checks and the external reputation concern have been resolved.

EVIDENCE

- The homepage is identified as a hosting-placeholder or welcome page and contains no login or sensitive-data form.
- The homepage offers hosting and domain promotions but does not provide a license authority or license number.
- Behavioral testing recorded 35 external XHR requests, 26 external POST requests, and 9 non-whitelisted external requests across two successful runs.

Summary Verdict

The website should be treated as an **established-domain but currently untrusted service endpoint**. The decisive external reputation contradictions outweigh the otherwise ordinary hosting-page presentation and

historical continuity, making sensitive interaction inappropriate absent independent validation and remediation of the reputation findings.

Infrastructure Integrity

The site resolves directly to a single likely origin address rather than operating behind a detected CDN or WAF, with no edge-IP layer identified. This provides limited infrastructure-based mitigation: the transport is encrypted, but the hosting arrangement itself does not establish legitimacy or reduce the significance of the external threat detections.

Closing Assessment

The proportionate course is to limit activity to non-sensitive observation and defer login, credential submission, payment, or other financial interaction until independent operator validation and security clearance are complete.

Written analysis generated 2026-08-20 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, behaviour in a sandbox, 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
- The page made background requests to destinations TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_XHR
- The page sent data to a destination TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_POSTS
- The page exchanged network traffic with destinations TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_TRAFFIC
- Most of what the page loaded came from other domains rather than from this one.
Behaviour in a sandbox rule:BEHAV_EXTERNAL_RATIO_HIGH
- 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 [douvagroup.com](#).

- The request stayed on [douvagroup.com](#). It was not redirected to another domain. CLEAR
- Registration is published under GKG.Net, Inc.. CLEAR
- DNS for this domain is served by [idwebhost.com](#), across 2 name servers. NOTED
- The registration is paid up to 2027-06-30. NOTED
- The earliest public archive of this site is from 2013-12-21. CLEAR
- It is hosted on GMEDIA-AS-ID, from a server in ID. NOTED

Domain intelligence

Registrar	GKG.Net, Inc.
Hosting	GMEDIA-AS-ID - Global Media Teknologi, PT, ID
Country	ID
Server IP	202.52.146.249
Name servers	NS1.IDWEBHOST.COM, NS2.IDWEBHOST.COM
SSL issuer	YR1
SSL expiry	2026-10-11
Domain age	13.15 years (continuous registration)
Domain expiry	2027-06-30
Archive first seen	2013-12-21
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 7 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about [douvagroup.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.