

Is 246bdb.org a scam? TrustSniffer's high-risk assessment: 0/100

246bdb.org

Verdict

0

OUT OF 100

CRITICAL RISK

246bdb.org 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 2026-08-18 by automated analysis. Classification confidence 70%.

What this site appears to be

Page is an automated browser/JavaScript check ("Checking your browser... Javascript required"). No service content, forms, or monetization 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.

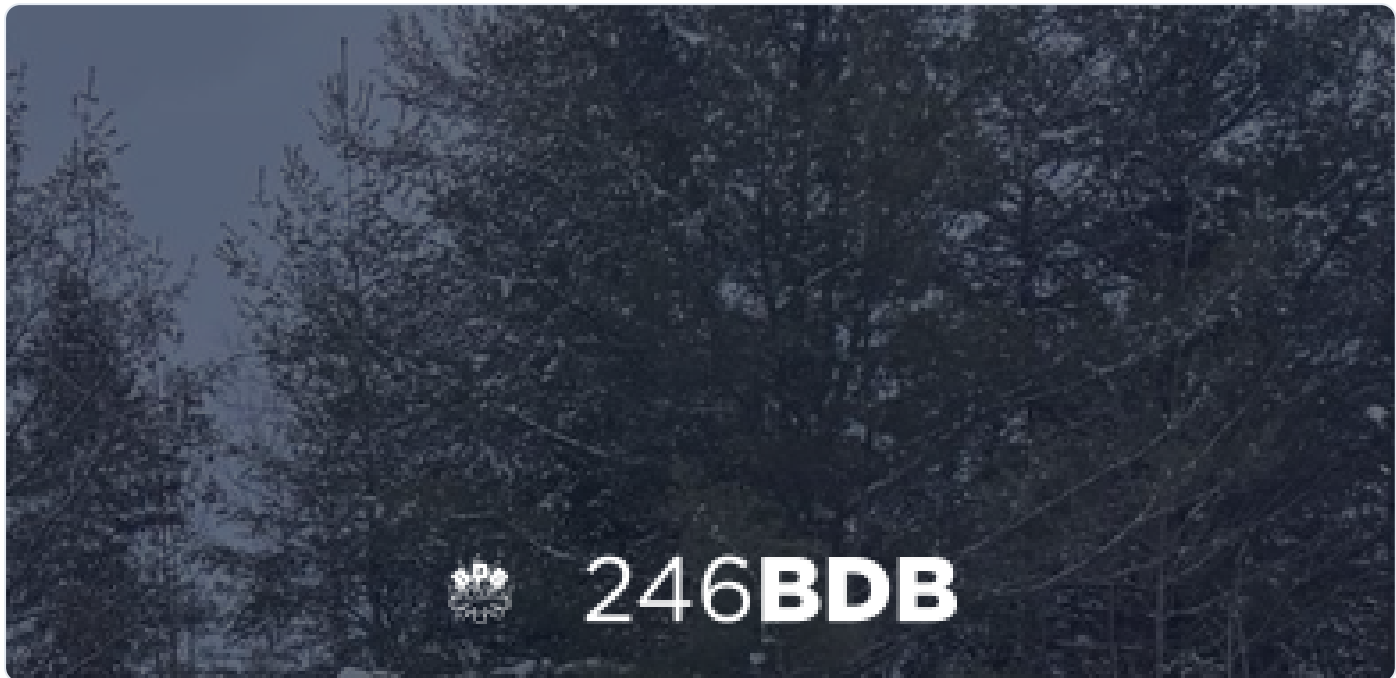
At a glance

The checks that decide most of this verdict.

Malware engines	11 flagged it VirusTotal	RISK
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	2% confidence AbuseIPDB, 2 reports; shared hosting inflates reports	CLEAR
Domain age	25 years old Registered history	CLEAR
Web archive	Archived since 2002 45 snapshots	CLEAR
Certificate	Encrypted connection Issued by WR1	NOTED

The page as captured

<https://246bdb.org/>



What 246bdb.org served when TrustSniffer captured it on 2026-08-18. 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 2002.
- 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.

The website at 246bdb.org currently presents an automated browser-verification checkpoint stating that JavaScript is required and that the check will take a few seconds. No service description, commercial offering, account flow, or other business purpose is visible to a visitor, so the site's intended operator and operating model cannot be established from the accessible page.

Scam/Impersonation Risk

Confirmed external reputation contradictions create a critical sensitive-interaction risk. The domain is blacklisted by two external sources, with 11 malicious detections and one additional suspicious detection recorded in the supplied reputation evidence; one tier-one security provider also identified a threat. These findings outweigh the otherwise neutral page presentation. The separate abuse reports concern an IP attributed to Automattic's shared infrastructure, so they are not by themselves proof that this specific domain generated the activity, but they remain an adverse environmental signal. The page-level capture did not show a login form, credential form, financial workflow, phishing indicators, or brand-impersonation content; accordingly, the

evidence confirms a serious reputation problem rather than proving a specific credential-theft mechanism on the captured page.

EVIDENCE

- The homepage returned an anti-bot checkpoint with the text “Checking your browser... Javascript required” and no visible service content.
- External reputation evidence recorded 11 malicious detections and 1 suspicious detection for the domain, with a confirmed blacklist status.
- Two abuse reports were associated with IP address 192.0.78.25, attributed to Automattic, Inc. shared infrastructure with usage classified as a Content Delivery Network.
- The domain was registered on 2001-07-18T13:58:04Z and is approximately 25.1 years old; archival records contain 45 snapshots spanning 2002-11-19T15:48:08Z through 2025-04-01T10:53:08Z, covering 24 tracked years.

Regulatory Verification Notes

The accessible site does not provide a usable legal, corporate, or licensing disclosure, and the real-world operator identity remains unverified. This is a material transparency gap for any site that may later introduce onboarding, account access, payments, or other regulated activity; it is not, by itself, proof of fraud, but it prevents independent attribution of the service to a responsible entity. The domain is administered through Automattic Inc., while the transport certificate is domain-validated rather than organization-validated. No matching broker entry was identified in the supplied third-party context, which provides limited contextual reassurance but is not a licensing or regulatory determination.

EVIDENCE

- The captured homepage exposed no company name, license authority, registration number, terms, privacy disclosure, or service description.
- The domain registrar is Automattic Inc.; the domain creation date is 2001-07-18T13:58:04Z and the recorded expiration date is 2027-07-18T13:58:04Z.
- The site is served from AS2635 (AUTOMATTIC - Automattic, Inc, US).
- The TLS certificate was issued by WR1 at DV validation level and is valid through 2026-11-02T05:51:24+00:00.

What to Verify Next

Before any sensitive interaction, an independent security or compliance process should confirm the operator’s legal identity and any claimed authorization through authoritative corporate and regulatory registries, rather than relying on information presented by the site. The checkpoint and its scripts should also be reviewed in an isolated environment to confirm the final destination and all network requests before permitting access from an enterprise workstation.

EVIDENCE

- The browser interaction generated 11 external XHR requests, including 7 non-whitelisted XHR requests.
- Three external POST requests were observed, including 1 non-whitelisted POST request.
- One suspicious inline script was detected, and interaction produced a maximum DOM difference of 2,403 elements.
- No sensitive form, password-external form, wallet connection, wallet provider, or clipboard-write activity was detected during the two successful runs.

Summary Verdict

The overall posture is **critical and unsuitable for sensitive interaction**. The available evidence does not establish a trustworthy operating identity, and the combination of confirmed external malicious detections, blacklist status, and access-gated presentation supports a clear decision to treat the site as untrusted for credentials, account access, or financial activity.

Infrastructure Integrity

The site resolves through Automattic-hosted infrastructure without a detected protective CDN or WAF, and two likely origin addresses were identified. This provides no meaningful infrastructure-based mitigation against the reputation findings; the observed “fast-flux-like” DNS heuristic is treated only as an unconfirmed technical indicator, not as a standalone finding.

Closing Assessment

Enterprise controls should block or isolate the domain, prevent credential and payment interaction, and require independent identity and regulatory confirmation before any future engagement is considered.

Written analysis generated 2026-08-18 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, behaviour in a sandbox.

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
- The page exchanged network traffic with destinations TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_TRAFFIC
- The page carried inline scripts written in a style TrustSniffer treats as suspicious.
Behaviour in a sandbox rule:BEHAV_SUSPICIOUS_INLINE_SCRIPTS
- The page rewrote itself after it was interacted with, so what a visitor first sees is not what they end up on.
Behaviour in a sandbox rule:BEHAV_DOM_DIFF_AFTER_INTERACTION
- Most of what the page loaded came from other domains rather than from this one.
Behaviour in a sandbox rule:BEHAV_EXTERNAL_RATIO_HIGH
- The structure of the page changed sharply while it was loading.
Behaviour in a sandbox rule:BEHAV_DOM_DENSITY_SPIKE
- The page sent data to a destination TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_POSTS
- The page made background requests to destinations TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_XHR

Signals weighed against the site

- AbuseIPDB: 2 reports on hosting IP 192.0.78.25 (Automattic, Inc, Content Delivery Network), 2% 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 246bdb.org.

- The request stayed on 246bdb.org. It was not redirected to another domain. [CLEAR](#)
- Registration is published under Automattic Inc.. [CLEAR](#)
- DNS for this domain is served by wordpress.com, across 3 name servers. [NOTED](#)
- The registration is paid up to 2027-07-18. [NOTED](#)
- The earliest public archive of this site is from 2002-11-19. [CLEAR](#)
- It is hosted on AUTOMATTIC, from a server in US. [NOTED](#)

Domain intelligence

Registrar	Automattic Inc.
Hosting	AUTOMATTIC - Automattic, Inc, US
Country	US
Server IP	192.0.78.25
Name servers	ns1.wordpress.com, ns2.wordpress.com, ns3.wordpress.com
SSL issuer	WR1
SSL expiry	2026-11-02
Domain age	25.10 years (continuous registration)
Domain expiry	2027-07-18
Archive first seen	2002-11-19
Archive snapshots	45
Reputation	VirusTotal: 11 flagged AbuseIPDB: 2% confidence, 2 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about 246bdb.org 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/246bdb.org> · assessed 2026-08-18