

Is pub-309aaffb1a3643d58aaa9c444941fef3.r2.dev safe? TrustSniffer's low-trust assessment: 40/100

pub-309aaffb1a3643d58aaa9c444941fef3.r2.dev

Verdict

40

OUT OF 100

LOW TRUST

pub-309aaffb1a3643d58aaa9c444941fef3.r2.dev 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 2026-09-24 by automated analysis. Classification confidence 55%.

What this site appears to be

A 404 Not Found page for an object storage/bucket indicating the object is not publicly accessible. No forms, monetization, or active malicious behavior detected.

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.

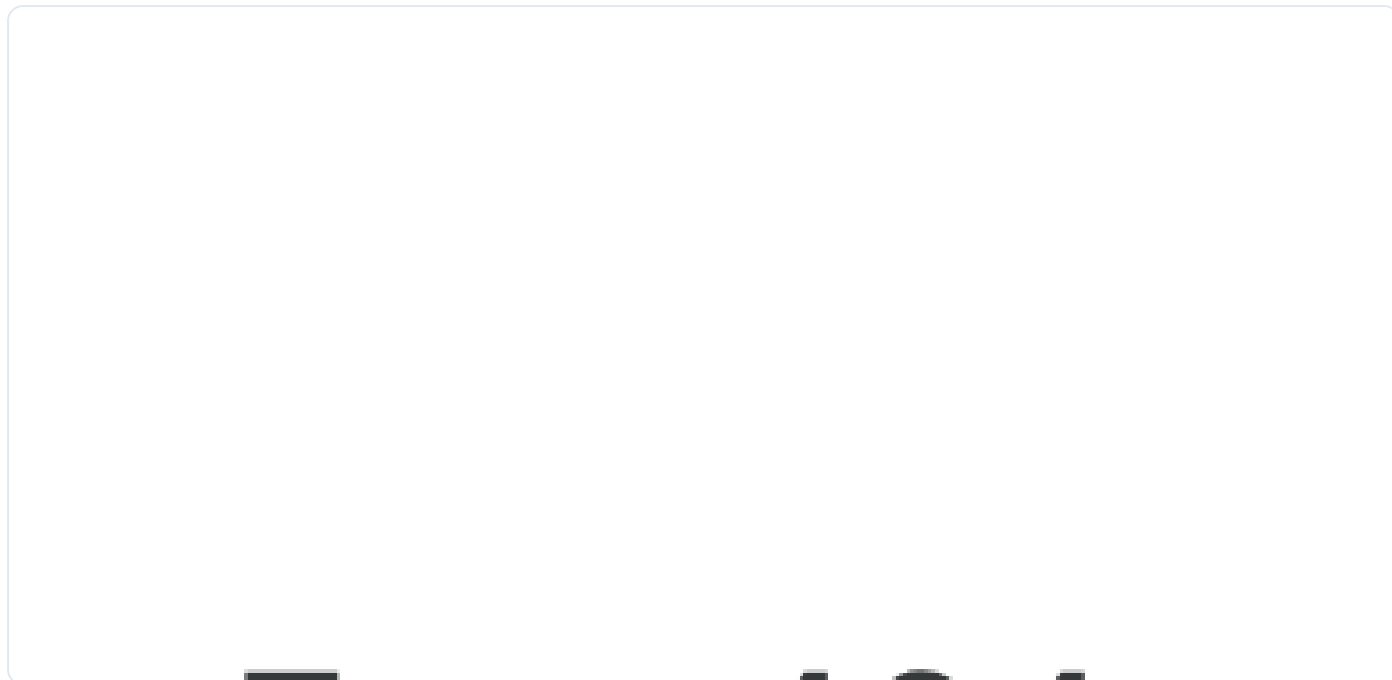
At a glance

The checks that decide most of this verdict.

Malware engines	2 flagged it VirusTotal	RISK
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	0% confidence AbuseIPDB, 1 report; shared hosting inflates reports	CLEAR
Domain age	Not available No registration record was returned	NOTED
Web archive	Never archived No public history of this site	WATCH
Certificate	Encrypted connection Issued by YE1	NOTED

The page as captured

<https://pub-309aaffb1a3643d58aaa9c444941fef3.r2.dev/>



What pub-309aaffb1a3643d58aaa9c444941fef3.r2.dev served when TrustSniffer captured it on 2026-09-24. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- 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

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

What is presented is an object-storage endpoint returning a “404 Not Found” placeholder rather than an identifiable business website. The page states that the requested object does not exist or is not publicly accessible, provides no commercial offering, and does not establish a clear operator or business purpose.

Scam/Impersonation Risk

Contradictory risk signals are present. External reputation checks identified malicious detections and a confirmed blacklist, which materially outweighs the otherwise neutral 404 content. The supplied page does not show brand impersonation, phishing forms, or conflicting legal identities; however, the blacklist status remains a direct reason for treating sensitive interaction as unsafe. A separate report associated with a shared content-delivery IP was explicitly discounted because the address is whitelisted shared infrastructure and carried zero confidence as a site-specific attribution.

EVIDENCE

- The homepage returns a 404 object-storage page stating “Object not found” and that the object may not be publicly accessible.
- External reputation analysis recorded 2 malicious detections and 1 suspicious detection, with the site present on an external blacklist.
- The single IP abuse report concerned shared CDN infrastructure, was whitelisted, and had a confidence score of 0; it is not treated as proof of site-specific abuse.

Regulatory Verification Notes

The observed site does not provide an identifiable operator, legal-entity information, licensing statement, or regulatory registration details, leaving its real-world identity unverified and its disclosure position unclear. Because the captured page is only an object-storage error page, this is a transparency and verification gap rather than, by itself, proof of fraud. No matching third-party broker record was returned. The transport layer provides technical encryption, but a domain-validated certificate confirms control of the web endpoint, not the legitimacy of the operator.

EVIDENCE

- The observed page contains no company name, legal notice, licensing claim, registration number, or regulatory disclosure.
- The site is served through Cloudflare’s CDN infrastructure on AS13335 (CLOUDFLARENET - Cloudflare, Inc., US).
- TLS is issued by YE1 at DV validation level and is valid to 2026-12-06.
- No matching third-party broker record was identified.

What to Verify Next

Before any sensitive interaction, an independent registry or authoritative corporate source should be used to establish who operates the endpoint and whether that operator is authorised for any activity associated with the domain. Any proposed login, payment, or other high-impact workflow should be reached only through independently confirmed official channels, with the endpoint’s blacklist status and malicious detections resolved first.

EVIDENCE

- The captured page contains no login form, password field, payment form, or other sensitive-input mechanism.
- The page contains no commercial offering from which a licence or financial-service authorisation could be assessed.
- Browser analysis recorded no wallet connection, wallet-sensitive activity, clipboard hijacking, hidden form, or external password form.

Summary Verdict

The site warrants a low-trust and high-risk posture for sensitive interaction. Its operator identity is unverified, and the available evidence does not support treating the endpoint as appropriate for credentials, account access, or financial activity.

Infrastructure Integrity

Cloudflare CDN/WAF protection provides a mitigating layer against direct exposure of the hosting environment, but all observed addresses were CDN edge servers and the origin server was not observable. This infrastructure arrangement is a protective delivery characteristic, not evidence that the underlying site or operator is legitimate.

Closing Assessment

Interaction should remain limited to non-sensitive observation until the operator’s identity and the external security findings have been independently resolved.

Written analysis generated 2026-09-24 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.

- 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

Signals weighed against the site

- AbuseIPDB: 1 report on hosting IP 2606:4700:311b::6812:3222 (Cloudflare, Inc., Content Delivery Network), 0% 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 pub-309aaffb1a3643d58aaa9c444941fef3.r2.dev.

- The request stayed on pub-309aaffb1a3643d58aaa9c444941fef3.r2.dev. It was not redirected to another domain. CLEAR
- It is hosted on CLOUDFLARENET, from a server in US. NOTED

Domain intelligence

Registrar	Not available
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US
Server IP	2606:4700:311b::6812:3222
Name servers	Not available
SSL issuer	YE1
SSL expiry	2026-12-06
Domain age	Not available (no registration date was returned)
Domain expiry	Not available
Archive first seen	Not available
Archive snapshots	0
Reputation	VirusTotal: 2 flagged AbuseIPDB: 0% confidence, 1 report Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about pub-309aaffb1a3643d58aaa9c444941fef3.r2.dev 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/pub-309aaffb1a3643d58aaa9c444941fef3.r2.dev> · assessed 2026-09-24