

Is pub-0216fa08b2b94e129cb9e002cf7cb1f4.r2.dev a scam?

TrustSniffer's high-risk assessment: 5/100

pub-0216fa08b2b94e129cb9e002cf7cb1f4.r2.dev

Verdict

5

OUT OF 100

CRITICAL RISK

pub-0216fa08b2b94e129cb9e002cf7cb1f4.r2.dev 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 2026-09-24 by automated analysis. Classification confidence 55%.

What this site appears to be

A 404-style object storage/bucket page indicating the requested object is missing or not publicly accessible. No forms, calls to action, payments, or credential requests 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.

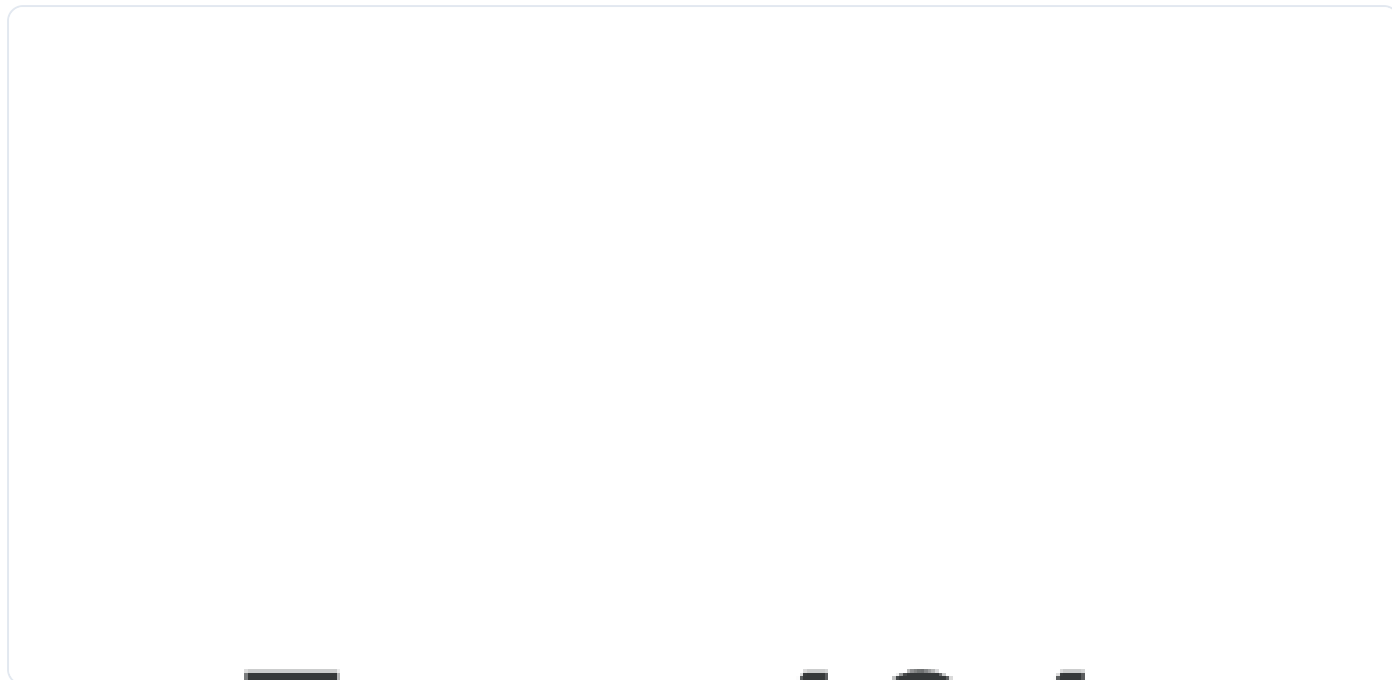
At a glance

The checks that decide most of this verdict.

Malware engines	12 flagged it VirusTotal	RISK
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	0% confidence AbuseIPDB, 2 reports; 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-0216fa08b2b94e129cb9e002cf7cb1f4.r2.dev/>



What pub-0216fa08b2b94e129cb9e002cf7cb1f4.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

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

This website currently presents a 404-style object-storage bucket page stating that the requested object was not found or is not publicly accessible. It shows no apparent commercial service, transaction flow, credential request, or other active business model, and appears intended only to report an unavailable or restricted object.

Scam/Impersonation Risk

The site presents a **critical sensitive-interaction risk** despite the absence of overt scam content on the accessible page. External reputation evidence records a confirmed blacklist and multiple malicious detections, which are material contradictions that outweigh the page's otherwise neutral 404 presentation. No brand impersonation, conflicting legal identities, or active phishing form was identified in the supplied page evidence; however, the available evidence is insufficient to treat the site as benign. The two abuse reports associated with shared delivery infrastructure are not treated as direct attribution to this site, but they do not offset the separate blacklist and malicious-detection findings.

EVIDENCE

- The homepage returns a “Not Found / Error 404 / Object not found” message and provides no commercial, payment, login, or credential function.
- External reputation telemetry records 12 malicious detections and 1 suspicious detection.
- The site is recorded as blacklisted by external reputation sources.
- The accessible page has no detected login form, hidden form, wallet connection, or credential-submission mechanism.

Regulatory Verification Notes

The accessible page does not identify an operating company, regulated entity, license, registration number, or governing jurisdiction. This is a transparency gap rather than proof of fraud, but it prevents meaningful regulatory validation and leaves the real-world operator identity unverified. The site’s transport and hosting controls provide technical protection, not evidence of legal standing or ownership. No matching broker-reputation record was identified in the supplied third-party context.

EVIDENCE

- The accessible homepage contains only an object-storage error message and does not provide operator, licensing, or registration disclosures.
- The site is served through AS13335, Cloudflare, Inc., United States.
- The TLS certificate is issued by YE1 at DV validation level and is valid to 2026-12-06T05:31:56+00:00.
- The accessible page contains no legal, terms, regulatory, or corporate-identity links.

What to Verify Next

Before any sensitive interaction, an independent party should identify the operator through an authoritative corporate or regulatory registry and confirm that any claimed service is authorized in the relevant jurisdiction. Official contact channels should be validated through an independently sourced route rather than relying solely on information presented by the site. Until those checks succeed, credentials, account access, payments, and other financial interactions should not be undertaken.

EVIDENCE

- The available page provides no operator name or licensing reference against which a registry check can be performed.
- The available page provides no independent legal, regulatory, or support-channel reference for corroboration.
- The site’s observed content is an unavailable object rather than a functioning service, so the intended business purpose cannot be independently confirmed from the page.

Summary Verdict

The overall posture is critically untrusted for sensitive interaction. The combination of confirmed external reputation conflict, unverified identity, and absent operating disclosures does not support treating the site as a legitimate service endpoint.

Infrastructure Integrity

Cloudflare CDN/WAF protection is present, and all observed addresses were CDN edge infrastructure with no origin candidate identified. This reduces direct exposure of the origin and can mitigate some hosting-level abuse, but it is only a protective infrastructure characteristic and does not establish legitimacy or neutralize the external threat findings.

Closing Assessment

The appropriate disposition is to restrict activity to passive observation and require independent identity, authorization, and channel validation before considering any account, credential, payment, or financial action.

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: 2 reports on hosting IP 2606:4700:311b::6812:362d (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-0216fa08b2b94e129cb9e002cf7cb1f4.r2.dev.

- The request stayed on pub-0216fa08b2b94e129cb9e002cf7cb1f4.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::6812:362d
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: 12 flagged AbuseIPDB: 0% confidence, 2 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about pub-0216fa08b2b94e129cb9e002cf7cb1f4.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-0216fa08b2b94e129cb9e002cf7cb1f4.r2.dev> · assessed 2026-09-24