

Is pub-364c6b3011ca492cab2354176cfaf3f0.r2.dev a scam?

TrustSniffer's high-risk assessment: 5/100

pub-364c6b3011ca492cab2354176cfaf3f0.r2.dev

Verdict

5

OUT OF 100

CRITICAL RISK

pub-364c6b3011ca492cab2354176cfaf3f0.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 2026-09-22 by automated analysis. Classification confidence 55%.

What this site appears to be

The page is a standard 404/object-not-found response indicating the requested object is not publicly accessible. No forms, links, or monetization elements 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.

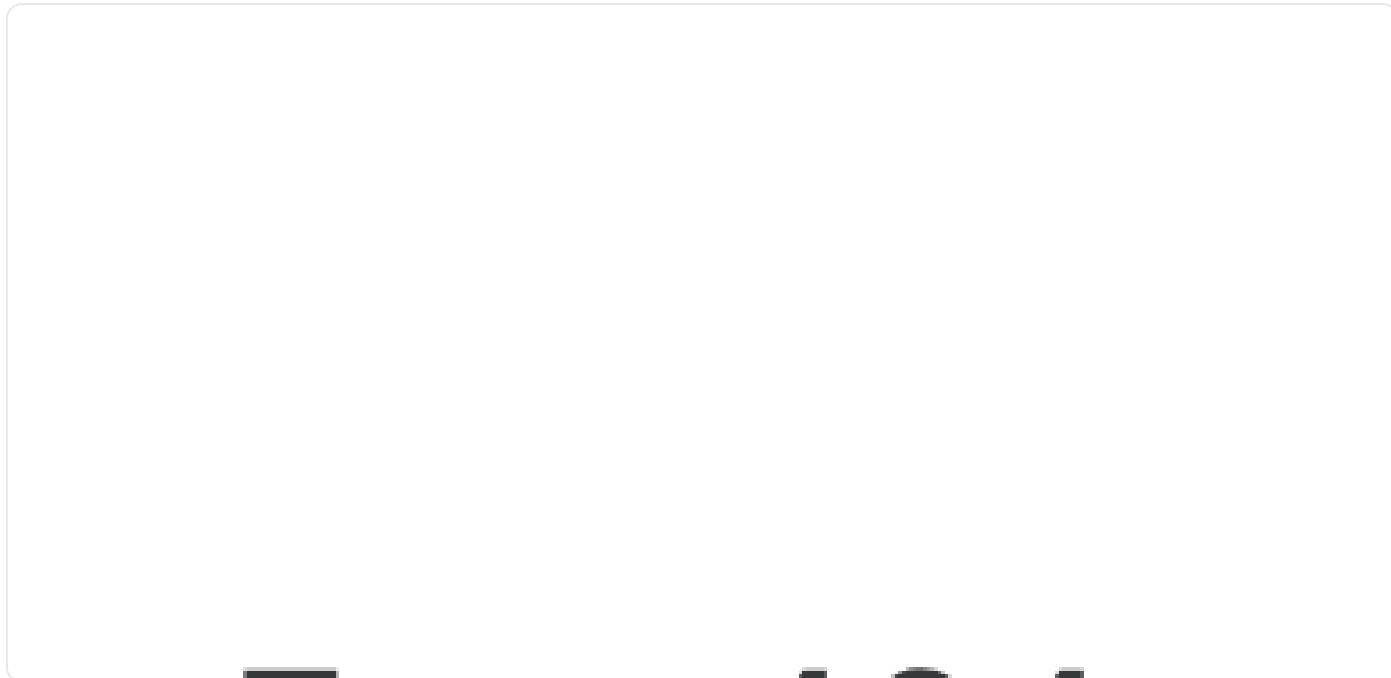
At a glance

The checks that decide most of this verdict.

Malware engines	15 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	2 months old Most scam domains are under a year old	RISK
Web archive	Never archived No public history of this site	WATCH
Certificate	Encrypted connection Issued by YE1	NOTED

The page as captured

<https://pub-364c6b3011ca492cab2354176cfaf3f0.r2.dev/>



What pub-364c6b3011ca492cab2354176cfaf3f0.r2.dev served when TrustSniffer captured it on 2026-09-22. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: less than 1 year (registration continuity).
- 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, Kaspersky, Sophos flagged this site in external intelligence checks, indicating elevated compromise/scam exposure that requires immediate caution.

The website currently resolves to a minimal object-not-found page on an R2-hosted subdomain. It presents only a 404 response stating that the requested object does not exist or is not publicly accessible, with no visible products, services, commercial activity, or identifiable operating purpose.

Scam/Impersonation Risk

The site presents a **materially elevated interaction risk** because external security telemetry records malicious detections and a confirmed blacklist status, including detections from multiple security providers. The accessible page itself contains no login form, payment mechanism, wallet connection, or explicit impersonation content, so the page does not independently establish the nature of the underlying threat; however, the external detections are sufficient to create a clear contradiction to treating the domain as benign. Two abuse reports associated with shared CDN infrastructure are discounted as non-attributable to this site, but that attribution issue does not offset the separate malicious and blacklist findings. The domain's operator identity also remains unverified.

EVIDENCE

- The domain was registered in 2026 and is approximately 0.20 years old, based on registration-continuity data.
- External reputation telemetry recorded 15 malicious detections, with threat detections from three major security providers.
- The homepage returned “Not Found,” “Error 404,” and “Object not found,” and contained no forms, links, or monetization elements.

Regulatory Verification Notes

No legal, corporate, licensing, or business disclosures are available on the accessible page. Because the site exposes only an object-not-found response, its regulatory status and business purpose cannot be established from the website itself; this is a verification gap rather than proof of a particular regulatory violation. The available third-party broker dataset produced no name match, but that result is contextual only and does not establish licensing or legitimacy. A valid domain-validation certificate and identifiable hosting network provide transport and infrastructure facts, not evidence of operator identity or authorization.

EVIDENCE

- The accessible homepage contains no legal-entity name, terms, privacy notice, licensing statement, registration number, or regulatory authority reference.
- The site is served from AS13335, operated by CLOUDFLARENET — Cloudflare, Inc., US.
- The TLS certificate uses issuer YE1 with DV validation and is valid through 2026-12-06.

What to Verify Next

Before any sensitive interaction, an independent party should identify the intended operator through authoritative corporate records and confirm any claimed authorization directly with the relevant regulator. Any business, login, payment, or download destination associated with the domain should be validated through an independently sourced official channel rather than through links or contact details presented by the site. If the domain was encountered in a message, advertisement, or referral, the originating communication should also be authenticated separately.

EVIDENCE

- The accessible page provides no operator identity or regulatory reference from which authorization can be independently confirmed.
- The site's only visible content is an object-not-found response, so its intended function cannot be validated from the page.
- The external threat findings require independent confirmation of the domain's provenance before any sensitive use.

Summary Verdict

The overall posture is critical and unsuitable for sensitive interaction. The evidence does not establish a legitimate operating identity or a trustworthy business purpose, and the confirmed external threat conflict

outweighs the limited positive technical observations.

Infrastructure Integrity

Cloudflare CDN/WAF protection is present, and all observed addresses are CDN edge infrastructure rather than an independently attributable origin. This can reduce direct exposure of the origin system and complicate infrastructure attribution, but it is only a mitigating hosting characteristic and does not validate the website or its operator.

Closing Assessment

Sensitive actions should not be undertaken through this domain unless its operator, purpose, and authorization have first been independently established through trusted channels.

Written analysis generated 2026-09-22 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
 - 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

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-364c6b3011ca492cab2354176cfaf3f0.r2.dev.

- The request stayed on pub-364c6b3011ca492cab2354176cfaf3f0.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	0.20 years (continuous registration)
Domain expiry	Not available
Archive first seen	Not available
Archive snapshots	0
Reputation	VirusTotal: 15 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-364c6b3011ca492cab2354176cfaf3f0.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-364c6b3011ca492cab2354176cfaf3f0.r2.dev> · assessed 2026-09-22