

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

justinwithrow.com

Verdict

0

OUT OF 100

CRITICAL RISK

justinwithrow.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

Governance Risk

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

What this site appears to be

Default WordPress sample blog page in Vietnamese. Contains the standard first-post copy and site navigation. No forms, no payment flows, no social links or scripts detected in provided DOM.

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 reports AbuseIPDB; shared hosting inflates this count	NOTED
Domain age	1 months old Most scam domains are under a year old	RISK
Web archive	Archived since 2022 Public history exists	CLEAR
Certificate	Encrypted connection Issued by WE1	NOTED

The page as captured

<https://justinwithrow.com/>

harum4d



Blog

What justinwithrow.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: less than 1 year (registration continuity).
- Public web-archive history exists since 2022.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

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

The website is a Vietnamese-language WordPress sample blog presented under the page title “harum4d” on justinwithrow.com, with a default first-post message, generic navigation, and no apparent commercial, credential-collection, or payment function.

Scam/Impersonation Risk

Confirmed external reputation contradictions make this site unsuitable for sensitive interaction despite the benign appearance of the captured homepage. The domain is recorded as blacklisted by two external sources, with malicious detections from multiple scanners and a Tier-1 vendor detection; this is materially inconsistent with treating the site as trustworthy. The page itself does not show a login, payment flow, phishing form, or brand impersonation, but its generic sample-blog content does not explain the confirmed external detections.

Provenance is also inconsistent: the registration record describes a recently registered domain, while historical records indicate an older multi-year archival presence. No conflicting legal-entity names were observed, so the available evidence does not establish an identity contradiction in the strict legal-entity sense.

EVIDENCE

- External reputation: 12 malicious detections, 1 suspicious detection, and a confirmed blacklist status; Sophos is identified among the flagged vendors.
- Domain registration record: registered 2026 (~0.12 years old); creation date 2026-07-07T06:40:57Z.
- Web archive: 64 snapshots spanning 2022–2025 (4 years tracked).

Regulatory Verification Notes

The captured homepage is informational rather than an apparent regulated financial or commercial service, and it presents no license, registration number, or regulatory authority. That is a transparency gap if the operator later represents the site as a regulated business, but the page does not make such a claim in the supplied content. The available identity evidence remains unverified, and the use of a privacy service in the registration record is an administrative limitation rather than proof of misconduct. A valid domain-validation certificate and mainstream hosting do not independently establish the operator's identity or regulatory standing.

EVIDENCE

- Homepage: no license claim, registration number, or named regulatory authority is displayed.
- Hosting telemetry: served from AS13335 (CLOUDFLARENET - Cloudflare, Inc., US).
- Transport encryption: TLS certificate issued by WE1, validation level DV, valid to 2026-10-06T09:05:59+00:00.

What to Verify Next

Sensitive interaction should remain suspended unless the intended operator can be independently connected to a real-world legal entity through an authoritative registry or an offline contact route. If the site is presented as a financial or regulated service, its claimed authorization should be checked directly with the relevant regulator using the legal entity and license details obtained independently of the site. Enterprise users should also require endpoint review in a controlled security environment before permitting credentials, account access, downloads, or financial activity.

EVIDENCE

- Homepage: 0 forms detected and no sensitive form or untrusted form destination observed.
- Browser observation: no login form, hidden form, wallet connection, clipboard write, or wallet-drainer behavior detected.
- Captured page: HTTP status 200 in 2 successful runs, with 12 console errors recorded.

Summary Verdict

The overall posture is **critical and unsuitable for sensitive interaction**. The site's apparently harmless presentation does not overcome the confirmed external reputation contradictions, and the operator's real-world identity is not independently verified.

Infrastructure Integrity

Cloudflare CDN/WAF protection is present, with all observed addresses resolving to Cloudflare edge infrastructure and no origin candidate exposed in the supplied analysis. This provides a mitigating layer against direct origin exposure but cannot validate the site’s legitimacy or offset the external reputation findings.

Closing Assessment

Treat the site as read-only at most, and do not proceed with login, credential submission, downloads, or financial transactions unless independent identity and security validation produces a satisfactory result.

Written analysis generated 2026-08-20 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, external reputation.

- 01 Governance Risk

 - Registration details are held behind a privacy service, so no operator is named publicly. This is common and legal, and it also means there is nobody to check.
Registration and ownership rule:KF_WHOIS_PRIVATE
 - The registration record withholds contact details for the operator.
Registration and ownership rule:KF_WHOIS_HIDDEN
- 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
 - 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	25%

- 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 justinwithrow.com.

- The request stayed on justinwithrow.com. It was not redirected to another domain. CLEAR
- Registration is published under NAMECHEAP INC. CLEAR
- DNS for this domain is served by cloudflare.com, across 2 name servers. NOTED
- The registration is paid up to 2027-07-07. NOTED
- The earliest public archive of this site is from 2022-02-07. CLEAR
- It is hosted on CLOUDFLARENET, from a server in US. NOTED

Domain intelligence

Registrar	NAMECHEAP INC
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US
Server IP	2606:4700:3031::6815:553d
Name servers	CODY.NS.CLOUDFLARE.COM, RUTH.NS.CLOUDFLARE.COM
SSL issuer	WE1
SSL expiry	2026-10-06
Domain age	0.12 years (continuous registration)
Domain expiry	2027-07-07
Archive first seen	2022-02-07
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 12 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about justinwithrow.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.