

Is bookofblue.com safe? TrustSniffer's moderate-trust assessment: 50/100

bookofblue.com

Verdict

50

OUT OF 100

MODERATE TRUST

bookofblue.com is moderately trusted.

Most signals looked ordinary, and some evidence was missing. Read the checks below before you pay or hand over personal details.

Sensitive Interaction Risk

Governance Risk

Assessed 2026-08-21 by automated analysis. Classification confidence 55%.

What this site appears to be

A Substack-hosted newsletter page titled 'Book of Blue' containing posts, archive, about and subscribe/sign-in links. Content is editorial and adult-themed; standard Substack cookie/privacy notices are 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.

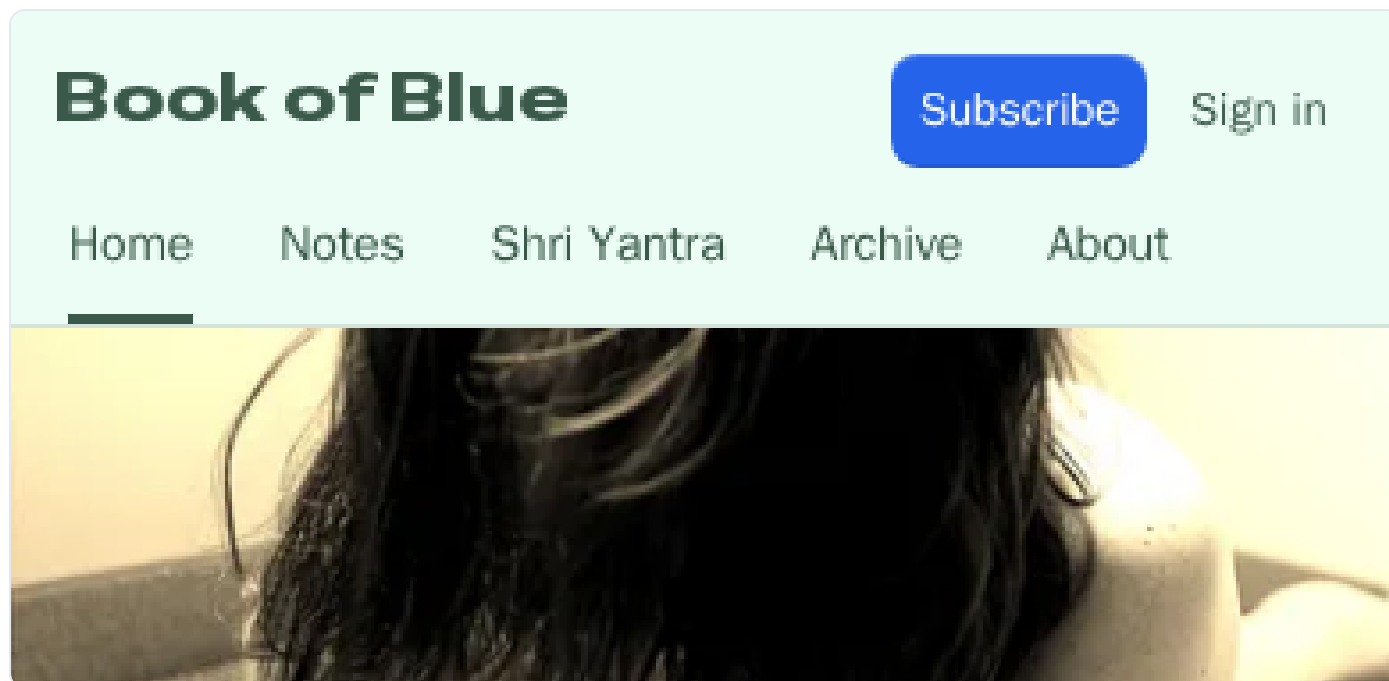
At a glance

The checks that decide most of this verdict.

Malware engines	3 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	21 years old Registered history	CLEAR
Web archive	Archived since 2005 Public history exists	CLEAR
Certificate	Encrypted connection Issued by WE1	NOTED

The page as captured

<https://www.bookofblue.com/>



What bookofblue.com served when TrustSniffer captured it on 2026-08-21. 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 2005.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Overview

Book of Blue is a Substack-hosted newsletter presenting personal essays, archive material, and adult-themed editorial content under the “Book of Blue” title, with subscriptions and possible donations as its apparent business model.

Scam/Impersonation Risk

The site has a **material external reputation contradiction**: multiple threat-intelligence detections are present and the domain is confirmed on external blacklists. This outweighs the otherwise ordinary presentation of the homepage, which contains editorial material, standard Substack subscription and sign-in links, and no detected sensitive form, wallet connection, brand impersonation, or phishing behavior in the captured page. The content itself contains no stated investment, financial, or cryptocurrency proposition; nevertheless, the blacklist findings create a clearly elevated risk for sensitive interactions. No separate identity contradiction was observed across the supplied site content.

EVIDENCE

- The homepage is identified as a Substack newsletter with posts, archive, about, subscribe, and sign-in elements; page-level findings recorded no red flags.
- External reputation assessment recorded 3 malicious and 1 suspicious detections among evaluated results, together with a confirmed blacklist status.
- The domain was registered on 2005-07-19 and is approximately 21.1 years old.
- Historical records show 166 archive snapshots spanning 2005–2024, covering 20 tracked years.

Regulatory Verification Notes

The available pages describe an editorial publication and subscription service rather than a regulated financial offering. No licensing claim or registration number is presented in the supplied content, so regulatory applicability and the real-world operator remain unverified; this is a transparency matter rather than independent evidence of fraud. Registration was conducted through NAMECHEAP INC with a privacy service, which is an administrative limitation on public registrant identification and does not, by itself, establish an identity contradiction. The site's apparent use of mainstream transport and hosting infrastructure supports technical continuity but does not validate the publisher's identity or business standing.

EVIDENCE

- The homepage and About content describe an erotic diary, personal essays, and newsletter posts rather than a financial or investment service.
- WHOIS records list NAMECHEAP INC as registrar and "Withheld for Privacy ehf" as the privacy service.
- The site's transport layer is served through AS13335 (Cloudflare); the TLS certificate was issued by WE1 at DV validation level and is valid to 2026-11-18.
- Page-authority assessment places the site in a mid-range authority band; this is contextual only and does not independently verify the operator.

What to Verify Next

Before any subscription payment or account-related interaction, independently confirm the publisher's legal identity, ownership of the publication, and the applicable subscription, refund, and cancellation terms. Confirm official support and contact channels through an independent route rather than relying solely on links presented on the page. Any organization considering business engagement should also reconcile the external blacklist findings with the publisher and the hosting platform before permitting credentialed or financial access.

EVIDENCE

- The About page is the relevant location for confirming the publisher attribution and stated editorial purpose.
- The homepage's Subscribe and Sign in paths should be checked against the official Substack interface and the intended publication.
- The subscription flow should be reviewed for the contracting party, payment recipient, cancellation process, and refund terms.

Summary Verdict

The website presents as an established editorial publication with a long registration history and technically normal page behavior, but its overall posture is **moderate trust with elevated sensitive-interaction risk**. Apparent legitimacy is not equivalent to independently verified operator identity, and the external reputation contradiction prevents a positive trust determination.

Infrastructure Integrity

The site is protected by an AWS CDN/WAF arrangement, with observed edge infrastructure on AS14618 operated by Amazon.com, Inc.; the origin server was not identified in the analysis. The observed Cloudflare and AWS delivery layers provide a mitigating reduction in direct exposure, but CDN protection is not proof of publisher legitimacy and can limit independent infrastructure attribution.

Closing Assessment

Reading public content may proceed with caution, but credential submission, payment, or other sensitive engagement should remain deferred until the publisher’s identity, transaction terms, and the external reputation findings have been independently resolved.

Written analysis generated 2026-08-21 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 registration record withholds contact details for the operator.
Registration and ownership rule:KF_WHOIS_HIDDEN
- 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

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

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 bookofblue.com.

- The request stayed on bookofblue.com. It was not redirected to another domain. CLEAR
- Registration is published under NAMECHEAP INC. CLEAR
- DNS for this domain is served by ui-dns.biz, across 4 name servers. NOTED
- The registration is paid up to 2027-07-19. NOTED
- The earliest public archive of this site is from 2005-11-24. 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	2606:4700:4406::ac40:97e8
Name servers	NS1045.UI-DNS.BIZ, NS1045.UI-DNS.COM, NS1045.UI-DNS.DE, NS1045.UI-DNS.ORG
SSL issuer	WE1
SSL expiry	2026-11-18
Domain age	21.10 years (continuous registration)
Domain expiry	2027-07-19
Archive first seen	2005-11-24
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 3 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

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