

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

enxuga.com.br

Verdict

0

OUT OF 100

CRITICAL RISK

enxuga.com.br 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 2026-08-21 by automated analysis. Classification confidence 55%.

What this site appears to be

Portuguese-language site offering 26 free, client-side browser tools for PDF and image manipulation (compress, merge, split, convert, edit). Emphasizes privacy (no upload), no registration, and ad-supported revenue.

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	5 flagged it VirusTotal	RISK
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	0% confidence AbuseIPDB, 12 reports; shared hosting inflates reports	CLEAR
Domain age	4 months old Most scam domains are under a year old	RISK
Web archive	Archived since 2019 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YR2	NOTED

The page as captured

https://www.enxuga.com.br/



Enxuga



● Privacidade real • 26 ferramentas grátis

What enxuga.com.br served when TrustSniffer captured it on 2026-08-21. 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 2019.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

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

Enxuga is a Portuguese-language browser utility website presenting 26 free tools for compressing, merging, splitting, converting, editing, and otherwise processing PDF and image files locally in the browser; it states that files do not leave the device, requires no registration, and is supported primarily by advertising.

Scam/Impersonation Risk

The site's ordinary utility content contains no observed brand-impersonation, login, payment, or other overt phishing features, and the advertised service is technically consistent with a client-side file-processing model. However, this benign presentation is outweighed by confirmed external threat detections: five malicious detections were recorded, including detections from Fortinet and Sophos, and the domain is blacklisted by two external sources. Twelve abuse reports associated with a shared Vercel CDN address are discounted because they apply to shared infrastructure rather than being site-specific; that attribution does not negate the separate malicious detections and blacklist findings. No conflicting legal-entity names or direct brand impersonation were

observed. The overall implication is that sensitive interaction with the site is not appropriate despite its low-risk page content.

EVIDENCE

- External reputation assessment: 5 malicious detections among 10 effective detections; Fortinet and Sophos were specifically flagged, with blacklist status reported by VT and EXTERNAL_BLACKLIST.
- The domain registration record states creation on 2026-04-26 and an age of 0.32 years.
- Historical records show the domain first recorded on 2019-11-02 and last recorded on 2025-02-27, representing 7 years tracked.
- The shared-infrastructure signal concerns 12 abuse reports for 64.29.17.65, attributed to Vercel, Inc. as a CDN address and explicitly discounted for that reason.

Regulatory Verification Notes

The captured homepage describes a free, advertising-supported utility service and makes no licensing or regulated-service claim. It does not provide a registration number or a clearly independently verifiable corporate identity in the supplied page content; the registration record names Andre Railon Souto Melo, but the available evidence does not independently establish that person as the operator of the website. This is an identity and disclosure matter rather than a standalone finding of fraud. The decisive regulatory concern remains the confirmed external blacklist and malicious-detection record, while the valid transport certificate and mainstream hosting environment provide technical assurances only, not legal or operational validation.

EVIDENCE

- The homepage presents PDF and image processing tools, “no upload” and “no registration” claims, and advertising-supported operation; no license number or regulated-service disclosure is shown in the captured content.
- The registration record lists Andre Railon Souto Melo as the owner and shows expiration on 2028-04-26.
- The site is served through AS16509, AMAZON-02 - Amazon.com, Inc., US.
- TLS uses issuer YR2 with DV validation and is valid to 2026-09-25T00:19:09+00:00.

What to Verify Next

Any prospective engagement should be limited to non-sensitive inspection until the operator’s identity and the external detections have been independently resolved. Licensing or registration should be checked directly with the relevant Brazilian registry if the service is being considered for organizational use, and official contact channels should be confirmed through an independent route rather than relying solely on the website. Security teams should also obtain a current endpoint assessment before permitting the domain in environments that process confidential files.

EVIDENCE

- The homepage contains no login form, password field, hidden form, or untrusted form destination.
- Browser testing recorded 0 wallet-connect runs, 0 wallet-sensitive runs, 0 wallet-drainer runs, and 0 clipboard-write detections.
- The captured page returned successfully in 2 of 2 behavioral runs, but stable page behavior does not resolve the external reputation findings.

Summary Verdict

The website presents a coherent file-utility service, but its overall trust posture is critical because confirmed external malicious detections and blacklist findings materially conflict with the otherwise benign page presentation. The real-world operator identity also remains unverified, so the site should not be treated as established or suitable for sensitive interaction.

Infrastructure Integrity

The site is protected by Cloudflare CDN/WAF infrastructure, with observed edge addresses 216.198.79.65 and 64.29.17.65 on AS16509, AMAZON-02 - Amazon.com, Inc. All observed addresses were CDN edges and no origin candidate was identified. This protection mitigates direct infrastructure exposure but cannot establish legitimacy or offset the external threat signals.

Closing Assessment

Enterprise controls should block or isolate the domain for login, credential, confidential-file, and financial workflows pending independent resolution of the reputation findings and operator identity.

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, external reputation.

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.
- 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

Signals weighed against the site

- AbuseIPDB: 12 reports on hosting IP 64.29.17.65 (Vercel, 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 enxuga.com.br.

- The request stayed on enxuga.com.br. It was not redirected to another domain. [CLEAR](#)
- DNS for this domain is served by cloudflare.com, across 2 name servers. [NOTED](#)
- The registration is paid up to 2028-04-26. [CLEAR](#)
- The earliest public archive of this site is from 2019-11-02. [CLEAR](#)
- It is hosted on AMAZON-02, from a server in US. [NOTED](#)

Domain intelligence

Registrar	Not available
Hosting	AMAZON-02 - Amazon.com, Inc., US
Country	US
Server IP	64.29.17.65
Name servers	coco.ns.cloudflare.com, mario.ns.cloudflare.com
SSL issuer	YR2
SSL expiry	2026-09-25
Domain age	0.32 years (continuous registration)
Domain expiry	2028-04-26
Archive first seen	2019-11-02
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 5 flagged AbuseIPDB: 0% confidence, 12 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about enxuga.com.br 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/enxuga.com.br> · assessed 2026-08-21