

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

aaniqtyrxr.com

Verdict

0

OUT OF 100

CRITICAL RISK

aaniqtyrxr.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

Chinese-language news portal page containing multiple article links, news tickers, image assets and advertisement slots. Primary function is content publishing and aggregation of topical news.

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	2.6 years old Registered history	CLEAR
Web archive	Archived since 2023 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YR2	NOTED

The page as captured

https://aaniqtyrxr.com/

[收藏本页](#) [回到首页](#)

请稍等片刻

What aaniqtyrxr.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: 1 to 3 years (registration continuity).
- Public web-archive history exists since 2023.
- 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 Chinese-language news and media portal presenting editorial articles, news feeds, topical headlines, image assets, and advertising placements. Its apparent business model is ad-supported content publishing, with possible sponsored-content or subscription monetization rather than an identified financial-services or transactional offering.

Scam/Impersonation Risk

The principal risk is not the site's visible editorial presentation but the convergence of confirmed external threat detections and blacklist results associated with the domain. These findings constitute a material contradiction to the otherwise low-risk appearance of the homepage. No identity inconsistency or brand-impersonation signal was detected in the supplied page analysis, and the homepage contained no login form, password form, or other sensitive input surface; nevertheless, the external detections warrant treating the domain as unsuitable for credentials, account access, financial activity, or other sensitive interaction. The site should be regarded as

potentially compromised, misclassified, or otherwise unsafe for sensitive use until the domain's status is independently resolved.

EVIDENCE

- External reputation telemetry recorded 12 malicious detections and 2 suspicious detections; the domain was blacklisted by two external sources, with a Tier-1 security provider among the flagging vendors.
- The homepage was identified as a news/media page with no login form, hidden form, or sensitive form detected during capture.
- Historical telemetry records 10 archive snapshots from 2023-09-09 through 2026-05-19, with 4 years tracked and no detected semantic repurposing.

Regulatory Verification Notes

The available evidence does not independently verify the real-world operator behind the website. The homepage is editorial in character and does not present a claimed license, licensing authority, or license number; this is a disclosure gap rather than, by itself, proof of fraud. The displayed Chinese company name should therefore not be treated as proof that the registrant, publisher, or operator is that entity. A valid domain-validated TLS certificate confirms encrypted transport, but does not establish ownership or regulatory standing. The negative external reputation signal remains the decisive concern, while the absence of a broker-dataset match provides no affirmative licensing or safety conclusion.

EVIDENCE

- WHOIS records show registration on 2026-01-20, approximately 0.58 years old, through NameSilo, LLC; the registrant is recorded as "wei li."
- The site is served from AS54600, PEG-SV - PEG TECH INC, US.
- The site's TLS certificate is issued by YR2, uses DV validation, and is valid through 2026-10-16.
- The homepage title displays "宁安市菲杨股份有限公司," while the captured content consists of news articles, feeds, and advertising placements rather than an independently verified corporate or regulated-services disclosure.

What to Verify Next

Before any sensitive interaction, an independent source should confirm that this is the intended official domain for the publisher named on the page. Any claimed corporate relationship should be checked through an authoritative corporate registry or a separately sourced publisher contact, and any activity that could involve regulated services should be matched against the relevant licensing register. Security teams should also confirm whether the domain has been remediated or incorrectly classified through independent reputation checks before permitting it in credentialed or transactional workflows.

EVIDENCE

- The captured homepage contains no sensitive form or login mechanism, so its editorial appearance does not demonstrate that sensitive interaction would be appropriate elsewhere on the domain.
- The available identity evidence is insufficient to independently connect the displayed publisher name with a verified real-world operator.
- The site's advertising and external-request behavior should be reviewed separately from the editorial content before allowing broader enterprise access.

Summary Verdict

The overall posture is **critical and unsuitable for sensitive interaction**. Although the website presents a coherent editorial-media experience, the confirmed external threat and blacklist contradictions outweigh that surface appearance. The operator's real-world identity is not independently verified.

Infrastructure Integrity

The domain resolves directly to a single likely origin address, with no detected CDN, WAF vendor, or edge-IP layer. This infrastructure provides no additional protective edge-layer mitigation, although the presence of resolved hosting and valid transport encryption confirms basic technical availability rather than legitimacy.

Closing Assessment

Enterprise controls should restrict the domain to tightly controlled passive review, prevent credentialed and financial use, and require independent domain and operator validation before any broader access is authorized.

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

- 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
- The page exchanged network traffic with destinations TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_TRAFFIC
- The page made background requests to destinations TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_XHR
- 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	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 aaniqtyrxr.com.

- The request stayed on aaniqtyrxr.com. It was not redirected to another domain. CLEAR
- Registration is published under NameSilo, LLC. CLEAR
- DNS for this domain is served by aaniqtyrxr.com, across 2 name servers. NOTED
- The registration is paid up to 2027-01-20. NOTED
- The earliest public archive of this site is from 2023-09-09. CLEAR
- It is hosted on PEG-SV, from a server in US. NOTED

Domain intelligence

Registrar	NameSilo, LLC
Hosting	PEG-SV - PEG TECH INC, US
Country	US
Server IP	192.74.235.172
Name servers	NS1.AANIQTYRXR.COM, NS2.AANIQTYRXR.COM
SSL issuer	YR2

SSL expiry	2026-10-16
Domain age	2.64 years (continuous registration)
Domain expiry	2027-01-20
Archive first seen	2023-09-09
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 aaniqtyrxr.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.

This report online: <https://trustsniffer.com/report/aaniqtyrxr.com> · assessed 2026-08-20