

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

arvinryu.com

Verdict

0

OUT OF 100

CRITICAL RISK

arvinryu.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 2026-08-22 by automated analysis. Classification confidence 55%.

What this site appears to be

Chinese-language ecommerce site selling pre-verified WeChat accounts (various ages/regions) and device+SIM bundles with automated post-payment delivery and 7-day after-sales support. Offers bulk discounts and claims实名认证功能; lacks verifiable corporate contact or legal credentials in the extracted content.

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	6 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	11 days old Most scam domains are under a year old	RISK
Web archive	Archived since 2013 Public history exists	CLEAR
Certificate	Encrypted connection Issued by WE1	NOTED

The page as captured

https://www.arvinryu.com/

雅域微信号批发平台



⚡ 2026 优选平台 · 自动发货

What arvinryu.com served when TrustSniffer captured it on 2026-08-22. 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 2013.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

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

arvinryu.com presents a Chinese-language ecommerce marketplace for pre-registered WeChat accounts, including domestic, international, and “original-device” packages containing phones and SIM cards. The site promotes bulk purchasing, automated payment-to-delivery fulfillment, account features such as real-name verification and payment capability, and a seven-day after-sales policy.

Scam/Impersonation Risk

The site presents a materially elevated risk for sensitive interaction. External security intelligence recorded six malicious detections and a confirmed blacklist status across multiple sources, which is a direct contradiction to treating the marketplace as a safe commercial counterparty. The homepage’s sale of pre-registered WeChat accounts—advertised with payment, transfer, red-envelope, and “anti-ban” or “anti-complaint” characteristics—also creates a high-abuse business model: account access is obtained after payment through automated delivery, while the site provides limited evidence supporting the provenance or lawful control of those accounts.

No separate brand-impersonation finding or conflicting legal-entity identity was established, but those absences do not offset the confirmed external detections and the site's account-trading mechanics.

EVIDENCE

- Homepage: advertises five-month, three-month, six-month, one-year, two-year, and five-year WeChat accounts, including claims of real-name verification, payment capability, transfer functionality, and resistance to bans or complaints.
- Homepage: offers original-device Android and Apple packages containing a phone, SIM or data card, and an associated verified WeChat account, with automated post-payment fulfillment.
- External reputation telemetry: 6 malicious detections were recorded, with a confirmed blacklist result from 2 sources.
- Domain provenance record: first seen 2013-06-18T20:30:20Z; authoritative reconciled domain age 13.174537987679672 years; last seen 2026-05-19T13:52:38Z; 0 archive snapshots reported across 14 years tracked.

Regulatory Verification Notes

The site's legal and commercial disclosures are insufficient for a regulated counterparty assessment. Extracted content does not provide a verifiable corporate contact, legal entity, registration number, or claimed licensing authority, and the business model involves the sale of accounts that may carry significant platform, privacy, and compliance implications. These are verification gaps rather than independent proof of fraud, but they prevent reliable attribution of the operator and prevent confirmation that the advertised account transfers and payment-related features are authorized. The absence of a broker-dataset match provides no licensing or regulatory assurance.

EVIDENCE

- Homepage and business-content extraction: identifies the operator only through the marketplace presentation and does not establish a verifiable corporate identity or legal credential.
- Homepage: describes one-time purchases, wholesale discounts, automated delivery, and seven-day after-sales support without identifying a licensing or registration basis.
- Registration telemetry: registrar recorded as NameSilo, LLC; current WHOIS creation date is 2026-08-09T13:51:52Z and expiry date is 2027-08-09T13:51:52Z.
- Transport and hosting telemetry: hosted by CLOUDFLARENET - Cloudflare, Inc., US, on AS13335; TLS certificate issued by WE1 at DV validation level, valid to 2026-11-10T15:54:39+00:00.

What to Verify Next

Before any operational engagement, an institution should independently establish the seller's legal identity, physical jurisdiction, and authority to trade or transfer the advertised accounts. Any claimed payment, real-name, or account-history attributes should be validated through the relevant platform's policies and an independent channel rather than relying on the marketplace's own descriptions. Payment arrangements should be assessed for reversibility, buyer protection, and sanctions or acceptable-use exposure, and the official support and contact channels should be confirmed through an offline or independently sourced route.

EVIDENCE

- Homepage: product descriptions rely on seller assertions regarding account age, verification, payment functionality, stability, and resistance to enforcement.
- Purchase flow: a purchase form and automated checkout require payment before access or delivery.
- Site content: no independently verifiable corporate contact or legal credential was identified in the extracted material.

Summary Verdict

The available evidence supports a **critical trust posture** with a clear risk of sensitive interaction. The combination of confirmed external malicious detections, blacklist status, unverified operator identity, and an abuse-prone account marketplace is incompatible with normal credential, payment, or business-counterparty confidence.

Infrastructure Integrity

Cloudflare CDN and WAF protection provide a mitigating layer against direct exposure of the hosting environment, but they do not establish the legitimacy of the operator or the safety of the marketplace. All observed addresses were Cloudflare edge infrastructure, and the origin server was not observable in this analysis.

Closing Assessment

The site should be treated as unsuitable for account login, credential submission, payment, or other sensitive transactions unless the operator, legal basis, product provenance, and payment protections are independently confirmed to an institutional standard.

Written analysis generated 2026-08-22 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, page content, external reputation.

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
- A form on the page submits to a destination TrustSniffer could not verify.
Page content rule:PAGE_FORM_UNTRUSTED_DEST
- 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 arvinryu.com.

- The request stayed on arvinryu.com. It was not redirected to another domain. CLEAR
- Registration is published under NameSilo, LLC. CLEAR
- DNS for this domain is served by cloudflare.com, across 2 name servers. NOTED
- The registration is paid up to 2027-08-09. NOTED
- The earliest public archive of this site is from 2013-06-18. CLEAR
- It is hosted on CLOUDFLARENET, from a server in US. NOTED

Domain intelligence

Registrar	NameSilo, LLC
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US
Server IP	2606:4700:3033::ac43:c712
Name servers	ISLA.NS.CLOUDFLARE.COM, KIANCHAU.NS.CLOUDFLARE.COM
SSL issuer	WE1
SSL expiry	2026-11-10
Domain age	0.03 years (continuous registration)
Domain expiry	2027-08-09

Archive first seen	2013-06-18
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 6 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about arvinryu.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/arvinryu.com> · assessed 2026-08-22