

Is xn--im-1z5cr40w.top a scam? TrustSniffer's high-risk assessment: 5/100

xn--im-1z5cr40w.top

Verdict

5

OUT OF 100

CRITICAL RISK

xn--im-1z5cr40w.top 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 50%.

What this site appears to be

Chinese-language 404 error page indicating the requested page was not found; invites user to return to homepage.

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.

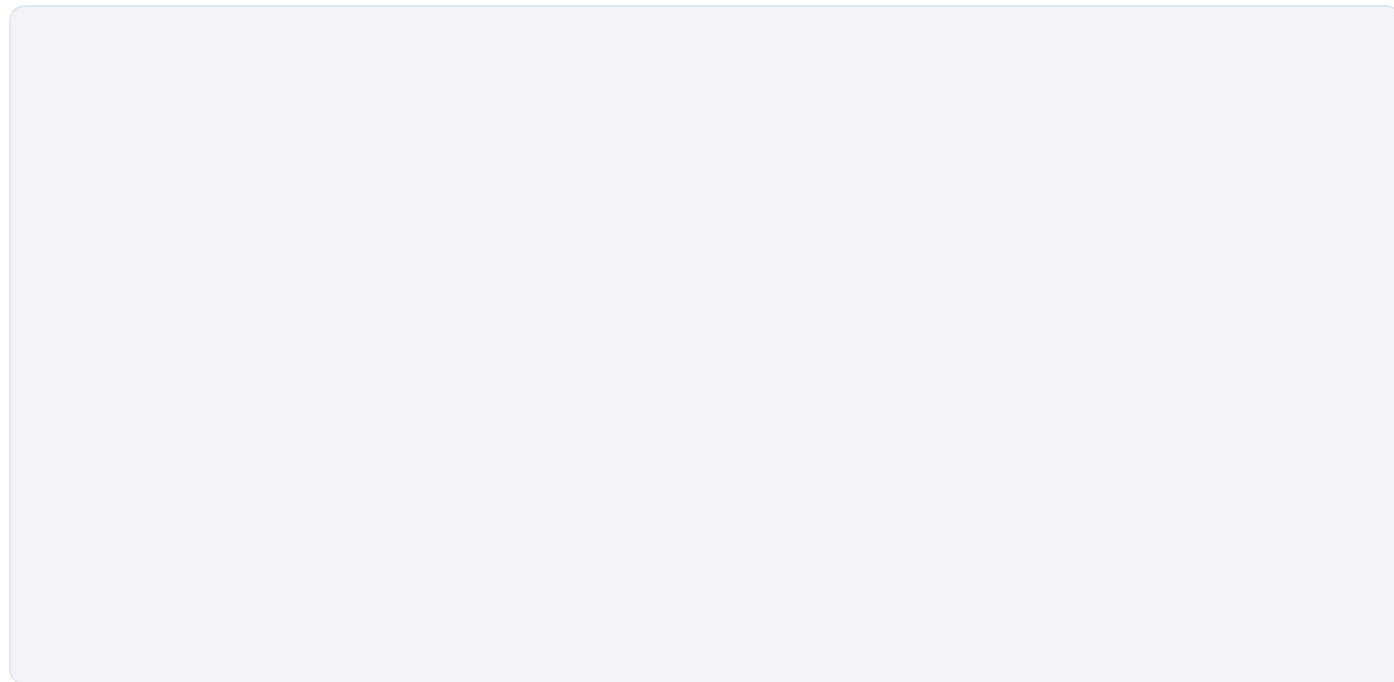
At a glance

The checks that decide most of this verdict.

Malware engines	None flagged it VirusTotal	CLEAR
Google Safe Browsing	Listed as unsafe Google	RISK
Abuse reports on the host	0 reports AbuseIPDB; shared hosting inflates this count	NOTED
Domain age	1.2 years old Registered history	CLEAR
Web archive	Archived since 2025 Public history exists	CLEAR
Certificate	Encrypted connection Issued by WE1	NOTED

The page as captured

https://h6maj5.walletstore.app/web_home_cn/



What xn--im-1z5cr40w.top served when TrustSniffer captured it on 2026-08-21. 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 2025.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Overview

This website is a Chinese-language informational web presence currently presenting a “page not found” error, with an invitation to return to the homepage; the observed content does not establish a functioning commercial, financial, or other service purpose.

Scam/Impersonation Risk

Confirmed external threat detections materially elevate the risk of sensitive interaction. The domain is listed by Google Safe Browsing and an external blacklist, with the recorded threat classification involving social-engineering risk. These findings are stronger than the benign characteristics of the captured page, which contains no login form, payment form, wallet connection, or evident monetization. No separate identity inconsistency or brand-impersonation finding was observed, but the blacklist status requires the site to be treated as untrusted for credentials, account access, and financial activity.

EVIDENCE

- External reputation telemetry records a Google Safe Browsing malicious match and an external blacklist listing for the domain.
- Domain registration telemetry records creation in 2025, with an age of approximately 1.16 years.
- Archive telemetry records 1 snapshot on 2025-07-10, covering 1 year of tracked history.
- The homepage capture displays a Chinese-language 404 page and contains no login, sensitive form, wallet connection, or payment interaction.

Regulatory Verification Notes

The observed page does not provide a company identity, regulatory licence, registration number, or description of a regulated service. This is a disclosure gap rather than independent proof of fraud, but the absence of an identifiable operating entity prevents meaningful confirmation of legal responsibility or licensing status. The domain's independent identity remains unverified. Its transport and hosting controls are technically valid, although those controls do not establish regulatory standing or operator legitimacy.

EVIDENCE

- The captured homepage is titled “404 - 页面未找到” and contains only an error message and a return-to-homepage option.
- The site's business-model assessment identifies static informational content and no presented commercial offering.
- The domain is registered through Chengdu west dimension digital.
- The site is served from AS13335 (CLOUDFLARENET - Cloudflare, Inc., US); its TLS certificate is issued by WE1, uses DV validation, and is valid to 2026-09-21T17:04:37+00:00.

What to Verify Next

Before any sensitive interaction, an independent source should confirm the intended official domain and identify the responsible legal entity. Any claimed financial, investment, trading, or payment service should be checked directly against the relevant regulator's public register, and the official support and contact channels should be confirmed through an offline or independently sourced route. If those checks cannot be completed, activity should remain limited to passive observation.

EVIDENCE

- The only observed page is a 404 response and does not define the site's operator or service scope.
- No licence claim, licensing authority, or licence number is present in the analysed site content.
- The captured page exposes no authenticated workflow or commercial transaction process against which operator claims could be validated.

Summary Verdict

The overall posture is **critical trust risk**, driven by confirmed external threat detections and the inability to establish a verified real-world operator from the available evidence. The site should not be treated as suitable for sensitive interaction.

Infrastructure Integrity

Cloudflare CDN/WAF protection is present, and the observed addresses are Cloudflare edge servers rather than directly exposed origin infrastructure. This provides a defensive hosting layer but is only a mitigating technical characteristic; it cannot offset the external threat detections or establish legitimacy.

Closing Assessment

Prospective users should restrict activity to passive viewing and should not provide credentials, authenticate accounts, or conduct financial transactions unless the domain, operator, and service claims have been independently validated.

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
 - 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
 - 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 xn--im-1z5cr40w.top.

- The request for xn--im-1z5cr40w.top ended on h6majs.walletstore.app, a different domain.

WATCH

- Registration is published under Chengdu west dimension digital. CLEAR
- DNS for this domain is served by dnspod.net, across 2 name servers. NOTED
- The registration is paid up to 2027-06-22. NOTED
- The earliest public archive of this site is from 2025-07-10. CLEAR
- It is hosted on CLOUDFLARENET, from a server in US. NOTED

Domain intelligence

Registrar	Chengdu west dimension digital
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US
Server IP	172.67.178.197
Name servers	lee.dnspod.net, kent.dnspod.net
SSL issuer	WE1
SSL expiry	2026-09-21
Domain age	1.16 years (continuous registration)
Domain expiry	2027-06-22
Archive first seen	2025-07-10
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 0 flagged AbuseIPDB: 0 reports Google Safe Browsing: 1 match

About this assessment

A trust score summarises the evidence TrustSniffer could collect about xn--im-1z5cr40w.top 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/xn--im-1z5cr40w.top> · assessed 2026-08-21