

Is iman23.com a scam? TrustSniffer's high-risk assessment: 0/100

iman23.com

Verdict

0

OUT OF 100

CRITICAL RISK

iman23.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

Page contains a single short Chinese text '刷新一下' ("refresh"). No links, forms, social references, or identifiable business model.

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.

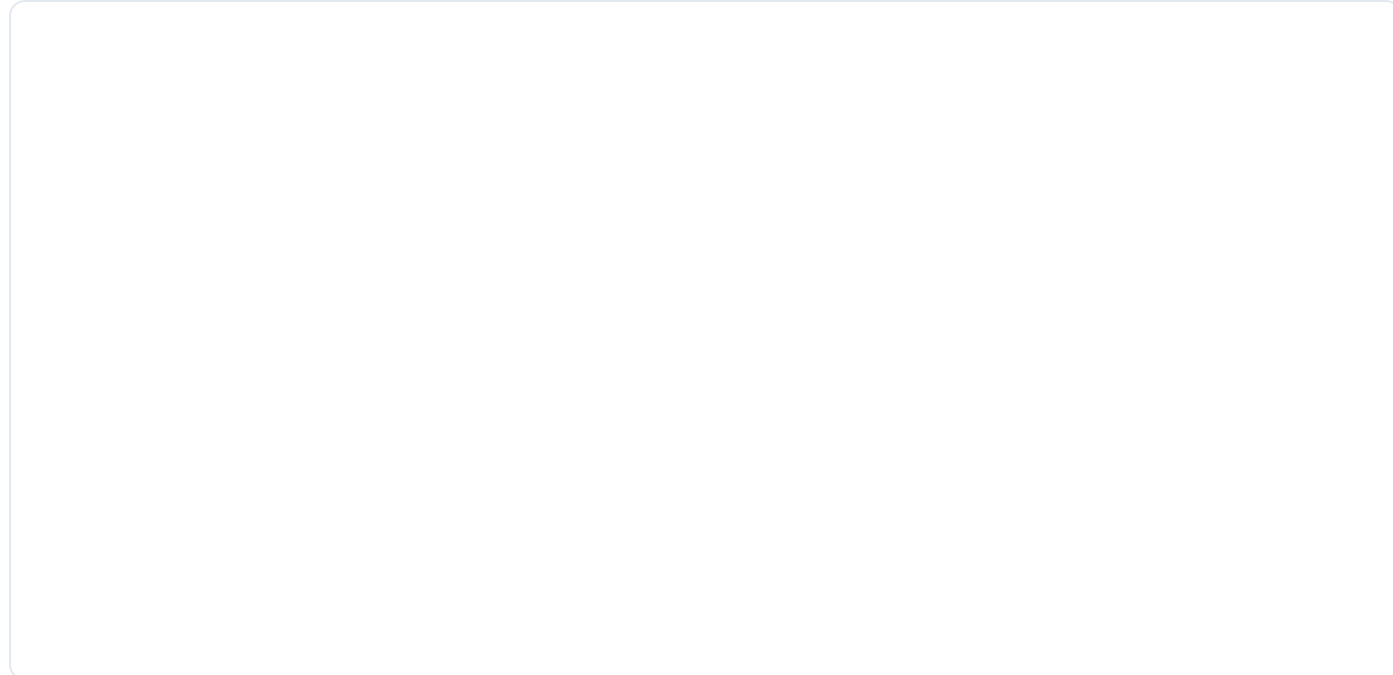
At a glance

The checks that decide most of this verdict.

Malware engines	18 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	6.6 years old Registered history	CLEAR
Web archive	Archived since 2021 Public history exists	CLEAR
Certificate	Encrypted connection Issued by WE1	NOTED

The page as captured

<https://iman23.com/>



What iman23.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: 3 to 10 years (registration continuity).
- Public web-archive history exists since 2021.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

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

This website is a minimally presented domain whose homepage displays only the Chinese phrase “刷新一下” (“refresh”). It provides no identifiable service description, product information, business identity, navigation, or visible transaction functionality, leaving its apparent purpose and operating model undetermined.

Scam/Impersonation Risk

Confirmed external threat contradictions make this a critical-risk website for sensitive interaction. The domain is reported as malicious by 18 evaluated detections, including signals from Fortinet, Kaspersky, and Sophos, and it is also present on an external blacklist; these findings are materially more significant than the absence of a Google Safe Browsing malicious result. The homepage itself contains no clear impersonated brand, phishing form, or identifiable business model, so the available evidence does not establish a specific impersonation target. However, the combination of confirmed blacklist status, malicious detections, minimal site content, and suspicious external network activity warrants a security-forward posture.

EVIDENCE

- External reputation telemetry records 18 malicious detections, with Fortinet, Kaspersky, and Sophos among the flagged vendors; the domain is also recorded on an external blacklist.
- The homepage contains only “刷新一下” and no links, forms, business identity, service description, or transaction flow.
- Browser observation recorded 9 external XHR requests and 9 external POST requests, including 3 non-whitelisted XHRs and 4 non-whitelisted POSTs; interaction produced a maximum DOM difference of 622.

Regulatory Verification Notes

The available page does not identify a legal entity, licensing authority, registration number, governing jurisdiction, or substantive terms of service. This is a significant disclosure gap for any site that might later request credentials, payments, or other sensitive information, while the real-world operator remains independently unverified. Technical registration and transport signals provide limited contextual support: the domain is long-established and registered through NameCheap, Inc., and its TLS certificate is valid, although domain-validated TLS confirms encrypted transport rather than legal identity or authorization. No matching broker signal was identified in the available third-party context.

EVIDENCE

- Domain registration records show creation on 2020-01-03 and an age of 6.64 years; the registrar is NameCheap, Inc., with expiration on 2027-01-03.
- Archive coverage records first observation on 2021-12-08 and last observation on 2026-02-17, with 6 years tracked and sparse historical coverage.
- The site uses a valid DV TLS certificate issued by WE1, valid through 2026-10-29T23:15:53+00:00.

What to Verify Next

Before any sensitive interaction, an independent route should confirm the operator’s legal identity, business purpose, and any licensing or registration claimed outside the site. Any proposed payment destination, credential request, download, or referral should be validated through a separately sourced official channel, and browser or endpoint security controls should review the domain before permitting continued interaction.

EVIDENCE

- The homepage supplies no operator, service, licensing, or contact disclosure against which independent identity verification can be performed.
- The available technical assessment records confirmed malicious and blacklist-related reputation signals, requiring independent validation before sensitive use.

Summary Verdict

The overall posture is **critical trust risk**, with the site unsuitable for credentials, login activity, or financial interaction on the available evidence. The site’s limited presentation and lack of independently verified identity do not provide a credible basis to overcome the confirmed external threat findings.

Infrastructure Integrity

The website is protected by Cloudflare CDN/WAF infrastructure, and all observed addresses were CDN edge servers rather than an independently observable origin. This reduces direct origin exposure but is only a mitigating infrastructure characteristic; it does not validate the operator or offset the external reputation risk.

EVIDENCE

- Served from AS13335 (CLOUDFLARENET - Cloudflare, Inc., US); 3 observed IP addresses were identified as CDN edges and 0 as likely origin addresses.

Closing Assessment

The appropriate institutional action is to restrict the domain to passive observation, block sensitive interaction, and require independent identity and authorization confirmation before any operational engagement.

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, 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 sent data to a destination TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_POSTS
- 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
- The structure of the page changed sharply while it was loading.
Behaviour in a sandbox rule:BEHAV_DOM_DENSITY_SPIKE
- 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 iman23.com.

- The request stayed on iman23.com. It was not redirected to another domain. CLEAR
- Registration is published under NameCheap, Inc.. CLEAR
- DNS for this domain is served by cloudflare.com, across 2 name servers. NOTED
- The registration is paid up to 2027-01-03. NOTED
- The earliest public archive of this site is from 2021-12-08. 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	104.21.2.13
Name servers	CHRIS.NS.CLOUDFLARE.COM, ROXY.NS.CLOUDFLARE.COM
SSL issuer	WE1
SSL expiry	2026-10-29
Domain age	6.64 years (continuous registration)
Domain expiry	2027-01-03
Archive first seen	2021-12-08
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 18 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about iman23.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/iman23.com> · assessed 2026-08-22