

Is iman227.com a scam? TrustSniffer's high-risk assessment: 0/100

iman227.com

Verdict

0

OUT OF 100

CRITICAL RISK

iman227.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 2026-08-21 by automated analysis. Classification confidence 55%.

What this site appears to be

GPT summary status=skipped | No usable content for GPT summary (clean/dom/html all empty)

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.

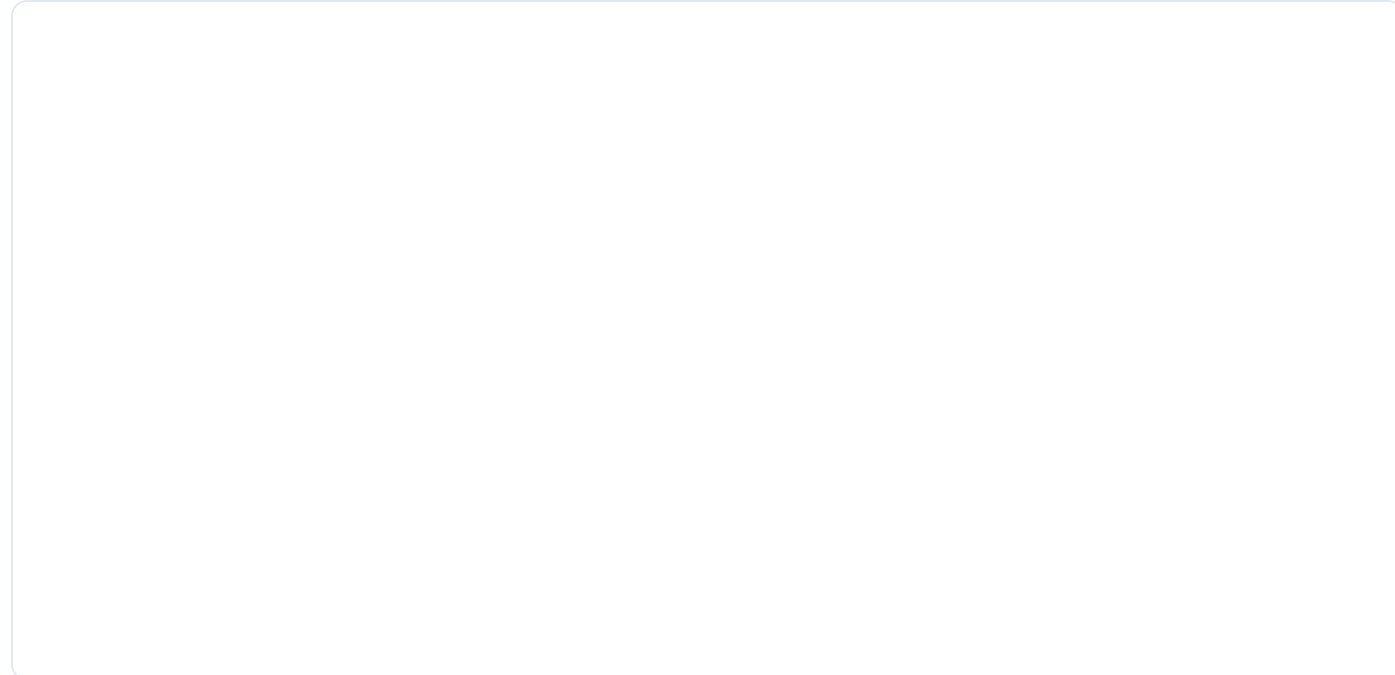
At a glance

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://iman227.com/



What iman227.com served when TrustSniffer captured it on 2026-08-21. 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.

iman227.com is a web domain whose available homepage material does not establish a named service, product, or operator; its apparent business purpose therefore cannot be reliably determined from the supplied site content.

Scam/Impersonation Risk

The site presents a **critical sensitive-interaction risk**. Confirmed blacklist and malicious-reputation findings are direct contradiction signals, even though no separate identity contradiction, impersonation, or phishing-page determination was established. Browser behavior also showed suspicious external communications, substantial page mutation after interaction, and a password-form surface; these characteristics increase concern around credential or other sensitive interaction. A valid certificate and stable web response do not offset the external threat detections.

EVIDENCE

- The domain received a confirmed blacklist hit from two evaluated sources, with malicious detections recorded by multiple security providers.
- Homepage interaction telemetry recorded 9 external XHR requests, 9 external POSTs, 3 non-whitelisted XHRs, 4 non-whitelisted POSTs, and 2,886 DOM mutations.
- Behavioral telemetry recorded 1 password form, 2 successful analysis runs, and no detected wallet-drainer, clipboard-hijack, or cloaking activity.

Regulatory Verification Notes

The available evidence does not independently verify the real-world operator or establish that the website represents a regulated entity. The registration record identifies NAMECHEAP INC as registrar and uses a privacy service; that is an administrative registration detail, not proof of misconduct, but it does not independently establish the operator's legal identity. Licensing and regulatory status remain unconfirmed, and the site material supplied does not provide a sufficient basis for a legal or licensing conclusion. The transport certificate is valid but uses domain validation, which authenticates control of the domain rather than the legal entity behind it.

EVIDENCE

- Domain registration: 2020-01-18; approximately 6.59 years old; registrar NAMECHEAP INC.
- Hosting telemetry identifies AS13335, CLOUDFLARENET - Cloudflare, Inc., US.
- TLS certificate issued by WE1 with DV validation, valid to 2026-10-18T22:14:57+00:00.

What to Verify Next

Any prospective engagement should first identify the responsible legal entity and independently confirm its registration and any claimed authorization through the relevant official registry. Contact channels should be validated through an independently sourced route, and security teams should review the domain's confirmed threat-reputation status before permitting authentication, payment, or other sensitive workflows. Until those checks are resolved, access should remain limited to non-sensitive observation.

EVIDENCE

- Independent operator identity verification is currently unknown.
- The supplied site material does not establish a confirmed regulated status or licensed business activity.
- The authoritative assessment identifies login, credential submission, and financial interaction as unsafe use cases.

Summary Verdict

The website has a **critical trust posture** driven by corroborated external threat detections and confirmed blacklist status. Its apparent identity and business purpose are not independently established, so the available evidence does not support treating it as a legitimate destination for sensitive interaction.

Infrastructure Integrity

The website is protected by Cloudflare CDN/WAF infrastructure and resolves through Cloudflare edge servers on AS13335; the observed addresses were 104.21.17.33 and 172.67.220.124, with no origin-server candidate observable in the analysis. This infrastructure can mitigate direct exposure of the hosting environment, but it is only a protective control and does not establish legitimacy or neutralize the reputation findings.

Closing Assessment

Prospective users and organizations should defer login, credential submission, payments, and other financial activity until the operator and security reputation have been independently validated; enterprise controls should block or isolate the domain pending that review.

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, behaviour in a sandbox, 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
- 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
- The page sent data to a destination TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_POSTS
- The structure of the page changed sharply while it was loading.
Behaviour in a sandbox rule:BEHAV_DOM_DENSITY_SPIKE
- The page rewrote itself after it was interacted with, so what a visitor first sees is not what they end up on.
Behaviour in a sandbox rule:BEHAV_DOM_DIFF_AFTER_INTERACTION
- 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	UNKNOWN
Identity score	50/100
Identity verification confidence	15%

- AI page analysis unavailable (page captured; identity not AI-verified)

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 iman227.com.

- The request stayed on iman227.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 2027-01-18. NOTED
- The earliest public archive of this site is from 2021-12-04. 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	172.67.220.124
Name servers	BUCK.NS.CLOUDFLARE.COM, POLA.NS.CLOUDFLARE.COM
SSL issuer	WE1
SSL expiry	2026-10-18
Domain age	6.59 years (continuous registration)
Domain expiry	2027-01-18
Archive first seen	2021-12-04
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 iman227.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/iman227.com> · assessed 2026-08-21