

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

mcas.me

Verdict

0

OUT OF 100

CRITICAL RISK

mcas.me 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

Marketing/product page for a Hospital Management System offering register modules and a contact form; contains a login link and basic placeholder content. No aggressive conversion or financial claims detected.

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	7.9 years old Registered history	CLEAR
Web archive	Archived since 2018 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YR2	NOTED

The page as captured

<https://mcas.me/>



What mcas.me 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 2018.
- 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.

The website is a Hospital Management System product site presenting healthcare administration modules for outpatient, inpatient, laboratory, dietary, radiology, operating-theatre, bed-occupancy, and doctor-related workflows. Its apparent business model is the provision of hospital management software, supported by product information, a contact channel, and an account-login route.

Scam/Impersonation Risk

The site has a **critical sensitive-interaction risk posture** because external reputation telemetry records a confirmed blacklist condition and multiple malicious detections. This is a material contradiction to the otherwise benign software presentation and warrants treating login, credential submission, and other sensitive interactions as unsafe. No conflicting legal-entity names, phishing form, or confirmed brand impersonation were observed in the supplied page analysis; the risk determination is instead driven by the external threat and blacklist findings. One major web-safety check did not classify the site as malicious, but that isolated result does not offset the broader confirmed detections.

EVIDENCE

- Domain registration records show creation on 2018-09-13, with an age of 7.94 years, through GoDaddy.com, LLC.
- Historical records span 2018-10-10 through 2025-05-03, representing 8 years tracked.
- External reputation telemetry recorded 12 malicious detections, 1 suspicious detection, and blacklist status; Fortinet, Kaspersky, and Sophos were among the flagged security vendors.

Regulatory Verification Notes

The homepage presents a Hospital Management System with named OPD, IPD, laboratory, diet, radiology, operating-theatre, procedure, and bed-occupancy registers. The About area contains generic “About your Firm” wording, placeholder card text, and “Powerd By : Golf Soft,” while the available content does not state a legal entity, licensing basis, or applicable authorization. This is a significant transparency gap for a healthcare-software supplier, although the absence of a stated license is a verification issue rather than independent proof of fraud. The site's real-world operator remains unverified, and the available third-party broker dataset produced no match.

EVIDENCE

- The homepage is titled “Hospital Management System” and contains one contact form plus a Login link.
- The About and service areas contain generic placeholder text, including repeated “Card title” content and “Some quick example text.”
- Hosting is recorded on AS394695, PUBLIC-DOMAIN-REGISTRY - PDR, US.
- Transport encryption uses a DV TLS certificate issued by YR2, valid to 2026-10-04T04:27:29+00:00.

What to Verify Next

Before any sensitive engagement, the prospective customer should independently confirm the legal entity behind the software and establish whether any healthcare-sector registration, authorization, data-processing commitment, or contractual support obligation applies. The login route should not be used until the organization has confirmed the official service endpoint, account-recovery process, and support contacts through an independently obtained business channel. Any procurement should also require written terms covering data handling, service ownership, incident notification, and termination or export of hospital records.

EVIDENCE

- The site's About page provides generic firm information rather than a clearly identified operating entity.
- The site's contact page supplies a web form that can be used only as an initial channel for independent business verification.
- The homepage exposes an account-login route despite limited supplier-identification content.

Summary Verdict

The overall posture is critical, with the website unsuitable for credentials, account access, financial activity, or other sensitive interaction on the evidence available. Its apparent software purpose and technically functioning

presentation do not overcome the confirmed external threat contradiction, while operator identity remains unverified.

Infrastructure Integrity

The site resolves directly to hosting infrastructure associated with PUBLIC-DOMAIN-REGISTRY - PDR in India, with no detected CDN edge and a likely origin address. This configuration provides limited protective mitigation; valid transport encryption improves connection security but does not establish the legitimacy of the operator or the safety of the application.

Closing Assessment

Sensitive engagement should be deferred unless independent organizational, contractual, and technical validation establishes that the service is operated by a legitimate and accountable healthcare-software provider.

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

- The public registration record for this domain is incomplete.
Registration and ownership rule:KF_WHOIS_INCOMPLETE
- 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
- 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	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 mcas.me.

- The request stayed on mcas.me. It was not redirected to another domain. CLEAR
- Registration is published under GoDaddy.com, LLC. CLEAR
- The registration is paid up to 2026-09-13. NOTED
- The earliest public archive of this site is from 2018-10-10. CLEAR
- It is hosted on PUBLIC-DOMAIN-REGISTRY, from a server in IN. NOTED

Domain intelligence

Registrar	GoDaddy.com, LLC
Hosting	PUBLIC-DOMAIN-REGISTRY - PDR, US
Country	IN
Server IP	103.53.40.15
Name servers	Not available
SSL issuer	YR2
SSL expiry	2026-10-04
Domain age	7.94 years (continuous registration)
Domain expiry	2026-09-13
Archive first seen	2018-10-10
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 mcas.me 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.