

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

metamask.ro

Verdict

0

OUT OF 100

CRITICAL RISK

metamask.ro 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 2026-08-20 by automated analysis. Classification confidence 55%.

What this site appears to be

The provided HTML is an empty page (<head></head><body></body>) with no text, links, forms, scripts, or metadata.

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	19 flagged it VirusTotal	RISK
Google Safe Browsing	Listed as unsafe Google	RISK
Abuse reports on the host	72% confidence AbuseIPDB, 21 reports; shared hosting inflates reports	RISK
Domain age	1.7 years old Registered history	CLEAR
Web archive	Archived since 2024 Public history exists	CLEAR
Certificate	Encrypted connection Issued by Encryption Everywhere DV TLS CA - G2	NOTED

The page as captured

https://metamask.ro/



What metamask.ro served when TrustSniffer captured it on 2026-08-20. 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 2024.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

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

The website currently presents visitors with a completely blank page and provides no visible text, links, forms, metadata, or interactive functionality; its intended purpose and business model therefore cannot be established from the site itself.

Scam/Impersonation Risk

Confirmed external threat contradictions are present. Multiple reputation systems identify the domain as malicious or blacklisted, including a Google Safe Browsing malicious result and 19 malicious detections from 25 evaluated security engines, with Google, Kaspersky, and Sophos among the flagged providers. This convergence materially outweighs the absence of visible phishing forms or brand-impersonation content in the captured page. The available evidence does not establish a specific impersonation or phishing mechanism, but it supports a critical-risk assessment for sensitive interaction.

EVIDENCE

- The domain is blacklisted by Google Safe Browsing and external blacklist sources; the Google result identifies a social-engineering threat.
- Security-engine evaluation recorded 19 malicious and 1 suspicious detection out of 25 evaluated results.
- The hosting IP, 64.190.63.222, has 21 abuse reports with a confidence score of 72; the reports apply to shared SEDO infrastructure rather than being uniquely attributed to this domain.

Regulatory Verification Notes

The site does not provide a substantive legal, corporate, licensing, or governance disclosure because the captured homepage contains no content from which an operator or regulated status can be identified. This is a transparency and verification gap, not independent proof of unlawful operation; however, the operator identity remains unverified and the confirmed external threat findings prevent the site from being treated as a legitimate regulated service. No matching broker-reputation record was identified in the available third-party context, but that absence is not a regulatory determination.

EVIDENCE

- WHOIS records identify ICI - Registrar and a creation date of 2025-11-20; the domain is approximately 1.68 years old according to reconciled registration-continuity analysis.
- The site's transport encryption uses a DV certificate issued by Encryption Everywhere DV TLS CA - G2, valid to 2026-09-20.
- No license claim, license number, or licensing authority is presented in the available site content.

What to Verify Next

Before any sensitive interaction, an independent source should confirm the intended operator, any claimed relationship to a recognizable brand, and—if the service is presented elsewhere as financial or regulated—the applicable authorization directly with the relevant official registry. Official contact details should be obtained through an independently trusted channel rather than from the site, and any investigation should avoid credential entry, payment, wallet connection, or the reuse of passwords.

EVIDENCE

- The homepage has no title, metadata, text, links, forms, or scripts, preventing on-site validation of ownership or service purpose.
- Browser analysis observed 3 external XMLHttpRequests and 2 external POST requests, all classified as non-whitelisted, with no visible form destination to explain them.
- The site generated 3 console errors across 2 successful behavioral runs, while no login form, hidden form, wallet connection, or credential field was observed.

Summary Verdict

The overall posture is critical risk, with the available evidence unsuitable for account access, credential submission, or financial interaction. The operator identity is unverified, and the external threat convergence is

sufficiently strong that the site should not be regarded as a trustworthy service endpoint.

Infrastructure Integrity

The domain resolves to a single likely origin address with no CDN detected, so there is no evident edge-layer separation to mitigate direct exposure. The hosting environment is a shared SEDO platform; its shared nature limits the extent to which the reported IP activity can be attributed specifically to this domain, but the infrastructure provides no basis for reducing the site-level risk assessment.

EVIDENCE

- Served from AS47846, SEDO-AS - SEDO GmbH, DE, using IP address 64.190.63.222.
- Infrastructure resolution identified 1 unique IP, 0 edge IPs, and 1 likely origin IP.
- The certificate is DV-validated, issued by Encryption Everywhere DV TLS CA - G2, and expires 2026-09-20.

Closing Assessment

Prospective users should not conduct sensitive activity on the site; any necessary examination should remain read-only and proceed only through independently verified official channels.

Written analysis generated 2026-08-20 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 made background requests to destinations TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_XHR
- 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
- 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

Signals weighed against the site

- AbuseIPDB: 21 reports on hosting IP 64.190.63.222 (SEDO GmbH, Data Center/Web Hosting/Transit), 72% confidence. The reports are attributed to shared infrastructure, not specifically to this website.

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 metamask.ro.

- The request stayed on metamask.ro. It was not redirected to another domain. CLEAR
- Registration is published under ICI - Registrar. CLEAR
- DNS for this domain is served by sedoparking.com, across 2 name servers. NOTED
- The earliest public archive of this site is from 2024-12-13. CLEAR
- It is hosted on SEDO-AS, from a server in DE. NOTED

Domain intelligence

Registrar	ICI - Registrar
Hosting	SEDO-AS - SEDO GmbH, DE
Country	DE
Server IP	64.190.63.222
Name servers	ns1.sedoparking.com, ns2.sedoparking.com
SSL issuer	Encryption Everywhere DV TLS CA - G2
SSL expiry	2026-09-20
Domain age	1.68 years (continuous registration)
Domain expiry	Not available
Archive first seen	2024-12-13
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 19 flagged AbuseIPDB: 72% confidence, 21 reports Google Safe Browsing: 1 match

About this assessment

A trust score summarises the evidence TrustSniffer could collect about metamask.ro 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/metamask.ro> · assessed 2026-08-20