

Is opsecmod.st safe? TrustSniffer's moderate-trust assessment: 40/100

opsecmod.st

Verdict

40

OUT OF 100

LOW TRUST

opsecmod.st is low-trust and potentially risky.

Several risk patterns were present. Do not send money or personal details until you have verified this business another way.

Sensitive Interaction Risk

Governance Risk

Assessed 2026-10-01 by automated analysis. Classification confidence 75%.

What this site appears to be

Project site for OpSec Mod, a free open-source Fabric mod that blocks server tracking, hides installed mods via spoofing, blocks forced resource packs, and provides account switching and chat/key privacy. Includes downloads, install guide, FAQ, and legal note disavowing affiliation with Mojang.

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	3 flagged it VirusTotal	RISK
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	0% confidence AbuseIPDB, 0 reports; shared hosting inflates reports	CLEAR
Domain age	15 days old Most scam domains are under a year old	RISK
Web archive	Archived since 2026 3 snapshots	CLEAR
Certificate	Encrypted connection Issued by YR2	NOTED

The page as captured

<https://opsecmod.st/>



What opsecmod.st served when TrustSniffer captured it on 2026-10-01. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: less than 1 year (registration continuity).
- Public web-archive history exists since 2026.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

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

This website presents OpSec Mod 26.2, a free open-source Minecraft Fabric modification intended to provide multiplayer privacy controls, including server-tracking protection, mod concealment, resource-pack blocking, account switching, and chat and key privacy.

Scam/Impersonation Risk

The site's content is presented as a software project rather than a payment, investment, or credential-collection service. Its homepage describes specific privacy functions, provides installation guidance, and contains no login form, sensitive form, wallet connection, or obvious payment request; no brand impersonation or conflicting legal identities were identified in the supplied page evidence. However, this benign presentation is outweighed by confirmed external blacklist detections and multiple malicious classifications, creating a material risk that downloaded files or the delivery environment may be unsafe. The site should therefore not be treated as safe for downloading or execution solely because its pages appear technically and editorially coherent.

EVIDENCE

- The homepage describes OpSec Mod 26.2 as a Fabric mod with vanilla spoofing, forced-resource-pack blocking, server-tracking controls, account management, and chat-signature privacy.
- The download and installation content distributes mod files and instructions; the page analysis recorded no login form, hidden form, password submission, wallet connection, or clipboard-hijacking behavior.
- External reputation analysis recorded a confirmed blacklist condition, three malicious detections, and one suspicious detection; the blacklist sources were identified as VT and EXTERNAL_BLACKLIST.
- The domain was registered on 2026-09-16 and is approximately 0.04 years old.

Regulatory Verification Notes

This is not presented as a regulated financial or investment service, and no regulatory authorization is claimed. The legal material includes a disclaimer that the project is not affiliated with Mojang, but the available pages do not independently establish the operator's real-world identity or a responsible corporate entity. That identity and governance uncertainty is a transparency gap rather than, by itself, proof of fraud; in this case, it compounds the separate external threat findings. The site's valid transport encryption confirms connection security, not operator legitimacy or software safety.

EVIDENCE

- The legal and FAQ content includes a non-affiliation disclaimer concerning Mojang.
- The site describes the project as free and open source and shows no obvious monetization or payment request.
- The site's transport encryption uses a DV certificate issued by YR2, valid to 2026-12-15 18:33 UTC.
- Archive records contain 3 snapshots spanning 1 year tracked, from 2026-09-17 to 2026-09-29.

What to Verify Next

Before any download or execution, obtain the project source and release artifacts through an independently authenticated, well-established distribution channel and compare cryptographic hashes against a trusted maintainer-controlled reference. Confirm the maintainer's identity and project ownership through an independent channel, and review the mod's permissions, dependencies, and build provenance in a controlled environment. Any organizational, licensing, or affiliation claim should be checked against the relevant official registry or rights holder rather than accepted from the site alone.

EVIDENCE

- The homepage identifies the software as "Free & Open Source" and offers a current build plus legacy builds.
- The installation material directs users to install the mod with Minecraft Fabric components.
- The supplied analysis found no independent social-domain presence or external links in the site's link graph.

Summary Verdict

The website has a low-trust posture with a high risk of sensitive interaction. Although its pages describe a coherent open-source software project and show no obvious credential-harvesting behavior, confirmed blacklist and malicious-detection signals are decisive, while the operator identity remains unverified.

Infrastructure Integrity

The site is protected by Cloudflare CDN/WAF, which provides a mitigating layer against direct origin exposure but does not establish legitimacy or neutralize the external reputation risk. The observed address was an edge address, and the origin was not visible in this analysis.

Closing Assessment

The appropriate posture is read-only review pending independent validation; downloads, execution, credential submission, and other sensitive interaction should be withheld until the project and its artifacts are separately authenticated.

Written analysis generated 2026-10-01 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

5 findings contributed to this verdict, raised by governance, external reputation, history in the web archive, hosting and network, behaviour in a sandbox.

01 Governance What the site offers, as described on its own pages, limits how high the score can go until more of it can be verified. Governance rule:gov_business_model_cap
02 External reputation Several malware engines flagged this domain. External reputation rule:EXT_BLACKLIST_HIGH
03 History in the web archive The web archive has almost no record of this domain, which fits a site that is new. History in the web archive rule:ARCH_PEN_YOUNG_AND_SPARSE
04 Hosting and network - The domain was registered less than three months ago. - The hosting and network setup shows a moderate level of risk indicators. Hosting and network rule:DNS_NEW_DOMAIN_90D Hosting and network rule:DNS_RISK_MED

05 Behaviour in a sandbox

- A large share of what the page loaded came from other domains.

Behaviour in a sandbox rule:BEHAV_EXTERNAL_RATIO_MODERATE

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 opsecmod.st.

- The request stayed on opsecmod.st. It was not redirected to another domain. [CLEAR](#)
- Registration is published under ST Registry. [CLEAR](#)
- DNS for this domain is served by cloudflare.com, across 2 name servers. [NOTED](#)
- The registration is paid up to 2027-09-16. [NOTED](#)
- The earliest public archive of this site is from 2026-09-17. [CLEAR](#)
- It is hosted on FEMOIT, from a server in SC. [NOTED](#)

Domain intelligence

Registrar	ST Registry
Hosting	FEMOIT - FEMO IT SOLUTIONS LIMITED, GB
Country	SC
Server IP	196.251.107.204
Name servers	clint.ns.cloudflare.com, miki.ns.cloudflare.com
CDN / edge network	Detected (cloudflare)
Resolved IP addresses	1
Edge IP addresses	1
Likely origin IP addresses	0
SSL issuer	YR2
SSL expiry	2026-12-15
Domain age	0.04 years (continuous registration)
Domain expiry	2027-09-16

Archive first seen	2026-09-17
Archive snapshots	3
Reputation	VirusTotal: 3 flagged AbuseIPDB: 0% confidence, 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about opsecmod.st 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/opsecmod.st> · assessed 2026-10-01