

Is noamaddons.com a scam? TrustSniffer's high-risk assessment: 5/100

noamaddons.com

Verdict

5

OUT OF 100

CRITICAL RISK

noamaddons.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 2026-09-22 by automated analysis. Classification confidence 55%.

What this site appears to be	Project website for NoamAddons, a free open-source Fabric mod for Minecraft focused on Hypixel SkyBlock dungeon features. Contains feature descriptions, demos, download links, installation steps and FAQ. No payment flows or credential collection observed.
------------------------------	---

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.

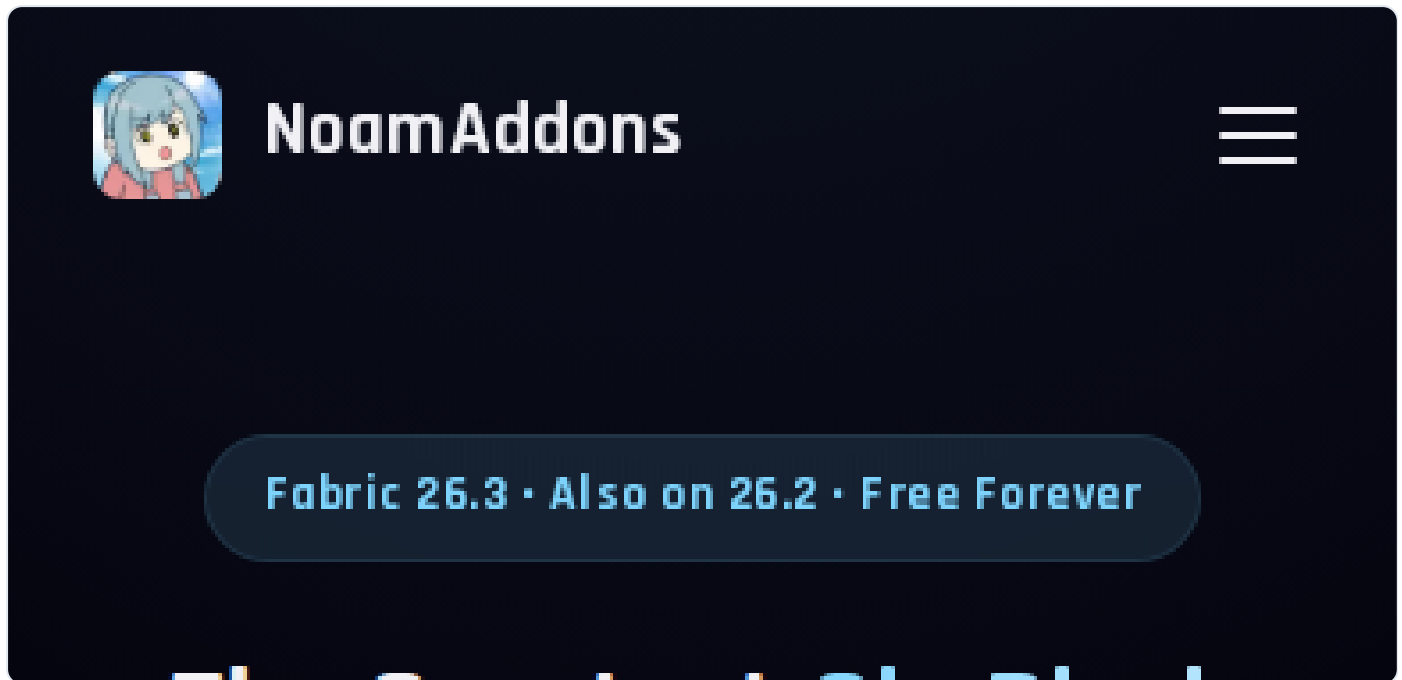
At a glance

The checks that decide most of this verdict.

Malware engines	5 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	4 months old Most scam domains are under a year old	RISK
Web archive	Never archived No public history of this site	WATCH
Certificate	Encrypted connection Issued by YR2	NOTED

The page as captured

<https://noamaddons.com/>



What noamaddons.com served when TrustSniffer captured it on 2026-09-22. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: less than 1 year (registration continuity).
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.
- The operator behind the site could not be independently connected to a real-world brand or person.

Full analysis

Security Alert

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

NoamAddons is a project website presenting a free, open-source Fabric modification for Minecraft's Hypixel SkyBlock, with feature descriptions, demonstrations, download options, installation guidance, and frequently asked questions intended to support mod discovery and installation.

Scam/Impersonation Risk

The site's presented function is a software download rather than a payment, investment, or credential-collection service. Its homepage advertises more than 80 features, including dungeon solvers, M7 dragon timers, automation functions, ESP overlays, custom interfaces, and gameplay enhancements; although no overt phishing form, payment flow, or credential collection was observed, downloadable software creates a supply-chain and execution risk if publisher provenance cannot be independently established. The decisive concern is external: the domain has a confirmed blacklist status and multiple malicious or suspicious detections from external security assessments. No direct brand impersonation or phishing behavior was identified in the supplied

page analysis, but the external detections constitute a material contradiction to the site's otherwise benign presentation.

EVIDENCE

- The homepage describes NoamAddons as a free, open-source Fabric mod and advertises dungeon automation, solvers, timers, ESP overlays, and other gameplay features.
- The homepage and installation flow contain no observed login form, password form, payment mechanism, or external sensitive-data submission.
- External reputation assessment recorded a confirmed blacklist hit together with multiple malicious and suspicious detections.
- Domain registration evidence records creation on 2026-05-19, approximately 0.35 years before assessment.

Regulatory Verification Notes

The supplied site material describes a software project rather than a regulated financial or investment service, so a financial licence is not the relevant validation mechanism. Nevertheless, the operator's real-world identity is not independently verified, and no licensing or formal registration claim is presented in the available site content. That is a disclosure and provenance gap, not by itself proof of fraud; in this case it must be considered alongside the confirmed external reputation contradiction. Transport security and hosting identifiers provide technical attribution, but neither establishes that the publisher is legitimate.

EVIDENCE

- The homepage, installation material, and FAQ identify the offering as a Minecraft mod project and do not present a regulated-service licence or registration claim.
- The domain registrar is Internet Domain Service BS Corp.; the registration record lists the domain as created in 2026 and privately registered.
- The site is served from AS214351 through FEMOIT - FEMO IT SOLUTIONS LIMITED, GB.
- The transport certificate is DV, issued by YR2, and valid to 2026-12-20.

What to Verify Next

Before any installation, an enterprise or user should obtain the project's publisher identity through an independent channel, verify that the download is linked to the genuine maintainer, and scan the mod and any bundled files in a controlled environment. The file should be checked for expected permissions, unexpected executables, credential access, network activity, and consistency with the stated open-source project. Any official repository, release history, or maintainer contact should be reached independently rather than relying solely on links presented by the site.

EVIDENCE

- The homepage provides download and installation instructions that should be matched against an independently verified project repository or release source.
- The FAQ and installation pages provide the stated operating assumptions against which the downloaded package and requested permissions can be compared.
- The site's observed behavior showed no external requests, hidden forms, wallet activity, or clipboard-hijacking activity during testing, but this does not validate the downloaded software itself.

Summary Verdict

The overall posture is critical, with sensitive interaction risk driven by a confirmed external reputation contradiction and unresolved publisher identity. The site's coherent software-project presentation and absence of observed credential or payment collection do not overcome that contradiction.

Infrastructure Integrity

The website is protected by Cloudflare CDN/WAF infrastructure, and all observed addressing was associated with an edge service rather than a directly exposed origin. This reduces direct origin exposure but is only a mitigating infrastructure characteristic; it does not validate the site's operator or downloaded content.

EVIDENCE

- Cloudflare CDN/WAF protection was detected for the website.
- One observed address was classified as a CDN edge address, with no origin candidate identified in the infrastructure analysis.

Closing Assessment

Prospective users should restrict activity to cautious inspection until publisher identity and software provenance have been independently validated, and should not log in, submit credentials, or conduct financial activity through or in connection with the site.

Written analysis generated 2026-09-22 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, 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
- 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 noamaddons.com.

- The request stayed on noamaddons.com. It was not redirected to another domain. [CLEAR](#)
- Registration is published under Internet Domain Service BS Corp.. [CLEAR](#)
- DNS for this domain is served by cloudflare.com, across 2 name servers. [NOTED](#)
- The registration is paid up to 2028-05-19. [CLEAR](#)
- It is hosted on FEMOIT, from a server in SC. [NOTED](#)

Domain intelligence

Registrar	Internet Domain Service BS Corp.
Hosting	FEMOIT - FEMO IT SOLUTIONS LIMITED, GB
Country	SC
Server IP	196.251.107.204
Name servers	LIA.NS.CLOUDFLARE.COM, OSWALD.NS.CLOUDFLARE.COM
SSL issuer	YR2
SSL expiry	2026-12-20
Domain age	0.35 years (continuous registration)
Domain expiry	2028-05-19
Archive first seen	Not available
Archive snapshots	0

About this assessment

A trust score summarises the evidence TrustSniffer could collect about noamaddons.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/noamaddons.com> · assessed 2026-09-22