

Is 1xlite-447029.top a scam? TrustSniffer's high-risk assessment: 0/100

1xlite-447029.top

Verdict

0

OUT OF 100

CRITICAL RISK

1xlite-447029.top 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 2026-08-18 by automated analysis. Classification confidence 70%.

What this site appears to be

Official product page for GreatFireVPN offering circumvention-focused VPN service with a 30-day free trial, subscription plans, multi-platform downloads, referral bonuses and payment guidance (including crypto). Contact and support details are provided.

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	7 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 months old Most scam domains are under a year old	WATCH
Web archive	Archived since 2026 2 snapshots	CLEAR
Certificate	Encrypted connection Issued by WE1	NOTED

The page as captured

<https://1xlite-447029.top/vpn/en/>



What 1xlite-447029.top served when TrustSniffer captured it on 2026-08-18. 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 flagged this site in external intelligence checks, indicating elevated compromise/scam exposure that requires immediate caution.

The website presents itself as GreatFireVPN, a consumer VPN and censorship-circumvention service offering a 30-day trial, subscription plans, multi-platform access, referral benefits, and payment options that include cryptocurrency, cards, and app stores.

Scam/Impersonation Risk

The site carries a **critical sensitive-interaction risk** because external security intelligence recorded malicious detections and confirmed blacklist listings for the assessed domain. This is a direct contradiction to the otherwise coherent GreatFireVPN presentation and materially weakens confidence that the domain is an authentic service endpoint. The assessed domain also does not correspond to the GreatFireVPN branding shown on the homepage, creating a significant provenance concern even though no conflicting legal-entity names or confirmed brand-impersonation finding were recorded. The homepage contains substantial product information and no login or hidden sensitive form was observed, but those content and behavior signals do not offset the external threat detections. Evidence:

- The homepage identifies the service as “GreatFireVPN” while the assessed domain is `1xlite-447029.top`, creating a domain-to-brand provenance mismatch.
- External reputation telemetry recorded 7 malicious detections and a confirmed blacklist hit; a Tier-1 security provider also flagged the domain.
- The domain was registered on 2026-01-27 and is approximately 0.55 years old, according to registration telemetry.
- Historical coverage contains 2 archive snapshots, first seen on 2026-05-19 and last seen on 2026-06-08, with 1 year tracked.

Regulatory Verification Notes

The site provides navigation to About, Legal, Privacy, Terms, FAQ, Payment, and Contact-related content, and presents itself as an anti-censorship NGO-operated service associated with GreatFire.org. That presentation is not independently verified by the available evidence. No license, registration number, or regulatory authority is claimed in the supplied material; for a VPN subscription service this is primarily a disclosure and operator-verification matter rather than standalone evidence of fraud. The combination of an unverified real-world operator identity and serious external reputation findings means the site's legal and organizational disclosures should not be treated as sufficient assurance. Evidence:

- The site's internal navigation includes `/about`, `/legal`, `/privacy`, and `/terms` pages.
- Registration was performed through NameSilo, LLC.
- The site is hosted on AS13335, CLOUDFLARENET - Cloudflare, Inc., US.
- The transport certificate is issued by WE1, uses DV validation, and is valid through 2026-10-22T01:38:28+00:00.

What to Verify Next

Before any sensitive interaction, an organization should independently confirm that GreatFire.org recognizes this domain as an authorized GreatFireVPN endpoint, using contact information obtained from an independently sourced GreatFire.org channel rather than relying solely on the assessed site. The operator's legal entity, service terms, refund commitments, and applicable licensing or registration position should be corroborated through authoritative public records where relevant. Payment should not proceed until the merchant identity and available payment-protection or dispute mechanisms have been independently established. Evidence:

- The About, Legal, Privacy, and Terms pages provide the appropriate locations for operator and contractual review.
- The homepage and product materials identify GreatFire.org as the purported organizational operator, but the available evidence does not independently verify that relationship.
- The site exposes a Payment page and subscription-payment workflow, making merchant-identity and payment-protection checks directly relevant.

Summary Verdict

The overall posture is critical and unsuitable for routine sensitive interaction. The apparent legitimacy of the service presentation is outweighed by confirmed external threat detections and the unresolved connection between the assessed domain and the presented brand.

Infrastructure Integrity

Cloudflare CDN and WAF protection is present, with observed traffic terminating at Cloudflare edge infrastructure rather than a directly exposed origin. This reduces direct origin exposure and is a mitigating technical control only; it does not validate the operator, content provenance, or reputation of the website.

Closing Assessment

Sensitive actions, including credential submission, account access, or payment, should remain suspended unless the domain and operator relationship are independently authenticated through trusted channels.

Written analysis generated 2026-08-18 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 registration record withholds contact details for the operator.
Registration and ownership rule:KF_WHOIS_HIDDEN
- 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

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 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	UNVERIFIED
Identity score	55/100
Identity verification confidence	30%

- 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 1xlite-447029.top.

- The request stayed on 1xlite-447029.top. It was not redirected to another domain. CLEAR
- Registration is published under NameSilo, LLC. CLEAR
- DNS for this domain is served by cloudflare.com, across 2 name servers. NOTED
- The registration is paid up to 2027-01-27. NOTED
- The earliest public archive of this site is from 2026-05-19. CLEAR
- It is hosted on CLOUDFLARENET, from a server in US. NOTED

Domain intelligence

Registrar	NameSilo, LLC
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US
Server IP	2606:4700:3031::ac43:89ab
Name servers	vin.ns.cloudflare.com, coco.ns.cloudflare.com
SSL issuer	WE1
SSL expiry	2026-10-22
Domain age	0.55 years (continuous registration)
Domain expiry	2027-01-27
Archive first seen	2026-05-19
Archive snapshots	2
Reputation	VirusTotal: 7 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about 1xlite-447029.top 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.