

Is 1111365.co a scam? TrustSniffer's high-risk assessment: 0/100

1111365.co

Verdict

0

OUT OF 100

CRITICAL RISK

1111365.co 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

A short multilingual navigation/access selection page (Chinese + English) asking users to choose a connection route (线路 A/线路 B). No forms, no payment requests, and minimal explanatory content.

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.

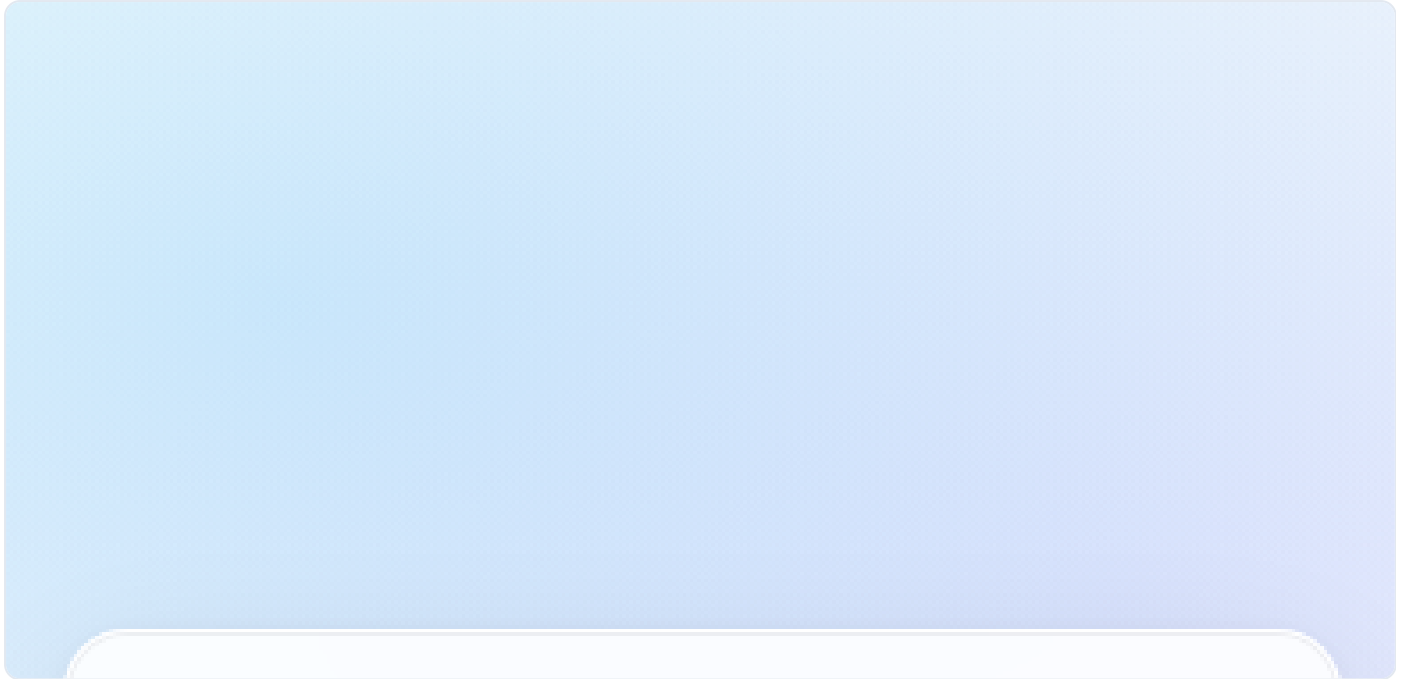
At a glance

The checks that decide most of this verdict.

Malware engines	15 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	12 months old Most scam domains are under a year old	WATCH
Web archive	Archived since 2017 192 snapshots	CLEAR
Certificate	Encrypted connection Issued by WE1	NOTED

The page as captured

<https://1111365.co/>



What 1111365.co 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 2017.
- 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 is a sparse bilingual navigation gateway that asks visitors to choose between two access routes, apparently to direct them to a separate destination rather than provide a substantive product, service, or transaction directly.

Scam/Impersonation Risk

The site presents no visible login form, payment request, or explicit phishing content on its homepage, and no direct brand impersonation was identified in the page content. However, the domain is subject to a confirmed blacklist finding and multiple malicious detections from external security services, creating a material contradiction that outweighs the benign appearance of the gateway page. Runtime activity also included external requests and posts to destinations not identified as trusted, while the final destination behavior was assessed as suspicious. The historical record demonstrates that the domain has existed across multiple years, but that continuity does not establish that the current operator or current content is legitimate.

EVIDENCE

- The homepage contains approximately 130 characters of bilingual navigation text and offers “线路 A (推荐)” and “线路 B (备用),” with no visible login or payment form.
- External reputation assessment recorded 15 malicious detections, a confirmed blacklist status, and two tier-one security vendors flagging the domain.
- Observed runtime behavior included 2 external XHR requests and 2 external POST requests, all classified as non-whitelisted.
- Registration records show creation on 2025-08-26, with a stated domain age of 0.98 years; archival coverage contains 192 snapshots spanning 2017-06-28 to 2026-03-04 across 10 tracked years.

Regulatory Verification Notes

The available site content does not identify a legal entity, licensing authority, registration number, or regulated-service authorization. This is a significant verification gap for any downstream service reached through the gateway, particularly because the operator’s real-world identity remains unverified. The site’s valid transport encryption and identifiable hosting infrastructure confirm technical service configuration only; they do not validate ownership, licensing, or regulatory standing. No broker match was returned in the available third-party reputational context, but that absence is not a legal or licensing determination.

EVIDENCE

- The homepage is labelled “Navigation Page,” has no substantive legal or business description, and contains no stated licence claim or licence number.
- WHOIS identifies DYNADOT LLC as registrar, with the registrant organization recorded as “Super Privacy Service LTD c/o Dynadot.”
- The site is served from AS13335, CLOUDFLARENET - Cloudflare, Inc., US.
- The TLS certificate is issued by WE1 at DV validation level and is valid through 2026-11-14.

What to Verify Next

Before any interaction beyond passive viewing, an independent source should identify the operator responsible for both access routes and confirm whether any service reached through them is authorized in the relevant jurisdiction. Any claimed financial, trading, or account-related service should be checked directly against the applicable regulator’s registry rather than relying on statements reached through this gateway. The route destinations should be examined in an isolated environment, and any request for credentials, software installation, payment, or sensitive data should be rejected unless independently validated through an established offline contact channel.

EVIDENCE

- The homepage supplies route-selection instructions but no legal, licensing, or operator-verification material.
- The available behavioral record identifies external XHR and POST activity associated with the access flow.
- The independent identity-verification status is unverified, with no positive identity signals recorded.

Summary Verdict

The overall posture is **critical trust risk** with a confirmed external threat contradiction. The site's minimal presentation provides insufficient context to offset that finding, and the available evidence does not support treating it as a trustworthy destination for sensitive interaction.

Infrastructure Integrity

Cloudflare CDN/WAF protection provides a mitigating layer against direct exposure of the underlying service, and all observed addresses were Cloudflare edge infrastructure associated with AS13335; the origin server was not observable. This infrastructure reduces some direct hosting exposure but does not establish legitimacy or neutralize the external threat findings.

Closing Assessment

Restrict activity to passive observation and do not use the site for login, credential submission, software installation, payment, or other financial interaction.

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
- A large share of what the page loaded came from other domains.
Behaviour in a sandbox rule:BEHAV_EXTERNAL_RATIO_MODERATE
- The page sent data to a destination TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_POSTS
- 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 1111365.co.

- The request stayed on 1111365.co. It was not redirected to another domain. CLEAR
- Registration is published under DYNADOT LLC. CLEAR
- DNS for this domain is served by cloudflare.com, across 2 name servers. NOTED
- The registration is paid up to 2026-08-26. NOTED
- The earliest public archive of this site is from 2017-06-28. CLEAR
- It is hosted on CLOUDFLARENET, from a server in US. NOTED

Domain intelligence

Registrar	DYNADOT LLC
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US
Server IP	2606:4700:3037::ac43:8ef9
Name servers	JILL.NS.CLOUDFLARE.COM, ROMAN.NS.CLOUDFLARE.COM
SSL issuer	WE1
SSL expiry	2026-11-14
Domain age	0.98 years (continuous registration)
Domain expiry	2026-08-26
Archive first seen	2017-06-28
Archive snapshots	192
Reputation	VirusTotal: 15 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about 1111365.co 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.

