

Is 198348.gl a scam? TrustSniffer's high-risk assessment: 0/100

198348.gl

Verdict

0

OUT OF 100

CRITICAL RISK

198348.gl 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

The page contains only a short error message ('bad request') and no other visible content, links, or forms. No indicators of transactions, accounts, or business operations.

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	13 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	2 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 YE1	NOTED

The page as captured

<https://198348.gl/>

bad request

What 198348.gl 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, Kaspersky, Sophos flagged this site in external intelligence checks, indicating elevated compromise/scam exposure that requires immediate caution.

198348.gl currently presents only a minimal error response stating “bad request,” with no visible business description, products, account functions, transaction mechanisms, or operator information; its apparent purpose therefore cannot be established from the accessible page.

Scam/Impersonation Risk

The domain is subject to a confirmed blacklist determination, with malicious detections recorded by multiple external security providers. This is the decisive risk signal and supports a clearly cautionary assessment for sensitive interaction. The page itself does not establish a brand, operator, or business model, so there is no positive site-level identity evidence to offset the external warning. No separate brand-impersonation or conflicting legal-entity finding was identified.

EVIDENCE

- The homepage returns HTTP 400 content consisting only of the text “bad request,” with no links, forms, or operational information.
- External reputation records classify the domain as blacklisted, and the evaluation recorded 13 malicious and 2 suspicious detections.
- The domain was registered on 2026-07-09 and is approximately 0.2 years old, according to the registration record.
- The registration record identifies NICENIC INTERNATIONAL GROUP CO., LIMITED as registrar.

Regulatory Verification Notes

Operator identity remains unverified, and the accessible site provides no meaningful legal, corporate, licensing, or regulatory disclosure. No license claim or license number is present for assessment; this is a material verification gap rather than a standalone determination of fraud. The site’s transport encryption is technically valid, but domain-validation TLS confirms encrypted communication only and does not establish the operator’s identity, authorization, or legitimacy. No broker match was identified in the available third-party reputational context.

EVIDENCE

- The homepage contains no legal notice, terms, company identification, registration detail, license authority, or license number.
- The site’s TLS certificate is DV, issued by YE1, and valid to 2026-12-07.
- The registration record lists NICENIC INTERNATIONAL GROUP CO., LIMITED as registrar and gives a creation date of 2026-07-09.
- The accessible page provides no business model or regulated-service description against which licensing could be assessed.

What to Verify Next

Before any interaction beyond passive observation, an independent authority should establish the real-world operator and confirm any claimed authorization directly with the relevant corporate or financial-services registry. The official support and contact channels should be confirmed through an independently sourced route, and any request for credentials, payment, software installation, or sensitive information should be rejected unless the domain’s status is resolved through trusted external channels.

EVIDENCE

- The homepage exposes no operator identity or contact route that can be independently assessed.
- The page has no login form, sensitive form, transaction flow, or wallet-connection function in the observed content.
- Browser analysis recorded no external requests, wallet activity, hidden forms, or suspicious inline scripts during the available runs.

Summary Verdict

The website has a **critical trust posture**. The confirmed blacklist status, malicious external detections, unverified identity, very limited site content, and recent registration together outweigh the limited technical assurance provided by valid transport encryption. The available evidence does not support treating the domain as a legitimate platform for sensitive interaction.

Infrastructure Integrity

The site resolves directly to infrastructure operated by NetCrafters OU, with no detected CDN or WAF layer and one likely origin address. This provides limited protective mitigation: the service is technically reachable and identifiable at the network layer, but the hosting arrangement does not establish legitimacy and does not offset the external reputation risk.

EVIDENCE

- Hosted on AS203273 through NetCraftersOU - NetCrafters OU, EE.
- The resolved service uses IP address 138.124.60.116 and is associated with country code CH in the technical records.
- No CDN was detected; the infrastructure assessment identified one likely origin IP and zero edge IPs.

Closing Assessment

No login, credential submission, payment, fund transfer, or other sensitive interaction should proceed unless independent identity and authorization checks produce authoritative, contradictory evidence to the current assessment.

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

- 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
- 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	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 198348.gl.

- The request stayed on 198348.gl. It was not redirected to another domain. [CLEAR](#)
- Registration is published under NICENIC INTERNATIONAL GROUP CO., LIMITED. [CLEAR](#)
- DNS for this domain is served by my-ndns.com, across 2 name servers. [NOTED](#)
- The registration is paid up to 2027-07-09. [NOTED](#)
- It is hosted on NetCraftersOU, from a server in CH. [NOTED](#)

Domain intelligence

Registrar	NICENIC INTERNATIONAL GROUP CO., LIMITED
Hosting	NetCraftersOU - NetCrafters OU, EE
Country	CH
Server IP	138.124.60.116
Name servers	NS3.MY-NDNS.COM, NS4.MY-NDNS.COM
SSL issuer	YE1
SSL expiry	2026-12-07
Domain age	0.20 years (continuous registration)
Domain expiry	2027-07-09
Archive first seen	Not available
Archive snapshots	0
Reputation	VirusTotal: 13 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about 198348.gl 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.

