

Is 029many.com a scam? TrustSniffer's high-risk assessment: 0/100

029many.com

Verdict

0

OUT OF 100

CRITICAL RISK

029many.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 2026-08-18 by automated analysis. Classification confidence 70%.

What this site appears to be

403 Forbidden (nginx) server response. Page returned no usable content for analysis.

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	1.9 years old Registered history	CLEAR
Web archive	Archived since 2016 16 snapshots	CLEAR
Certificate	Encrypted connection Issued by YR2	NOTED

The page as captured

https://029many.com/



What 029many.com served when TrustSniffer captured it on 2026-08-18. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: 1 to 3 years (registration continuity).
- Public web-archive history exists since 2016.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

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

The website at 029many.com currently presents no usable service, product, or business proposition to a visitor: the homepage returns a “403 Forbidden” response from nginx, leaving its intended purpose, operating model, and any customer-facing functionality unassessable.

Scam/Impersonation Risk

The site presents a **critical sensitive-interaction risk** because confirmed blacklist signals and multiple malicious detections materially outweigh the limited positive technical indicators. External reputation systems recorded 13 malicious detections and one suspicious detection, with Kaspersky and Sophos among the flagged vendors; the domain is also recorded as blacklisted by two sources. The unavailable homepage, suspicious network classification, one non-whitelisted external request, and substantial post-interaction DOM change further limit confidence that the observed site state is suitable for trusted interaction. No distinct legal-entity inconsistency or brand impersonation was identified, but the available evidence is sufficient to treat login, credential submission, and financial activity as inappropriate.

EVIDENCE

- The homepage returned HTTP 403 with only “403 Forbidden” and “nginx” visible; no usable service content, forms, or identity disclosures were available.
- External reputation telemetry recorded 13 malicious and 1 suspicious detection, including flags from Kaspersky and Sophos; blacklist status was confirmed by two sources.
- Domain registration data records creation on 2024-09-10 and an age of approximately 1.93 years; the archive contains 16 snapshots spanning 2016–2026, with 11 years tracked.

Regulatory Verification Notes

The site’s legal status, operator identity, licensing position, and governance arrangements cannot be assessed from the accessible content because the homepage is unavailable and no legal or identity material was presented. No license claim or license number is visible in the supplied page evidence; this is a verification gap rather than a standalone finding of fraud. Independent identity verification remains incomplete. The available broker-context check produced no match, but that result does not establish licensing or regulatory authorization.

EVIDENCE

- The captured homepage contains no company name, terms, privacy notice, licensing statement, registration number, or other legal disclosure.
- The domain is registered through Gname.com Pte. Ltd.; the registrant and organization fields are privacy-redacted.
- Hosting telemetry identifies AS132839, POWERLINE-AS-AP – POWER LINE DATACENTER, HK; the site’s country field is US.
- The site uses a DV TLS certificate issued by YR2, valid through 2026-10-01T07:55:24+00:00.

What to Verify Next

Before any sensitive interaction, an independent investigator should establish the real-world operator through a trusted offline or separately sourced channel, confirm any claimed authorization directly with the relevant financial or commercial regulator, and validate that the domain is the institution’s independently published official address. The domain and associated infrastructure should also be checked through enterprise malware, DNS, and reputation controls before any connection is permitted from a corporate environment.

EVIDENCE

- The homepage’s HTTP 403 response prevents validation of the site’s stated purpose, ownership, and operating terms.
- No login, password, payment, or wallet form was exposed during the available page and behavior assessment.
- The observed behavior included one non-whitelisted external XHR request, four console errors, and a maximum post-interaction DOM difference of 1,407 elements.

Summary Verdict

The available evidence supports a **critical, non-trustworthy posture** for sensitive use. The site's identity and purpose remain unverified, while confirmed external threat detections and blacklist status establish a level of concern that is not offset by ordinary transport-security or historical signals.

Infrastructure Integrity

The site resolves directly to one likely origin address, with no CDN or WAF detected and no edge-IP layer identified. Its infrastructure is associated with AS132839 and POWERLINE-AS-AP – POWER LINE DATACENTER, HK; this hosting arrangement provides no observed CDN-based mitigation, although infrastructure characteristics alone do not establish malicious intent.

Closing Assessment

Prospective users and enterprise administrators should restrict handling to non-sensitive observation and should not permit login, credential submission, or financial activity unless independent identity, authorization, and security validation produce a clear alternative assessment.

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

 - 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
 - The structure of the page changed sharply while it was loading.
Behaviour in a sandbox rule:BEHAV_DOM_DENSITY_SPIKE
 - Most of what the page loaded came from other domains rather than from this one.
Behaviour in a sandbox rule:BEHAV_EXTERNAL_RATIO_HIGH
 - 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 029many.com.

- The request stayed on 029many.com. It was not redirected to another domain. [CLEAR](#)
- Registration is published under Gname.com Pte. Ltd.. [CLEAR](#)
- DNS for this domain is served by share-dns.com, across 2 name servers. [NOTED](#)
- The registration is paid up to 2027-09-10. [NOTED](#)
- The earliest public archive of this site is from 2016-03-10. [CLEAR](#)
- It is hosted on POWERLINE-AS-AP, from a server in US. [NOTED](#)

Domain intelligence

Registrar	Gname.com Pte. Ltd.
Hosting	POWERLINE-AS-AP - POWER LINE DATACENTER, HK
Country	US
Server IP	107.163.132.17
Name servers	A4.SHARE-DNS.COM, B4.SHARE-DNS.NET
SSL issuer	YR2
SSL expiry	2026-10-01
Domain age	1.93 years (continuous registration)
Domain expiry	2027-09-10
Archive first seen	2016-03-10
Archive snapshots	16
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 029many.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/029many.com> · assessed 2026-08-18