

Is 278787.com a scam? TrustSniffer's high-risk assessment: 0/100

278787.com

Verdict

0

OUT OF 100

CRITICAL RISK

278787.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

Generic Chinese link portal / doorway page listing many popular Chinese sites and categories, with instructions to click routing links to reach a homepage. No forms or financial offerings detected.

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 2013 14 snapshots	CLEAR
Certificate	Encrypted connection Issued by YR1	NOTED

The page as captured

<https://278787.com/>



已通过安全检测

What 278787.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 2013.
- 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.

278787.com is a Chinese-language link portal and doorway page that presents categorized links to popular websites, including news, shopping, banking, entertainment, travel, and other services. Its homepage instructs visitors to select one of several routing links to reach the intended destination, indicating an informational directory or referral-based model rather than a direct financial or commercial service.

Scam/Impersonation Risk

The site has no detected login form, sensitive submission form, wallet interaction, or overt financial solicitation, and the homepage appears to be a generic directory rather than an impersonation of a named brand. However, these benign page characteristics are outweighed by confirmed external threat detections and a **blacklisted** status reported by multiple sources. The site is therefore unsuitable for credentials, account access, downloads, or other sensitive interaction. A separate reputation check returned no malicious result, but that isolated result does not offset the corroborated adverse detections. No identity contradiction, brand impersonation, or page-level phishing form was observed.

EVIDENCE

- The homepage is a generic Chinese-language portal with three routing choices and categorized links; page analysis detected no forms or financial offerings.
- External reputation assessment recorded 13 malicious detections and 2 suspicious detections, with blacklist status confirmed by two sources.
- Interaction testing recorded six non-whitelisted external XHR requests, eight console errors, and a maximum post-interaction DOM difference of 6,914.

Regulatory Verification Notes

The available evidence does not independently verify the real-world operator. The site presents generic copyright wording, but this does not establish a legal entity, regulated status, or accountable business operator. No license claim, licensing authority, or license number is disclosed in the supplied site content; because the homepage presents an informational directory rather than a financial offering, the principal regulatory issue is disclosure and accountability rather than a demonstrated licensing breach. Registration privacy is an administrative limitation and is not, by itself, evidence of misconduct. The historical record also requires careful interpretation: archived captures predate the current registration record, so historical presence should not be treated as proof of continuous control by the present operator.

EVIDENCE

- The domain registration record shows creation on 2024-10-05 and an age of approximately 1.87 years; registrar: Gname.com Pte. Ltd.
- Web archives contain 14 snapshots spanning 2013-08-30 to 2026-05-20, covering 14 tracked years; this predates the current registration record and does not independently establish operator continuity.
- The resolved hosting record identifies AS213802, operated by TF - Tianfeng (Hong Kong) Communications Limited, HK.
- The site's TLS certificate is issued by YR1 with DV validation and is valid to 2026-10-27.

What to Verify Next

Before any non-passive interaction, an enterprise security team should independently confirm that the routing destinations are intentionally operated by the organizations whose names appear in the directory, rather than assuming that the listed brands endorse the portal. The operator should also be required to provide a verifiable legal entity and, if it later presents financial or regulated services, confirm any claimed authorization directly with the relevant regulator. Security controls should block or isolate the domain pending resolution of the external detections, with any necessary review performed through a sandboxed environment and without credential or payment data.

EVIDENCE

- The homepage provides routing links to numerous third-party services but supplies no demonstrated relationship between those services and the portal operator.
- The supplied content identifies the page as an informational link directory and records no license authority or license number.
- Behavioral testing completed two successful runs, while all six observed external XHR requests were non-whitelisted.

Summary Verdict

The overall posture is **critical and cautionary**. The site's simple directory presentation does not overcome the decisive external trust concerns, and the available evidence is insufficient to connect the website to a verified real-world operator. Sensitive interaction should be treated as inappropriate.

Infrastructure Integrity

The site resolves directly to likely origin infrastructure rather than a detected CDN or WAF layer. Hosting is attributed to TF - Tianfeng (Hong Kong) Communications Limited through AS213802, with three likely origin IP addresses identified; this provides no protective intermediary to mitigate exposure or establish legitimacy.

EVIDENCE

- Hosting infrastructure: AS213802, TF - Tianfeng (Hong Kong) Communications Limited, HK.
- The technical sensor resolved the server IP as 128.241.245.117 and identified the server country as US.
- Infrastructure analysis identified 3 unique IP addresses, 0 edge IP addresses, and 3 likely origin IP addresses; no CDN was detected.

Closing Assessment

The appropriate disposition is to defer login, credential submission, downloads, and financial transactions unless independent security review and operator validation materially resolve the identified concerns.

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

- The page made background requests to destinations TrustSniffer does not recognise.

Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_XHR

- 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 278787.com.

- The request stayed on 278787.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 2026-10-05. [NOTED](#)
- The earliest public archive of this site is from 2013-08-30. [CLEAR](#)
- It is hosted on TF, from a server in US. [NOTED](#)

Domain intelligence

Registrar	Gname.com Pte. Ltd.
Hosting	TF - Tianfeng (Hong Kong) Communications Limited, HK
Country	US
Server IP	128.241.245.117
Name servers	A12.SHARE-DNS.COM, B12.SHARE-DNS.NET
SSL issuer	YR1

SSL expiry	2026-10-27
Domain age	1.87 years (continuous registration)
Domain expiry	2026-10-05
Archive first seen	2013-08-30
Archive snapshots	14
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 278787.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/278787.com> · assessed 2026-08-18