

Is 17dh06.com a scam? TrustSniffer's high-risk assessment: 0/100

17dh06.com

Verdict

0

OUT OF 100

CRITICAL RISK

17dh06.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

Short page containing a brand slogan and a classical Chinese poem. No forms, links, or monetization cues visible.

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	16 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	2.6 years old Registered history	CLEAR
Web archive	Archived since 2024 10 snapshots	CLEAR
Certificate	Encrypted connection Issued by WE1	NOTED

The page as captured

https://17dh06.com/CEMD62.html



What 17dh06.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 2024.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

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

This website is a very short informational webpage presenting the slogan “老品牌,值得您信耐!” alongside a classical Chinese poem. It provides no visible forms, links, credential prompts, payment requests, or apparent monetization, and its immediate purpose appears to be static informational presentation rather than an identifiable commercial service.

Scam/Impersonation Risk

A confirmed **blacklist** hit and malicious external detections create a materially elevated risk despite the benign appearance of the visible page. The supplied findings record malicious classifications from multiple external security providers, including Fortinet, Kaspersky, and Sophos. Runtime inspection also observed non-whitelisted external requests and posts, although no login form, hidden sensitive form, wallet connection, cloaking, clipboard manipulation, or brand-impersonation indicator was detected. No conflicting legal-entity names or other identity contradiction was established; however, the confirmed blacklist status remains the decisive risk signal.

EVIDENCE

- External reputation telemetry recorded 16 malicious detections, with Fortinet, Kaspersky, and Sophos among the flagged vendors; the domain was also recorded as externally blacklisted.
- Archived records show 10 snapshots spanning 2024-01-18 through 2026-06-10, covering 3 tracked years.
- The captured page contains 76 characters of visible text, with no forms, internal links, external links, login functionality, or payment solicitation.
- Runtime telemetry recorded 2 external XHR requests and 2 external POST requests, all classified as non-whitelisted.

Regulatory Verification Notes

The site does not present a licensing claim, license number, or clearly identified regulated operator in the supplied content. Its operator identity therefore remains unverified, and the available disclosure is insufficient to establish a responsible legal entity or regulatory status. The absence of a broker match in the supplied third-party dataset is only contextual and does not establish licensing or legitimacy. The domain is registered through Dynadot Inc.; that registration fact does not independently validate the operator.

EVIDENCE

- Registration telemetry records creation on 2025-02-16T05:56:12Z, expiration on 2027-02-16T05:56:12Z, and an age of 1.5 years; registrar: Dynadot Inc.
- Hosting telemetry records AS13335, CLOUDFLARENET - Cloudflare, Inc., US.
- The transport certificate is issued by WE1 at DV validation level and is valid to 2026-10-31T11:46:32+00:00.
- The captured content contains no license authority or license number.

What to Verify Next

Before any sensitive interaction, an independent registry check should confirm whether a legally identifiable operator exists and whether any activity associated with the site requires authorization. Any claimed business relationship, support channel, or ownership information should be confirmed through an independently sourced route rather than relying solely on the webpage. Security teams should also re-check the domain's current reputation and content before allowing authentication, credential submission, or financial use.

EVIDENCE

- Confirm the operator and any claimed authorization through the relevant official corporate and regulatory registries.
- Validate contact and ownership details through an independent, offline or previously trusted channel.
- Reassess current threat detections and page behavior immediately before permitting sensitive activity.

Summary Verdict

The website has a critical trust posture, with the available evidence supporting a sensitive-interaction risk classification rather than a trustworthy-use determination. Its limited informational presentation does not offset

the convergent external security findings and the lack of independently verified identity.

Infrastructure Integrity

Cloudflare CDN/WAF protection is present, and all observed addresses were CDN edge infrastructure rather than an independently observable origin. This provides a mitigating layer against direct origin exposure, but it is a shared protective service and is not evidence that the website itself is legitimate.

Closing Assessment

Prospective users should restrict activity to passive viewing and should not authenticate, submit credentials, or conduct financial activity unless independent identity, authorization, and current security status have first been established.

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 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
 - The page sent data to a destination TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_POSTS
 - A large share of what the page loaded came from other domains.
Behaviour in a sandbox rule:BEHAV_EXTERNAL_RATIO_MODERATE
 - 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 17dh06.com.

- The request stayed on 17dh06.com. It was not redirected to another domain. CLEAR
- Registration is published under Dynadot Inc. CLEAR
- DNS for this domain is served by cloudflare.com, across 2 name servers. NOTED
- The registration is paid up to 2027-02-16. NOTED
- The earliest public archive of this site is from 2024-01-18. CLEAR
- It is hosted on CLOUDFLARENET, from a server in US. NOTED

Domain intelligence

Registrar	Dynadot Inc
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US
Server IP	2606:4700:3033::ac43:9074
Name servers	BRYNNE.NS.CLOUDFLARE.COM, DANE.NS.CLOUDFLARE.COM
SSL issuer	WE1
SSL expiry	2026-10-31
Domain age	2.58 years (continuous registration)
Domain expiry	2027-02-16
Archive first seen	2024-01-18
Archive snapshots	10
Reputation	VirusTotal: 16 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about 17dh06.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.