

Is 025nh.com a scam? TrustSniffer's high-risk assessment: 0/100

025nh.com

Verdict

0

OUT OF 100

CRITICAL RISK

025nh.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

Chinese university research institute site (Law and Economics). Contains lecture listings, faculty names, academic news and course schedules. Appears institutional and informational.

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	8.2 years old Registered history	CLEAR
Web archive	Archived since 2019 10 snapshots	CLEAR
Certificate	Encrypted connection Issued by YR1	NOTED

The page as captured

https://025nh.com/



What 025nh.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: 3 to 10 years (registration continuity).
- Public web-archive history exists since 2019.
- 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 025nh.com presents itself as a Chinese university law-and-economics research institute, offering lecture listings, faculty profiles, academic news, research projects, and course schedules; its apparent purpose is informational and institutional rather than transactional.

Scam/Impersonation Risk

The site's academic presentation contains no visible login, payment, wallet, or sensitive-data form, and observed browser activity showed no external requests, hidden forms, or wallet-drainer behavior. However, these benign page-level characteristics are materially outweighed by confirmed external threat detections and a confirmed blacklist status, including multiple malicious classifications. The homepage also uses “365APP下载” as its title and repeatedly in navigation while presenting university research content, an unexplained branding mismatch that warrants scrutiny, although it is not by itself an identity contradiction. No separate conflicting legal-entity names or direct brand-impersonation finding were observed. The domain should therefore be treated

as unsuitable for credentials, account access, or financial interaction pending independent resolution of the security detections.

EVIDENCE

- The homepage presents law-and-economics lectures, faculty names, academic news, and course schedules, but its title and repeated navigation label are “365APP下载.”
- External security telemetry recorded 15 malicious detections and 1 suspicious detection; the domain is also marked blacklisted by multiple sources.
- The domain was registered on 2018-06-27 and is approximately 8.15 years old; archival records contain 10 snapshots spanning 2019–2026, with 8 years tracked.

Regulatory Verification Notes

The institute introduction claims an affiliation with China University of Political Science and Law and describes the organisation as a university teaching and research institution. That on-page claim is not independently verified by the supplied evidence, and the available material does not establish a licensing or regulatory status. This is a transparency and identity-verification gap rather than a standalone finding of fraud. A separate broker-reputation dataset produced no matching result, which provides no adverse broker-specific signal but also does not validate the university affiliation or website ownership.

EVIDENCE

- The institute-introduction content states that the organisation is a directly affiliated teaching and research institution of China University of Political Science and Law.
- No licence authority or licence number is stated in the supplied site content.
- The site is hosted on AS398823, PEG-LA - PEG TECH INC, US; its TLS certificate is DV-issued by YR1 and valid through 2026-10-31T00:44:47+00:00.

What to Verify Next

An independent route should confirm that the institute, its stated faculty and its lecture archive are listed in the university’s official directory or reached through a separately sourced university domain. Security teams should also obtain a current disposition for the confirmed blacklist and malicious detections before permitting the domain in enterprise environments. Until those checks are resolved, access should remain limited to passive review, with credentials, downloads, payments, and other sensitive interactions prohibited.

EVIDENCE

- The supplied content identifies the claimed university affiliation only within the site’s own institute-introduction material.
- The captured homepage contains no login form, sensitive form, or untrusted form destination.
- The observed browser sessions completed successfully with no external XHR or POST activity and no detected wallet connection.

Summary Verdict

The overall posture is **critical trust risk**. The site has a coherent academic-looking presentation, but the confirmed external threat and blacklist signals create a decisive contradiction that prevents the website from being treated as trustworthy for sensitive interaction. Its real-world operator identity remains unverified.

Infrastructure Integrity

The domain resolves directly to one likely origin address, 38.28.209.21, hosted by PEG-LA - PEG TECH INC in the United States on AS398823, with no detected CDN or WAF. The valid DV certificate provides transport encryption only and does not establish operator legitimacy or offset the external reputation risk.

Closing Assessment

Enterprise controls should block or quarantine sensitive interaction with the domain until independent institutional confirmation and security-detection remediation have been completed.

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, 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
 - 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 025nh.com.

- The request stayed on 025nh.com. It was not redirected to another domain. CLEAR
- Registration is published under NameSilo, LLC. CLEAR
- DNS for this domain is served by dnsowl.com, across 3 name servers. NOTED
- The registration is paid up to 2027-06-27. NOTED
- The earliest public archive of this site is from 2019-08-18. CLEAR
- It is hosted on PEG-LA, from a server in US. NOTED

Domain intelligence

Registrar	NameSilo, LLC
Hosting	PEG-LA - PEG TECH INC, US
Country	US
Server IP	38.28.209.21
Name servers	NS1.DNSOWL.COM, NS2.DNSOWL.COM, NS3.DNSOWL.COM
SSL issuer	YR1
SSL expiry	2026-10-31
Domain age	8.15 years (continuous registration)
Domain expiry	2027-06-27
Archive first seen	2019-08-18
Archive snapshots	10
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 025nh.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.