

Is 99yh4.com a scam? TrustSniffer's high-risk assessment: 0/100

99yh4.com

Verdict

0

OUT OF 100

CRITICAL RISK

99yh4.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 2026-08-21 by automated analysis. Classification confidence 55%.

What this site appears to be

Chinese-language academic department homepage (Electrical Engineering) containing navigation, news, announcements, program and lab information. No forms or financial solicitations 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	14 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	8.1 years old Registered history	CLEAR
Web archive	Archived since 2018 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YR2	NOTED

The page as captured

https://99yh4.com/



What 99yh4.com served when TrustSniffer captured it on 2026-08-21. 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 2018.
- 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 is a Chinese-language informational page presented as an electrical engineering academic department, with sections for institutional overview, faculty, laboratories, undergraduate programs, student administration, admissions, announcements, and departmental news. Its apparent business model is educational and informational rather than commercial, although the site's naming and external security reputation warrant treating its authenticity with substantial caution.

Scam/Impersonation Risk

A confirmed **blacklist** condition and multiple external malicious detections create a material risk that the domain is compromised, misused, or otherwise unsafe despite its benign academic presentation. The homepage contains no login form, payment mechanism, wallet connection, or financial solicitation, and no confirmed brand impersonation or conflicting legal identity was established; however, the security detections take precedence over the page's low-risk informational appearance. The mismatch between an apparently institutional academic

homepage and the title “bt365官方网站” is an additional authenticity concern because it is not readily consistent with the stated departmental content.

EVIDENCE

- The homepage presents electrical engineering news, program information, laboratories, admissions, and student-management content, with no forms or financial solicitation detected.
- The homepage title is “bt365官方网站,” while the visible navigation and article content describe an electrical engineering department.
- External security assessment recorded 14 malicious and 2 suspicious detections from 21 evaluated results, with Kaspersky and Sophos among the flagged vendors; a confirmed blacklist condition was also recorded.
- Domain registration telemetry shows creation on 2018-07-03T08:22:51Z, with an age of 8.14 years and expiration on 2027-07-03T08:22:51Z.

Regulatory Verification Notes

The available page content is consistent with an academic department, but the real-world operator remains unverified. No financial licence, registration number, or regulated-service claim appears on the reviewed page; this is a verification gap rather than standalone proof of fraud. The page also lacks a clear structured identity disclosure linking the domain to a named educational institution, while its reputational indicators are materially adverse. A page-authority signal was mid-range, but that signal does not offset the confirmed security findings or establish legitimacy.

EVIDENCE

- The homepage contains departmental sections for “学院概况,” undergraduate electrical engineering and automation programs, laboratories, faculty, admissions, and notices.
- The reviewed page contains no licence claim, licence number, or financial-service disclosure.
- Transport security is provided by a DV certificate issued by YR2, valid to 2026-10-11T03:12:46+00:00.
- Historical records identify first observation on 2018-08-06T12:09:00Z and last observation on 2026-02-16T17:26:29Z, covering 9 tracked years.

What to Verify Next

Before any sensitive interaction, an institution that operates the relevant academic department should be confirmed through an independently sourced official university directory or offline institutional contact route, rather than through contact details supplied by the domain alone. The domain should not be used for credential submission, account authentication, financial activity, downloads, or other sensitive transactions unless the operator has been independently authenticated and the security detections have been resolved by the responsible institution.

EVIDENCE

- The homepage contains no login form, hidden form, sensitive form, or external password submission.
- Two behavioral observation runs completed successfully, with zero external XHR or fetch requests recorded.
- No wallet provider, wallet connection, clipboard-write activity, or wallet-drainer behavior was detected during observation.

Summary Verdict

The overall posture is critical and unsuitable for sensitive interaction. The site's academic presentation does not overcome the confirmed adverse security reputation, and the operator's identity is not independently verified. Passive viewing may be less exposed than active use, but the domain should not be treated as a trusted institutional endpoint.

Infrastructure Integrity

The site resolves directly to hosting infrastructure rather than a detected CDN or WAF edge, with four likely origin IP candidates and no trusted CDN identified. This reduces the mitigating value normally associated with managed edge protection; infrastructure characteristics alone do not establish who operates the website.

EVIDENCE

- Hosting is identified as PEG-LA - PEG TECH INC, US, on AS398823.
- The resolved infrastructure is in the United States, with 4 unique IPs and 4 likely origin IPs.
- No CDN was detected and edge IP count was 0.
- The site's TLS certificate is DV, issued by YR2, and expires at 2026-10-11T03:12:46+00:00.

Closing Assessment

The appropriate action is to restrict the domain to passive, non-sensitive observation while independently confirming the legitimate institutional endpoint through an official channel; credential, financial, download, and authentication activity should remain off-limits pending that confirmation.

Written analysis generated 2026-08-21 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

- 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

- 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 99yh4.com.

- The request stayed on 99yh4.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 2027-07-03. [NOTED](#)
- The earliest public archive of this site is from 2018-08-06. [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	140.188.179.151
Name servers	NS1.DNSOWL.COM, NS2.DNSOWL.COM, NS3.DNSOWL.COM
SSL issuer	YR2
SSL expiry	2026-10-11
Domain age	8.14 years (continuous registration)
Domain expiry	2027-07-03
Archive first seen	2018-08-06

Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 14 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about 99yh4.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/99yh4.com> · assessed 2026-08-21