

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

aqhygg.com

Verdict

0

OUT OF 100

CRITICAL RISK

aqhygg.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 2026-08-19 by automated analysis. Classification confidence 55%.

What this site appears to be

Chinese-language local government / 人大 (people's congress) news page for Qixingguan District, heavy on meeting reports, notices, and representative activities. Footer shows site registration and copyright.

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 2013 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YR2	NOTED

The page as captured

<https://aqhygg.com/>



What aqhygg.com served when TrustSniffer captured it on 2026-08-19. 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 2013.
- 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 portal presenting local-government and people's-congress news, meeting reports, public notices, representative activities, and related civic material for Qixingguan District. Its apparent operating model is public-information publishing rather than direct financial or credential-based user interaction, although the homepage title and surrounding presentation are not fully consistent with that apparent purpose.

Scam/Impersonation Risk

The site presents a **critical sensitive-interaction risk** because external security intelligence recorded confirmed malicious detections and blacklist listings. This is materially more significant than the benign appearance of the homepage: the page contains government-style news content, but that content does not neutralize the domain-level reputation findings. No distinct legal-entity identity contradiction or confirmed brand-impersonation finding is recorded in the supplied assessment; nevertheless, the confirmed blacklist and

malicious-detection signals require a security-forward posture. The domain's historical presence also does not establish that its current content or operator is trustworthy.

EVIDENCE

- External reputation checks recorded 15 malicious detections and 1 suspicious detection; two major security vendors were among the flagged sources.
- The domain was recorded as listed by external blacklist sources, while the Google Safe Browsing result was not malicious.
- The homepage contains the title “28365365体育备用网址” alongside Qixingguan District people's-congress news and notices, creating an incongruous content-presentation signal.
- Archive records show 7 snapshots spanning 2013–2026, covering 14 years of tracked history.

Regulatory Verification Notes

The available page content resembles a local-government news portal and includes footer registration and copyright material, but the supplied evidence does not independently verify the real-world operator or establish an official connection to Qixingguan District. No financial-service license, licensing authority, or registration number is presented in the available material; for an informational site this is a disclosure gap rather than standalone proof of fraud, but any regulated or transactional use would require separate confirmation. The domain is registered through NameSilo, LLC, and its valid transport encryption provides technical protection only; neither fact verifies legal identity or public-sector affiliation.

EVIDENCE

- The homepage publishes Chinese-language meeting reports, public notices, poverty-relief and civic-affairs material, and people's-congress representative activities.
- The site footer displays registration and copyright information, but the supplied content does not provide an independently verifiable operating entity or financial-license reference.
- The domain was registered on 2018-06-25 and is recorded as approximately 8.16 years old; registrar: NameSilo, LLC.
- The site uses a DV TLS certificate issued by YR2, valid through 2026-10-30.

What to Verify Next

Independent confirmation should be obtained from an official Qixingguan District or relevant municipal-government directory before treating the site as an official public-information channel. Any request to authenticate, submit credentials, transfer funds, install software, or interact with a financial service should be declined unless the domain, operator, and purpose have been confirmed through an independently sourced channel. Where regulated activity is asserted, the responsible entity and authorization should be checked directly with the applicable regulator.

EVIDENCE

- The homepage has no login form, hidden form, or sensitive form in the observed capture.
- The observed page had zero external XMLHttpRequests and zero wallet-connection or wallet-sensitive runs.
- The site's behavior analysis recorded two successful runs with no detected cloaking, clipboard hijacking, suspicious inline scripts, or hidden forms.

Summary Verdict

The website should be treated as an unverified and materially unsafe domain for sensitive interaction. Its informational appearance is outweighed by confirmed external malicious detections and blacklist status, and the available evidence does not independently establish the operator's identity or official affiliation.

Infrastructure Integrity

The site resolves directly to a single likely origin rather than a CDN edge, with no trusted CDN detected. Hosting is provided by PEG-LA - PEG TECH INC in the United States on AS398823; this infrastructure supplies no meaningful protective mitigation against the domain-level reputation concerns.

EVIDENCE

- Served from AS398823, PEG-LA - PEG TECH INC, US.
- Infrastructure records show 1 unique IP, 0 edge IPs, and 1 likely origin IP.
- No CDN was detected, and the infrastructure record identifies no trusted CDN provider.

Closing Assessment

Passive viewing of non-sensitive material is the only proportionate use indicated by the available evidence; credentials, financial activity, downloads, and other consequential interactions should remain off-limits unless independent authenticity checks produce clear confirmation.

Written analysis generated 2026-08-19 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 aqhygg.com.

- The request stayed on aqhygg.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 2027-06-25. NOTED
- The earliest public archive of this site is from 2013-04-04. 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	38.28.209.10
Name servers	NS1.DNSOWL.COM, NS2.DNSOWL.COM, NS3.DNSOWL.COM
SSL issuer	YR2
SSL expiry	2026-10-30
Domain age	8.16 years (continuous registration)
Domain expiry	2027-06-25
Archive first seen	2013-04-04

Archive snapshots	Not counted (archive lookup incomplete)
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 aqhygg.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/aqhygg.com> · assessed 2026-08-19