

Is 3158-zs.com a scam? TrustSniffer's high-risk assessment: 0/100

3158-zs.com

Verdict

0

OUT OF 100

CRITICAL RISK

3158-zs.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 75%.

What this site appears to be

County-level government website (兴安县人民政府) providing news, announcements, government documents, public service links and contact details. Content is administrative and informational in Chinese.

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 2009 768 snapshots	CLEAR
Certificate	Encrypted connection Issued by YR1	NOTED

The page as captured

No screenshot is retained for this report.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: 3 to 10 years (registration continuity).
- Public web-archive history exists since 2009.
- 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 presents itself as a Chinese county-level government and public-service portal, displaying local news, government notices, policy information, departmental updates, public-service links, and contact details; however, its page title refers to “365滚球网址,” creating a material inconsistency between the apparent government presentation and the site’s visible identity.

Scam/Impersonation Risk

The site carries a confirmed **blacklist** signal, with external threat intelligence recording 14 malicious detections and one suspicious detection, including detections from Kaspersky and Sophos. This is a material contradiction that outweighs the otherwise administrative and apparently non-monetized page content. The homepage contains no login form, sensitive form, wallet connection, suspicious external submission, or detected cloaking behavior, but those benign observations do not neutralize the external threat findings or the inconsistent page title. No distinct legal-entity identity contradiction or confirmed brand-impersonation finding is established in the supplied evidence.

EVIDENCE

- External reputation data recorded 14 malicious detections and 1 suspicious detection for the site; Kaspersky and Sophos were among the flagged vendors.
- The homepage is categorized as a government/public-service page, while its visible title is “365滚球网址,” an inconsistency in the site’s presentation.
- The homepage contained no login form, sensitive form, hidden form, wallet connection, or external password-submission destination.

Regulatory Verification Notes

The available page content is consistent with a county government information portal, but the real-world operator remains unverified. The supplied evidence does not establish a licensing authority, registration number, or regulated-entity status. This is a regulatory and identity-verification gap rather than a standalone finding of fraud. The domain’s registration privacy is an administrative limitation; it should not be treated as independent proof of wrongdoing. No matching broker signal was identified in the available third-party context.

EVIDENCE

- The homepage publishes government news, public notices, departmental activity, policy-related material, and public-service information in Chinese.
- The domain was registered through NameSilo, LLC on 2018-07-09 and is approximately 8.12 years old.
- The site's transport certificate is issued by YR1, uses DV validation, and is valid through 2026-11-02.
- No licensing authority or license number is presented in the supplied business-model and page-disclosure evidence.

What to Verify Next

Before any sensitive interaction, an institution should confirm the site's official domain through an independently sourced government directory or offline government contact, compare the domain with the relevant county administration's published web presence, and obtain independent confirmation of the responsible organization. Any request for credentials, payment, document submission, or downloads should remain suspended until those checks and an endpoint-security review are complete.

EVIDENCE

- The homepage offers government contact details and departmental links that can be checked against independently sourced official records.
- The page contains no sensitive submission form, so any later request for credentials or personal information would represent a change in the observed interaction profile.
- The site's externally reported malicious detections and blacklist status require independent confirmation before sensitive use.

Summary Verdict

The overall posture is **critical trust risk**, with the site unsuitable for sensitive interaction based on the convergence of confirmed external threat findings and inconsistent identity presentation. The government-style content and stable technical behavior are insufficient to establish legitimacy or support normal account, credential, or financial use.

Infrastructure Integrity

The site resolves directly to a single US hosting endpoint operated by PEG-LA - PEG TECH INC, on AS398823, with no detected CDN or WAF layer and no separate edge-IP layer. Its TLS certificate is valid, which supports encrypted transport but does not establish the legitimacy of the operator or the safety of the hosted content.

Closing Assessment

The appropriate institutional action is to restrict use to non-interactive observation, block sensitive transactions and credential submission, and require independent organizational verification before any broader engagement.

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

- 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 3158-zs.com.

- The request stayed on 3158-zs.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 2027-07-09. [NOTED](#)
- The earliest public archive of this site is from 2009-05-13. [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	38.173.155.230

Name servers	NS1.DNSOWL.COM, NS2.DNSOWL.COM, NS3.DNSOWL.COM
SSL issuer	YR1
SSL expiry	2026-11-02
Domain age	8.12 years (continuous registration)
Domain expiry	2027-07-09
Archive first seen	2009-05-13
Archive snapshots	768
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 3158-zs.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/3158-zs.com> · assessed 2026-08-18