

Is 021bag.com a scam? TrustSniffer's high-risk assessment: 0/100

021bag.com

Verdict

0

OUT OF 100

CRITICAL RISK

021bag.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 2026-08-17 by automated analysis. Classification confidence 70%.

What this site appears to be

Local education bureau website (韩城教育网) containing news, notices, policy documents, public service links, contact details and affiliated links to government and education portals.

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	8.2 years old Registered history	CLEAR
Web archive	Archived since 2015 9 snapshots	CLEAR
Certificate	Encrypted connection Issued by YR1	NOTED

The page as captured

https://021bag.com/



What 021bag.com served when TrustSniffer captured it on 2026-08-17. 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 2015.
- 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 local education-bureau and public-service portal, offering education news, government notices, policy documents, departmental information, public-service links, consultation details, and contact information; however, its homepage also prominently repeats “365APP下载” and references a 365APP domain-change notice, creating a material mismatch between the apparent public-sector purpose and the site’s visible branding.

Scam/Impersonation Risk

The site has a **confirmed high-risk reputation contradiction**: external security intelligence records the domain as blacklisted, with 14 malicious detections and one suspicious detection, including alerts from Kaspersky and Sophos. This materially outweighs the benign-looking education content and the absence of visible login forms, payment flows, or solicitation. The repeated “365APP下载” branding on a page otherwise framed as a government education portal is an additional contact-and-identity warning, although the supplied evidence does

not establish two conflicting legal-entity names or confirmed brand impersonation. The domain's age and archive presence indicate persistence, but do not neutralize the current threat detections.

EVIDENCE

- The homepage displays local education news, departmental functions, public notices, and policy documents while also repeating “365APP下载” and referring to a 365APP new-domain announcement.
- External reputation checks recorded 14 malicious detections, one suspicious detection, and a blacklist hit; Kaspersky and Sophos were among the flagged vendors.
- The domain was registered in 2018 and is approximately 8.15 years old.
- Archive records contain 9 snapshots spanning 2015–2025, covering 11 tracked years.

Regulatory Verification Notes

The available page structure resembles a public education authority, with sections for institutional functions, leadership, public disclosure, planning, finance, project construction, policy documents, and public services. That presentation is not sufficient to independently verify that the current domain is operated by the represented authority, and identity verification remains unresolved. No third-party broker match was identified. The site's transport security is technically present, but a domain-validated certificate confirms encrypted transport only; it does not validate the operator or the institutional claims.

EVIDENCE

- The homepage contains institutional sections including “部门职能” (departmental functions), “领导介绍” (leadership introduction), “政务公开” (government disclosure), and “机构概况” (organizational overview).
- The site's hosting infrastructure is identified as AS398823, PEG-LA - PEG TECH INC, US.
- The TLS certificate is issued by YR1, uses DV validation, and is valid through 2026-10-30.
- The available content identifies the site as an education and public-service portal but does not independently connect the domain to a verified real-world operator.

What to Verify Next

Before any sensitive interaction, the represented education authority should be contacted through an independently sourced government channel to confirm that 021bag.com is an authorized domain. Any linked application, download, redirect, or request for credentials should be validated separately rather than trusted solely because it appears within the portal. If the domain cannot be confirmed through an official offline or independently obtained channel, activity should remain limited to non-interactive viewing and the domain should be reported to the relevant institutional security contact.

EVIDENCE

- The page analyzer classified the site as a local government or education public-service page and found no commercial transaction or investment solicitation.
- Behavioral testing found no login form, hidden sensitive form, wallet connection, external POST activity, or clipboard-hijacking behavior.
- The homepage contains a visible domain-change notice associated with the 365APP branding, which should be confirmed directly with the purported authority.
- The site's contact and consultation functions provide a potential verification route, but those details should be independently corroborated.

Summary Verdict

The overall posture is **critical and unsuitable for sensitive interaction**. The apparent public-service presentation does not overcome the confirmed external threat and blacklist contradictions, while the real-world operator remains unverified. The available evidence supports treating the domain as potentially compromised, repurposed, or otherwise unsafe for credentials, account access, downloads, or financial activity.

Infrastructure Integrity

The site resolves directly to a single likely origin endpoint, with no CDN or WAF detected and no edge-layer infrastructure identified. This provides no meaningful protective mediation between visitors and the hosting environment; the infrastructure should therefore be treated as a technical hosting fact, not as evidence of legitimacy.

EVIDENCE

- Hosted by PEG-LA - PEG TECH INC, US, on AS398823.
- The resolved address is 38.28.209.1 in the United States.
- No CDN was detected; one likely origin IP and zero edge IPs were identified.

Closing Assessment

Sensitive interaction should be suspended unless the domain is independently confirmed by the represented education authority and any subsequent destination or download is separately validated.

Written analysis generated 2026-08-17 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 021bag.com.

- The request stayed on 021bag.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 2015-04-27. [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	38.28.209.1

Name servers	NS1.DNSOWL.COM, NS2.DNSOWL.COM, NS3.DNSOWL.COM
SSL issuer	YR1
SSL expiry	2026-10-30
Domain age	8.15 years (continuous registration)
Domain expiry	2027-06-25
Archive first seen	2015-04-27
Archive snapshots	9
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 021bag.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/021bag.com> · assessed 2026-08-17