

Is 886ko.com a scam? TrustSniffer's high-risk assessment: 0/100

886ko.com

Verdict

0

OUT OF 100

CRITICAL RISK

886ko.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 2026-08-20 by automated analysis. Classification confidence 75%.

What this site appears to be

County-level news portal (郸城县委门户网站) publishing local government notices, community news, culture, education, and service information. Contact phone and email provided; technical support credited to a local vendor.

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	12 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 2019 314 snapshots	CLEAR
Certificate	Encrypted connection Issued by YR2	NOTED

The page as captured

<https://886ko.com/>



What 886ko.com served when TrustSniffer captured it on 2026-08-20. 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

Sophos flagged this site in external intelligence checks, indicating elevated compromise/scam exposure that requires immediate caution.

The website presents itself as a county-level Chinese government news and public-information portal, publishing local notices, community news, education, culture, public-service information, and event coverage under the attribution “郸城县委门户网站” and “郸城县委宣传部主办.” Its apparent business model is informational and editorial rather than financial or transactional, although the domain and page metadata do not consistently support that presentation.

Scam/Impersonation Risk

The site’s visible content is a local-government news portal with no login form, sensitive-data form, wallet connection, or observed external posting activity, and the page analyzer identified no direct deception indicators. However, these benign page characteristics are outweighed by confirmed external threat detections: twelve malicious and two suspicious detections were recorded, a tier-one security provider flagged the site, and the domain appears on external blacklists. The homepage’s unrelated metadata title, “www.bte365.com,” also creates a material coherence problem between the domain, page identity, and presented government attribution.

The available evidence does not establish a specific impersonated brand or conflicting legal identities, but the combined reputation findings justify treating the site as unsuitable for sensitive interaction.

EVIDENCE

- External reputation assessment recorded 12 malicious detections and 2 suspicious detections, with a tier-one security vendor among the flagging sources.
- The assessed domain was marked as present on external blacklists; the major safe-browsing result supplied separately was not malicious.
- The homepage displays a county-government portal identity while its raw page title is “www.bte365.com,” an identity and metadata mismatch.
- The homepage contains no login form, sensitive form, hidden form, or wallet-connection activity.

Regulatory Verification Notes

The portal attributes sponsorship to the county publicity department and identifies itself as a county committee portal, but the supplied evidence does not independently verify that real-world operator identity. The site is presented as an informational portal rather than a regulated financial service, and no license claim or license number is shown in the available business-model evidence. That is a disclosure and verification gap, not by itself evidence of fraud; in this case, however, it must be considered alongside the confirmed external reputation findings. The domain has a substantial registration and archival history, but those continuity signals do not validate the current operator or overcome the security detections.

EVIDENCE

- Domain registered on 2018-07-10 and recorded as 8.12 years old; registrar: NameSilo, LLC.
- Archive history contains 314 snapshots from 2019-08-22 through 2026-05-20, spanning 8 years tracked.
- Served from AS398823, PEG-LA - PEG TECH INC, US.
- TLS certificate issued by YR2 with DV validation, valid to 2026-11-02T19:00:00+00:00.

What to Verify Next

Before any sensitive interaction, an institution should independently confirm that the county publicity department officially operates or endorses the portal through a government directory or an offline institutional contact route. The portal’s contact details and technical-support attribution should be cross-checked against independently sourced government records rather than relying on the site alone. Any proposed credential, payment, download, or account-related activity should remain suspended until the external blacklist findings and the domain-to-portal relationship have been resolved by the responsible security team.

EVIDENCE

- The homepage identifies the county publicity department as sponsor and credits technical support to a local vendor.
- The homepage provides a news-submission phone number, hotline, and contact mailbox for independent comparison with official records.
- Behavioral testing completed 2 successful runs, with 0 external XHR/fetch requests and 0 hidden forms detected.
- The site resolved to 1 IP address with 1 likely origin candidate and no detected CDN edge IPs.

Summary Verdict

The overall posture is **critical and unsuitable for sensitive interaction**. The apparent informational purpose and stable historical presence do not reconcile the confirmed external threat and blacklist findings with the site's claimed identity. The operator's real-world identity remains unverified, so the portal should not be treated as an authenticated government service.

Infrastructure Integrity

The site is directly hosted through PEG-LA - PEG TECH INC in the United States on AS398823, without a detected CDN or WAF layer and with a visible likely origin address. Transport encryption is present through a DV certificate issued by YR2, but ordinary TLS protection confirms encrypted transport only and does not establish site legitimacy.

Closing Assessment

Restrict activity to passive viewing while the domain, government attribution, and external threat findings are independently adjudicated; credentials, downloads, payments, and other sensitive actions should not be performed through the site.

Written analysis generated 2026-08-20 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	55/100
Identity verification confidence	30%

- 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 886ko.com.

- The request stayed on 886ko.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 2027-07-10. NOTED
- The earliest public archive of this site is from 2019-08-22. 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	38.173.157.216
Name servers	NS1.DNSOWL.COM, NS2.DNSOWL.COM, NS3.DNSOWL.COM
SSL issuer	YR2
SSL expiry	2026-11-02
Domain age	8.12 years (continuous registration)
Domain expiry	2027-07-10
Archive first seen	2019-08-22

Archive snapshots	314
Reputation	VirusTotal: 12 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about 886ko.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/886ko.com> · assessed 2026-08-20