

Is bztlxx.com a scam? TrustSniffer's high-risk assessment: 5/100

bztlxx.com

Verdict

5

OUT OF 100

CRITICAL RISK

bztlxx.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 70%.

What this site appears to be

Chinese-language campus news page for 仲恺农业工程学院 with lists of announcements, events, lectures, and media links. Typical university newsroom content; no financial solicitations or credential-harvesting elements 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	None flagged it VirusTotal	CLEAR
Google Safe Browsing	Listed as unsafe Google	RISK
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 387 snapshots	CLEAR
Certificate	Encrypted connection Issued by YR1	NOTED

The page as captured

https://bztlxx.com/



What bztlxx.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 2018.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Overview

The website is a Chinese-language campus news and university-media portal presenting institutional announcements, campus events, lectures, 专题报道, downloadable resources, and links to related media channels for 仲恺农业工程学院; its apparent business model is informational rather than commercial or solicitation-focused.

Scam/Impersonation Risk

The page content itself resembles a conventional university newsroom and contains no financial solicitation, credential-harvesting form, wallet interaction, or detected brand-impersonation pattern. However, this benign presentation is outweighed by a confirmed blacklist signal: external safety intelligence records a Google Safe Browsing match and an external blacklist hit. No conflicting legal identities or direct phishing form were established in the supplied page evidence, but the blacklist status creates a material risk for sensitive interaction and means the apparent institutional presentation cannot be treated as proof of legitimacy.

EVIDENCE

- External safety intelligence identifies the domain as malicious in Google Safe Browsing and records an external blacklist hit.
- The homepage contains university-news and campus-media material, while behavioral inspection detected 0 external XHR requests, 0 hidden forms, 0 password-external forms, and 0 wallet-provider detections.
- The domain was registered on 2018-07-10 and is approximately 8.12 years old.
- Archive coverage records 387 snapshots spanning 2018–2026, with 9 years tracked.

Regulatory Verification Notes

The site presents an institutional news function, and no financial service, investment offer, license claim, or license number is identified in the analyzed content. The apparent connection to 仲恺农业工程学院 remains independently unverified; therefore, the content supports an apparent informational purpose but does not establish the real-world operator or institutional authorization. The absence of a regulated-service disclosure is a verification gap rather than a standalone finding of fraud. A broker-reputation dataset produced no match, which provides no independent regulatory validation.

EVIDENCE

- The homepage is categorized as a university news portal and informational site, with no sensitive forms or financial solicitation elements detected.
- The analyzed content contains no claimed license authority or license number.
- The site is served from AS398823, identified as PEG-LA - PEG TECH INC, US.
- Its TLS certificate is issued by YR1, uses Domain Validation (DV), and is valid to 2026-09-24.

What to Verify Next

An independent institutional source should confirm that the domain is an authorized web property of 仲恺农业工程学院, rather than relying on the site's own navigation or content. The destination of the homepage's “登录” link should be inspected and independently validated before any credential submission; the captured page contained no login form, but the presence of a login navigation item warrants destination checking. Any future page offering regulated services should be checked against the relevant regulator's registry using the legal entity and license number stated on that page. The external safety warning should also be confirmed as resolved through an independent, current security review before sensitive use.

EVIDENCE

- The homepage includes a “登录” navigation item, although sensor analysis recorded 0 forms and no sensitive form.
- The homepage links to established education and media domains including edu.cn, moe.edu.cn, xinhuanet.com, and people.com.cn, which can serve as independent reference points for affiliation checking.
- The page title is recorded as “365-818,” and no structured metadata or canonical title identifying the institution was detected.

Summary Verdict

The overall posture is critical and unsuitable for sensitive interaction. The site’s institutional-news appearance and technically normal page behavior do not overcome the confirmed external safety and blacklist detections, while the operator’s real-world identity remains unverified.

Infrastructure Integrity

The site resolves directly to a single US address, 38.173.127.182, with no detected CDN or WAF and no separate edge-IP layer. This provides little protective separation between the public service and its apparent hosting endpoint; infrastructure observations are mitigating or contextual only and do not establish legitimacy.

Closing Assessment

Passive viewing may be limited to non-sensitive purposes, but credentials, personal data, and financial information should not be submitted unless the domain’s institutional authorization and current security status have been independently established.

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, behaviour in a sandbox, 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
- The structure of the page changed sharply while it was loading.
Behaviour in a sandbox rule:BEHAV_DOM_DENSITY_SPIKE
- 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 bztlxx.com.

- The request stayed on bztlxx.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 2018-07-21. 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	38.173.127.182
Name servers	NS1.DNSOWL.COM, NS2.DNSOWL.COM, NS3.DNSOWL.COM
SSL issuer	YR1
SSL expiry	2026-09-24
Domain age	8.12 years (continuous registration)
Domain expiry	2027-07-10
Archive first seen	2018-07-21
Archive snapshots	387
Reputation	VirusTotal: 0 flagged AbuseIPDB: 0 reports Google Safe Browsing: 1 match

About this assessment

A trust score summarises the evidence TrustSniffer could collect about bztlxx.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.

