

Is bc365777.cn a scam? TrustSniffer's high-risk assessment: 0/100

bc365777.cn

Verdict

0

OUT OF 100

CRITICAL RISK

bc365777.cn 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 55%.

WHAT THIS SITE APPEARS TO BE

Short Chinese-language page containing a brand slogan and a classical poem excerpt; no forms, links, or monetization signals 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	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	2.0 years old Registered history	CLEAR
Web archive	Archived since 2024 Public history exists	CLEAR
Certificate	Encrypted connection Issued by WE1	NOTED

The page as captured

https://bc365777.cn/JoWuts.html



What bc365777.cn served when TrustSniffer captured it on 2026-08-20. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: 1 to 3 years (registration continuity).
- Public web-archive history exists since 2024.
- 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.

This website is a short Chinese-language static page presenting a promotional slogan—“老品牌,值得您信耐!” (“A long-established brand, worthy of your trust”)—alongside an excerpt from a classical Chinese poem. Its apparent purpose is informational or promotional, with no visible account, transaction, monetization, or other substantive business workflow.

Scam/Impersonation Risk

The site presents a **critical sensitive-interaction risk** because external security intelligence records a confirmed blacklist status, with malicious detections from multiple security providers, including Kaspersky and Sophos. This finding materially outweighs the benign appearance of the captured page. The page itself contains no login form, payment flow, or clear brand-impersonation indicators, and no identity contradiction between legal entities was observed; however, the absence of visible attack mechanics on a minimal static page does not resolve the external threat detections. No confirmed phishing or brand-impersonation finding is established by the supplied page-level evidence, but the blacklist status remains a direct contradiction to safe engagement.

EVIDENCE

- External reputation telemetry records 15 malicious detections and 1 suspicious detection from 21 evaluated results, including Tier-1 detections by Kaspersky and Sophos.
- The domain is recorded as blacklisted by two external sources; the automated protective response was activated because malicious detections met the configured threshold.
- The captured homepage contains 76 characters of Chinese text, no forms, no internal or external links, and no visible monetization or account workflow.

Regulatory Verification Notes

The available identity evidence is insufficient to independently connect the site to a verified real-world operator. The captured content does not claim a license, identify a licensing authority, or provide a registration number; this is a regulatory disclosure gap requiring independent confirmation, not by itself proof of fraud. The site's technical configuration provides ordinary transport and hosting signals, but these establish service delivery rather than legal legitimacy. No matching broker-reputation record was identified in the supplied third-party context.

EVIDENCE

- The registration record lists Dynadot Inc as registrar, a creation date of 2025-10-09, a reconciled domain age of 1.99 years, and registrant text “刘艳”.
- Historical coverage records 12 snapshots across 3 tracked years, from 2024-08-22 through 2026-02-20.
- The site is served from AS13335, CLOUDFLARENET – Cloudflare, Inc., US.
- The TLS certificate is issued by WE1 at DV validation level and is valid to 2026-10-30.

What to Verify Next

Before any sensitive interaction, an independent party should establish the operating entity, confirm whether the site's activities require authorization, and match any claimed authorization against the relevant official registry. Contact details should be validated through an independently sourced channel rather than relying solely on information presented by the site. A security review should also examine the site's outbound network destinations and determine whether the observed external activity is expected and benign.

EVIDENCE

- The site provides no visible license claim, license number, or licensing authority in the captured content.
- Behavioral capture recorded 2 external XHR requests and 2 external POST requests, all classified as non-whitelisted.
- Two successful behavioral runs recorded 2 console errors and a corrected “suspicious network” signal.

Summary Verdict

The website's overall posture is critical and is not suitable for sensitive interaction. Its minimal informational presentation does not offset the convergent external reputation findings, and the operator identity remains unverified. Passive viewing is the only proportionate use supported by the available evidence.

Infrastructure Integrity

Cloudflare CDN/WAF protection is present, with all observed addresses belonging to Cloudflare edge infrastructure and no origin server address observable in this analysis. This reduces direct exposure of the underlying host and may mitigate infrastructure-level abuse, but it does not establish the legitimacy of the website or neutralize the external reputation risk.

Closing Assessment

Access should remain limited to passive inspection until the operator, regulatory position, and external security findings have been independently resolved; credentials, financial information, and other sensitive data should not be submitted.

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 public registration record for this domain is incomplete.
Registration and ownership rule:KF_WHOIS_INCOMPLETE
- 02 Sensitive Interaction Risk

 - The analysis matched a pattern TrustSniffer treats as a direct threat to a visitor.
Analysis engine signal:direct_threat
 - A large share of what the page loaded came from other domains.
Behaviour in a sandbox rule:BEHAV_EXTERNAL_RATIO_MODERATE
 - The page sent data to a destination TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_POSTS
 - 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	50%

- 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 bc365777.cn.

- The request stayed on bc365777.cn. It was not redirected to another domain. CLEAR
- Registration is published under Dynadot Inc. CLEAR
- DNS for this domain is served by cloudflare.com, across 2 name servers. NOTED
- The registration is paid up to 2026-10-09. NOTED
- The earliest public archive of this site is from 2024-08-22. CLEAR
- It is hosted on CLOUDFLARENET, from a server in US. NOTED

Domain intelligence

Registrar	Dynadot Inc
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US
Server IP	2606:4700:3032::6815:4755
Name servers	brynn.ns.cloudflare.com, dane.ns.cloudflare.com
SSL issuer	WE1
SSL expiry	2026-10-30
Domain age	1.99 years (continuous registration)
Domain expiry	2026-10-09
Archive first seen	2024-08-22
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 bc365777.cn 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.