

Is 028k365.com a scam? TrustSniffer's high-risk assessment: 0/100

028k365.com

Verdict

0

OUT OF 100

CRITICAL RISK

028k365.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 70%.

What this site appears to be

Chinese-language corporate site for a printing/packaging materials supplier (inks, varnishes, color management, testing, and training). Presents company history, services, and product categories. No clear financial/investment solicitations 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	16 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	1.1 years old Registered history	CLEAR
Web archive	Archived since 2025 1 snapshot	CLEAR
Certificate	Encrypted connection Issued by YR1	NOTED

The page as captured

<https://028k365.com/>

403 Forbidden

openresty/1.25.3.2

What 028k365.com served when TrustSniffer captured it on 2026-08-18. 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 2025.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

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

The website is a Chinese-language corporate site presenting itself as a business-to-business supplier of printing and packaging materials, including inks, varnishes, chemicals, color-management systems, testing, technical support, and industry training. Its stated commercial model is the sale of production materials and related technical services to printing, food, pharmaceutical, cosmetics, electronics, and other packaging-sector customers.

Scam/Impersonation Risk

The site presents a material contradiction between its visible branding and its substantive content. The page title contains Chinese entertainment-platform wording, while the body describes a printing-materials supplier and displays product and service categories unrelated to that title. This inconsistency is accompanied by a **confirmed blacklist** status and multiple external malicious detections, including coverage from Fortinet, Kaspersky, and Sophos. The available evidence does not establish a specific brand impersonation or an identity inconsistency between two legal entities, but the combination of blacklist findings, malicious detections, and

inconsistent page presentation creates a high risk for sensitive interaction. The domain is not suitable for login, credential submission, or financial activity absent independent resolution of these findings.

EVIDENCE

- External reputation assessment recorded 16 malicious and 2 suspicious detections among 23 evaluated results, with Fortinet, Kaspersky, and Sophos identified among the flagged providers; the domain was also marked externally blacklisted.
- The homepage title displays “太阳成tyc娱乐,太阳城娱乐平台,” while the same page describes printing inks, coatings, packaging materials, color management, testing, and training.
- Registration data records creation on 2026-08-10, with an age of ~0.02 years; archival coverage records 1 snapshot spanning 2025–2025, with 1 year tracked.

Regulatory Verification Notes

The about content makes substantial corporate claims, including that the business was established in 1998, is controlled by a listed printing company, operates several wholly owned subsidiaries, and provides technical and certification-related services. Those claims are presented on the site but are not independently verified by the supplied evidence, and the identity status therefore remains unverified. No license, registration number, or regulatory authority is disclosed in the available business-model evidence; this is a transparency gap requiring independent confirmation rather than, by itself, proof of fraud. No match was identified in the supplied broker-reputation dataset.

EVIDENCE

- The about page claims that the company was established on 7 September 1998 and is a controlled subsidiary of Xi'an Global Printing Co., Ltd., identified there by stock code 002799.
- The about and service content claims operations in Beijing, Guangzhou, Dongguan, and Tianjin, together with services involving product testing, research, technical support, and G7, GMI, and PSO-related training.
- Hosting infrastructure is served from AS137951, ASLINE-AS-AP – ASLINE LIMITED, HK.
- The site uses a DV TLS certificate issued by YR1, valid to 2026-11-08T18:24:09+00:00.

What to Verify Next

Before any sensitive interaction, an independent party should confirm the claimed company, parent relationship, subsidiaries, and operating addresses through authoritative corporate records and direct confirmation obtained outside the website. Any regulated or certification-related service should be matched to the relevant authority, registry, or issuing body, and commercial counterparties should independently validate payment instructions and contractual contacts before placing orders or sharing business information.

EVIDENCE

- The site's corporate identity and ownership claims appear on the about page but remain independently unverified.
- The available disclosure state does not provide a license number or named licensing authority for independent confirmation.
- The site's transport encryption is present, but certificate validity does not establish operator identity or site legitimacy.

Summary Verdict

The overall posture is **critical trust risk**. The website's professional B2B presentation is outweighed by confirmed external reputation contradictions and unresolved identity and governance concerns. Sensitive interaction is not appropriate on the evidence supplied.

Infrastructure Integrity

The site resolves directly to a single apparent origin rather than through a detected CDN or WAF, and no trusted CDN protection was identified. This provides limited infrastructure-based mitigation and does not offset the external reputation findings.

Closing Assessment

Sensitive actions should be withheld unless independent corporate, regulatory, and security validation produces a clear and reliable basis for 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, 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

- Most of what the page loaded came from other domains rather than from this one.

Behaviour in a sandbox rule:BEHAV_EXTERNAL_RATIO_HIGH

- 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 028k365.com.

- The request stayed on 028k365.com. It was not redirected to another domain. [CLEAR](#)
- Registration is published under GMO Internet Group, Inc. d/b/a Onamae.com. [CLEAR](#)
- DNS for this domain is served by share-dns.com, across 2 name servers. [NOTED](#)
- The registration is paid up to 2027-08-10. [NOTED](#)
- The earliest public archive of this site is from 2025-07-10. [CLEAR](#)
- It is hosted on ASLINE-AS-AP, from a server in SC. [NOTED](#)

Domain intelligence

Registrar	GMO Internet Group, Inc. d/b/a Onamae.com
Hosting	ASLINE-AS-AP - ASLINE LIMITED, HK
Country	SC
Server IP	156.224.39.248
Name servers	A4.SHARE-DNS.COM, B4.SHARE-DNS.NET
SSL issuer	YR1
SSL expiry	2026-11-08
Domain age	1.10 years (continuous registration)
Domain expiry	2027-08-10
Archive first seen	2025-07-10
Archive snapshots	1
Reputation	VirusTotal: 16 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about 028k365.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/028k365.com> · assessed 2026-08-18