

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

paulaediogo.net

Verdict

0

OUT OF 100

CRITICAL RISK

paulaediogo.net 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 2026-08-19 by automated analysis. Classification confidence 55%.

What this site appears to be

Institutional website for 云顶国际8588yd(中国)股份有限公司 providing news, notices, admissions information, departmental pages, and contact details including ICP number and phone/address.

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	13 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	4.3 years old Registered history	CLEAR
Web archive	Archived since 2021 Public history exists	CLEAR
Certificate	Encrypted connection Issued by ZeroSSL ECC DV SSL CA 2	NOTED

The page as captured

<https://www.paulaediogo.net/>



What paulaediogo.net served when TrustSniffer captured it on 2026-08-19. 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 2021.
- 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 presents itself as the official institutional website of 云顶国际8588yd(中国)股份有限公司, offering campus and organizational information, news, public notices, admissions, academic departments, research, employment services, and contact details. Its apparent purpose is informational and educational rather than direct financial or consumer commerce.

Scam/Impersonation Risk

The site's content is institution-like and contains no observed login form, sensitive form, wallet function, or overtly fraudulent page language. However, this positive page presentation is materially outweighed by confirmed external threat detections: the domain is blacklisted by multiple sources, with malicious classifications reported by external security providers including Kaspersky and Sophos. The supplied evidence does not establish an identity contradiction between two legal entities or a confirmed brand-impersonation pattern, but the blacklist evidence is sufficient to make sensitive interaction inappropriate. No suspicious contact-email anomaly was reported.

EVIDENCE

- The homepage presents institutional navigation covering admissions, departments, research, employment, public services, notices, and campus information; page analysis recorded no red flags.
- External reputation assessment recorded 13 malicious detections from 18 effective detections, with Kaspersky and Sophos among the flagged providers.
- The domain registration record shows creation on 2023-09-18, with an age of 2.92 years.
- Historical records show 5 archive snapshots from 2021-12-20 through 2025-07-16, across 5 years tracked.

Regulatory Verification Notes

The website displays an ICP filing number, a public-security filing number, a Xi'an address, postal code, general telephone number, and admissions hotline. These details support the appearance of an educational or institutional information site, but they do not independently verify that the domain is operated by the named organization. No license or registration number specific to a regulated financial activity is claimed, and the available evidence does not establish an independently verified real-world operator. The site's low external authority signal and confirmed blacklist status should therefore be treated as reputational and security concerns rather than resolved by its on-page institutional disclosures.

EVIDENCE

- The homepage footer displays ICP number 陕ICP备15015903号 and public-security filing number 陕公网安备6101160200055.
- The contact information on the homepage states an address in Chang'an District, Xi'an, postal code 710100, telephone 029-68084609, and admissions hotline 029-68084661.
- The site's transport encryption uses a DV certificate issued by ZeroSSL ECC DV SSL CA 2, valid through 2026-11-08.
- Hosting is identified as AS26658, HENGTONG-IDC-LLC - HT, US.

What to Verify Next

Before any login, credential submission, payment, download, or other sensitive interaction, the claimed institution should be contacted through an independently sourced channel and asked to confirm that this domain is an authorized official website. The ICP and public-security filing details should be checked against the relevant official records, and any admissions or service transaction should use independently confirmed institutional payment and contact procedures. Until those checks succeed, use should be limited to passive review of publicly displayed information.

EVIDENCE

- The homepage provides institutional contact and filing details that can be checked against authoritative government or institutional records.
- The page analysis found no login form or sensitive form, so any later request for credentials or payment would represent a materially different interaction surface.
- The apparent institutional identity is not independently linked to the domain in the supplied evidence.

Summary Verdict

The website has a **critical trust posture** for sensitive interaction. Its institutional presentation does not overcome the confirmed external malicious detections and blacklist status, while the real-world operator remains unverified. Passive viewing does not establish that account, credential, payment, or other sensitive use is acceptable.

Infrastructure Integrity

The site resolves directly to a single origin address, with no detected CDN or WAF layer and no edge-IP separation. This provides less intermediary protection than a mainstream edge-security deployment; infrastructure characteristics are mitigating or limiting signals only and do not establish legitimacy.

Closing Assessment

Prospective users should refrain from sensitive interaction unless independent institutional confirmation and authoritative record checks first establish that the domain is genuine and authorized.

Written analysis generated 2026-08-19 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

- 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
- The page sent data to a destination TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_POSTS
- 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	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 paulaediogo.net.

- The request stayed on paulaediogo.net. It was not redirected to another domain. CLEAR
- Registration is published under Gname.com Pte. Ltd.. CLEAR
- DNS for this domain is served by gname-dns.com, across 2 name servers. NOTED
- The registration is paid up to 2026-09-18. NOTED
- The earliest public archive of this site is from 2021-12-20. CLEAR
- It is hosted on HENGTONG-IDC-LLC, from a server in HK. NOTED

Domain intelligence

Registrar	Gname.com Pte. Ltd.
Hosting	HENGTONG-IDC-LLC - HT, US
Country	HK
Server IP	45.127.160.34
Name servers	NS1.GNAME-DNS.COM, NS2.GNAME-DNS.COM
SSL issuer	ZeroSSL ECC DV SSL CA 2
SSL expiry	2026-11-08
Domain age	4.29 years (continuous registration)
Domain expiry	2026-09-18
Archive first seen	2021-12-20
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 13 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about paulaediogo.net 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.

