

Is 2dcafe.jp a scam? TrustSniffer's high-risk assessment: 0/100

2dcafe.jp

Verdict

0

OUT OF 100

CRITICAL RISK

2dcafe.jp 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

Assessed 2026-08-18 by automated analysis. Classification confidence 70%.

What this site appears to be

2D Cafe — Japanese local café site describing concept (2D/monochrome photo-spot), opening hours, address in Shinjuku, phone number, menu highlights and reservation/menu navigation. No evident forms requesting sensitive data and no financial/investment claims.

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.

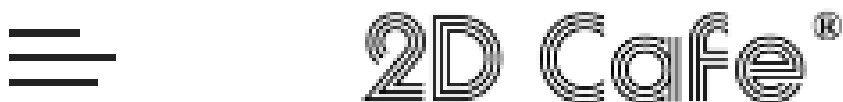
Malware engines	10 flagged it VirusTotal	RISK
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	0 reports AbuseIPDB; shared hosting inflates this count	NOTED
Domain age	4.7 years old Registered history	CLEAR
Web archive	Archived since 2021 29 snapshots	CLEAR
Certificate	Encrypted connection Issued by YR2	NOTED

The page as captured

<https://2dcafe.jp/>

営業時間：11:00～23:00 定休日：なし

住所：東京都新宿区百人町1-7-5 座ビル1F



What 2dcafe.jp served when TrustSniffer captured it on 2026-08-18. 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

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

2D Cafe is a Japanese local-café website presenting a monochrome, manga-inspired “café inside a picture” concept, with food and beverage sales and reservations intended to support visits to its Shinjuku location.

Scam/Impersonation Risk

The site presents a plausible local-business profile and no explicit phishing, brand-impersonation, investment, or cryptocurrency content was identified in the rendered page. However, this benign presentation is outweighed by a confirmed external blacklist condition and malicious reputation detections, creating a material contradiction for any sensitive interaction. Repeated behavioral testing also detected hidden forms despite no visible sensitive form in the page content; this discrepancy should be treated as a significant contact and interaction-integrity concern. No conflicting legal-entity names or direct brand-impersonation finding were observed. The available evidence therefore supports a clearly cautionary posture, with ordinary browsing separated from credential, payment, or other sensitive activity.

EVIDENCE

- External reputation telemetry recorded 10 malicious and 2 suspicious detections; Fortinet and Sophos were among the flagged vendors, and blacklist status was confirmed by two external sources.
- Behavioral testing detected hidden forms in both successful runs, while the homepage review found no visible sensitive form or login form.
- The domain has an authoritative age of 4.731006160164271 years, with 29 archive snapshots spanning 2021–2026 and 6 tracked years; historical continuity was present, but it does not offset the external threat detections.

Regulatory Verification Notes

The supplied site content identifies the operating presentation as “2D Cafe” but does not provide a distinct legal-entity name, registration number, or regulatory authority. For a café whose stated model is on-site food and beverage sales with reservations, the absence of a financial-services license is not itself a regulatory breach; nevertheless, the available disclosure is insufficient to independently connect the website to a verified real-world operator. A valid transport certificate confirms encrypted delivery, but certificate validity and hosting arrangements do not establish legal identity or regulatory standing.

EVIDENCE

- The homepage and footer identify “2D Cafe” and display “Copyright 2019,” without a separate legal-entity or registration disclosure.
- The site’s transport encryption uses a DV certificate issued by YR2, valid to 2026-10-04T05:10:11+00:00.
- The hosting infrastructure is served from AS131965 operated by XSERVER - Xserver Inc., JP.

What to Verify Next

Before any sensitive interaction, an independent source should corroborate that the café exists at the stated location and that its published telephone and reservation channels are official. The reservation pathway should be inspected for unexpected credential or payment requests, and any payment should use a method with meaningful dispute and chargeback protection. If the operator presents itself as a regulated or licensed business, the claimed entity and authorization should be checked directly with the relevant registry rather than relying on the website.

EVIDENCE

- The homepage provides opening-hours, location, telephone, menu, and reservation navigation that can be cross-checked independently.
- The page-level review classified the visible business model as a brick-and-mortar café and identified no financial or investment claims.
- The rendered page had no login form, while behavioral testing identified hidden forms, making destination and field-level inspection of the reservation flow necessary.

Summary Verdict

The overall posture is **critical trust risk**. The site’s ordinary local-business presentation is not sufficient to support safe sensitive interaction because confirmed external threat indicators and inconsistent form behavior materially undermine operational trust. Identity remains unverified, so the website should not be treated as an established or independently authenticated operator.

Infrastructure Integrity

The site resolves directly to a single likely origin server hosted by XSERVER - Xserver Inc. in Japan, with no CDN or WAF layer identified. This provides limited protective buffering against direct-origin exposure; the DV TLS certificate is a mitigating transport-control signal only and cannot counter the confirmed reputation concerns.

Closing Assessment

Sensitive actions should be withheld unless the operator, reservation channel, and transaction path are independently authenticated through trusted channels and protected payment controls.

Written analysis generated 2026-08-18 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

1 finding contributed to this verdict, raised by analysis engine, behaviour in a sandbox, external reputation.

01 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 contained a form a visitor cannot see.
Behaviour in a sandbox rule:BEHAV_HIDDEN_FORMS
- 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 2dcafe.jp.

- The request stayed on 2dcafe.jp. It was not redirected to another domain. CLEAR
- The earliest public archive of this site is from 2021-11-23. CLEAR
- It is hosted on XSERVER, from a server in JP. NOTED

Domain intelligence

Registrar	Not available
Hosting	XSERVER - Xserver Inc., JP
Country	JP
Server IP	162.43.121.32
Name servers	Not available
SSL issuer	YR2
SSL expiry	2026-10-04
Domain age	4.73 years (continuous registration)
Domain expiry	Not available
Archive first seen	2021-11-23
Archive snapshots	29
Reputation	VirusTotal: 10 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about 2dcafe.jp 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.