

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

otsumami.com.tw

Verdict

0

OUT OF 100

CRITICAL RISK

otsumami.com.tw 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 2026-08-21 by automated analysis. Classification confidence 55%.

What this site appears to be

{ "trust_quality": { "score": 0.6, "overall_assessment": "Small e-commerce storefront for packaged snacks; appears informational/retail with product listings and prices. No immediate high-risk financial solicitations detected." }, "dom_content": { "has_dom_text": true, "text_length_chars": 1034 }, "social_presence": { "social_domains": [] }, "link_graph": { "internal_links": [], "external_links": ["http://www.otsumami.com.tw/images/b/001[0].jpg", "http://www.otsumami.com.tw/images/b/001[1].jpg", "http://www.otsumami.com.tw/images/b/001[3].jpg", "http://www.otsumami.com.tw/images/b/001[4].jpg", "http://www.otsumami.com.tw/ima ges/...

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	5 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	20 years old Registered history	CLEAR
Web archive	Archived since 2008 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YR2	NOTED

The page as captured

https://otsumami.com.tw/



What otsumami.com.tw served when TrustSniffer captured it on 2026-08-21. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: more than 10 years (registration continuity).
- Public web-archive history exists since 2008.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Overview

The website is a Chinese-language online storefront for packaged snacks, nuts, and related food products, presenting product images, prices, inquiry-based purchasing, customer-service information, and a member-login link as part of a small retail business model.

Scam/Impersonation Risk

Confirmed external blacklist status and multiple malicious detections create a critical risk posture despite the storefront's apparently ordinary retail presentation. The captured homepage contains no sensitive credential form, deposit flow, or explicit phishing form, but behavioral testing recorded wallet-drainer activity in both

observed runs, which is materially inconsistent with a conventional snack retailer and warrants treating login, credential, and financial interactions as unsafe. The published contact channel also contains the anomaly `info@otsumami.come`, a contact-channel integrity issue consistent with a deliverability-breaking typo or possible typosquat. No separate conflicting legal-entity names or explicit brand impersonation were observed.

EVIDENCE

- Homepage: Chinese-language product catalog for packaged snacks and nuts, with product images, prices, inquiry functionality, and a member-login link.
- Behavioral testing: wallet-drainer activity recorded in 2 of 2 runs; no external XHR or hidden sensitive forms were detected.
- External reputation telemetry: 5 malicious detections, 2 suspicious detections, and a confirmed blacklist hit.

Regulatory Verification Notes

The site's apparent retail purpose does not by itself establish the identity of the operating merchant. The available on-page disclosure state is unclear, and no financial-regulatory licensing or registration number is identified in the supplied storefront content; this is a transparency and verification matter rather than standalone proof of a scam. The identity of the real-world operator remains unverified. The site's long registration continuity and valid transport encryption are positive technical facts, but they do not overcome the confirmed external threat indicators.

EVIDENCE

- Domain registration: Registered 2007; approximately 19.56 years old; registrar eNom, Inc.; registrant organization Taiwan Domain Name Service Center-TaiwanDNS.
- Hosting: Served from AS131149, YUANJHEN-AS-TW – Yuan-Jhen Info., Co., Ltd, Taiwan.
- Transport encryption: TLS certificate issued by YR2, domain validation (DV), valid through 2026-10-12T23:37:29+00:00.

What to Verify Next

Before any sensitive interaction, an independent check should confirm the merchant's legal identity, business registration, and the legitimacy of its customer-service channels. Any proposed payment should be limited to a method with meaningful buyer protection and should be preceded by confirmation that the transaction counterparty matches the independently verified merchant. The member-login function should not be used until the site's relationship to the genuine operator has been established through an offline or independently sourced route.

EVIDENCE

- Homepage: No sensitive form or financial-deposit flow was present in the captured content, although a member-login link was displayed.
- Site presentation: The captured page provides product and inquiry content but does not independently establish the operating entity.
- Technical behavior: Two successful test runs produced wallet-drainer detections requiring independent validation before account or payment activity.

Summary Verdict

The overall posture is **critical risk**, with the available evidence insufficient to support trusted sensitive interaction. The ordinary retail appearance is outweighed by confirmed external threat detections and anomalous runtime behavior, while the real-world operator remains unverified.

Infrastructure Integrity

The site resolves directly to infrastructure operated by Yuan-Jhen Info., Co., Ltd in Taiwan, with no detected mainstream CDN or WAF layer and one likely origin address. This provides limited protective mediation and should be treated only as an infrastructure characteristic, not as evidence of legitimacy.

Closing Assessment

Sensitive use should be suspended unless independent merchant-identity and channel checks resolve the identified concerns; any unavoidable engagement should remain limited to non-sensitive observation.

Written analysis generated 2026-08-21 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
- The page behaved in a way consistent with a crypto wallet drainer.
Behaviour in a sandbox rule:BEHAV_WALLET_DRAINER_SUSPECT
- 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	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 otsumami.com.tw.

- The request stayed on otsumami.com.tw. It was not redirected to another domain. [CLEAR](#)
- Registration is published under eNom, Inc.. [CLEAR](#)
- DNS for this domain is served by cx901.com. [NOTED](#)
- The registration is paid up to 2027-01-31. [NOTED](#)
- The earliest public archive of this site is from 2008-09-22. [CLEAR](#)
- It is hosted on YUANJHEN-AS-TW, from a server in TW. [NOTED](#)

Domain intelligence

Registrar	eNom, Inc.
Hosting	YUANJHEN-AS-TW - Yuan-Jhen Info., Co., Ltd, TW
Country	TW
Server IP	103.17.8.47
Name servers	ns47.cx901.com ns48.cx901.com
SSL issuer	YR2
SSL expiry	2026-10-12
Domain age	19.56 years (continuous registration)
Domain expiry	2027-01-31
Archive first seen	2008-09-22
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 5 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about otsumami.com.tw 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.

