

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

elcilantrillo.mx

Verdict

0

OUT OF 100

CRITICAL RISK

elcilantrillo.mx 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 2026-08-21 by automated analysis. Classification confidence 55%.

What this site appears to be

Spanish-language lodging site for 'Cabañas el Cilantrillo' showing cabins, prices, availability booking form, contact email and phone, and amenities. Appears to be a straightforward accommodation booking page.

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.

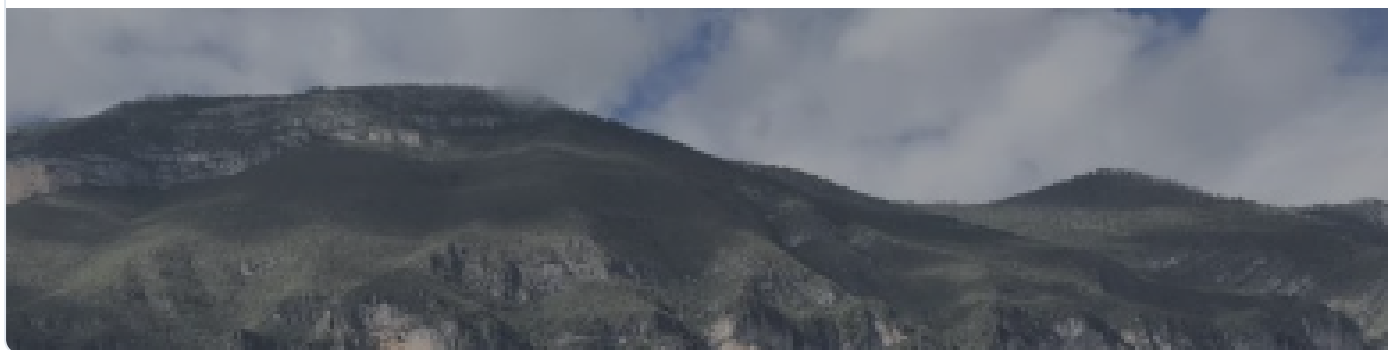
At a glance

The checks that decide most of this verdict.

Malware engines	9 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 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YR2	NOTED

The page as captured

<https://www.elcilantrillo.mx/>



What elcilantrillo.mx served when TrustSniffer captured it on 2026-08-21. 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, Kaspersky, Sophos flagged this site in external intelligence checks, indicating elevated compromise/scam exposure that requires immediate caution.

This is a Spanish-language hospitality website for Cabañas el Cilantrillo in Santiago, Nuevo León, presenting three cabins, local amenities, pricing, and an online availability and reservation interface for prospective guests.

Scam/Impersonation Risk

The site's visible content is consistent with a small lodging business and does not show a login form, credential-collection mechanism, wallet connection, brand-impersonation indicator, or conflicting legal identity. However, this benign presentation is outweighed by **confirmed external threat detections and blacklisting**, including multiple malicious assessments and a further suspicious assessment from independent security providers. The result is a material risk that the apparently ordinary booking page may not be suitable for sensitive interaction, even though the page itself contains no explicit fraud indicators.

EVIDENCE

- The homepage presents Cabañas el Cilantrillo, cabin reservations, availability checking, and amenities without a login or password form.
- External reputation checks recorded multiple malicious detections, a suspicious detection, and blacklist listings from Fortinet, Kaspersky, and Sophos.
- The domain was registered on 2024-01-27 and is approximately 2.57 years old through GoDaddy.com.
- Archive records show first observation on 2021-11-30 and last observation on 2026-01-06, with 6 years tracked.

Regulatory Verification Notes

The available page identifies the property by name and location but does not establish an independently verified operating entity. No licensing authority or registration number is disclosed in the supplied site content, leaving the legal and regulatory basis for taking reservations unclear. The homepage also contains template-style contact artifacts, including a San Francisco address and placeholder-format reservation details, which reduce confidence that the contact information was tailored to the stated Mexican lodging operation. This is a transparency and verification issue rather than a separate finding of fraud; the decisive concern remains the external threat and blacklist evidence described above.

EVIDENCE

- The homepage names “Cabañas el Cilantrillo” and locates the property in Santiago, Nuevo León, but does not identify a legal company or individual operator.
- The homepage contains no stated licensing authority or registration number.
- The reservation and contact area displays a generic United States address and placeholder-format contact details inconsistent with a clearly documented local operator.
- The site uses a Domain Validated TLS certificate issued by YR2, valid through 2026-10-14.

What to Verify Next

An organization considering engagement should independently confirm that the named property exists and that the domain is an authorized booking channel, using a telephone number or tourism listing obtained from an offline or independently sourced channel. The relevant Mexican local or state tourism and business registries should be checked for the operating entity and any lodging permissions applicable to the property. Reservation terms, cancellation conditions, payment destination, and refund protections should be confirmed before any booking commitment.

EVIDENCE

- The homepage provides a booking and availability form that creates a reservation-related interaction.
- The cabin pages display accommodation descriptions and prices but do not, in the supplied content, establish the contracting legal entity.
- The contact and reservation information should be compared with an independently sourced property listing before use.

Summary Verdict

The overall posture is **critical trust risk**. The site’s ordinary hospitality presentation does not overcome the confirmed external threat and blacklist indicators, and the real-world operator remains unverified. Sensitive interaction is therefore not supported by the available evidence.

Infrastructure Integrity

The site resolves to hosting operated by GoDaddy.com, LLC in the United States, using AS398101, with no CDN identified in the supplied infrastructure results. This is conventional hosting infrastructure and offers limited technical context only; it does not validate the site’s operator or offset the external reputation concerns.

Closing Assessment

Until independent property, operator, and payment-channel validation is completed, the appropriate posture is read-only review; credentials and payment details should not be submitted through the site.

Written analysis generated 2026-08-21 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
- 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 elcilantrillo.mx.

- The request stayed on elcilantrillo.mx. It was not redirected to another domain. CLEAR
- Registration is published under GoDaddy.com. CLEAR
- DNS for this domain is served by domaincontrol.com, across 2 name servers. NOTED
- The registration is paid up to 2027-01-27. NOTED
- The earliest public archive of this site is from 2021-11-30. CLEAR
- It is hosted on GO-DADDY-COM-LLC, from a server in US. NOTED

Domain intelligence

Registrar	GoDaddy.com
Hosting	GO-DADDY-COM-LLC - GoDaddy.com, LLC, US
Country	US
Server IP	208.109.228.65
Name servers	ns27.domaincontrol.com, ns28.domaincontrol.com
SSL issuer	YR2
SSL expiry	2026-10-14
Domain age	4.72 years (continuous registration)
Domain expiry	2027-01-27
Archive first seen	2021-11-30
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 9 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about elcilantrillo.mx 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.

