

Is 1cisp.coop a scam? TrustSniffer's high-risk assessment: 0/100

1cisp.coop

Verdict

0

OUT OF 100

CRITICAL RISK

1cisp.coop 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

Website for 1 Cooperative Insurance System of the Philippines (1CISP). Contains about, history, directors & management, products & services, corporate governance documents, annual report references, contact email, and mission/vision statements. Content focuses on cooperative insurance offerings and organizational information.

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.

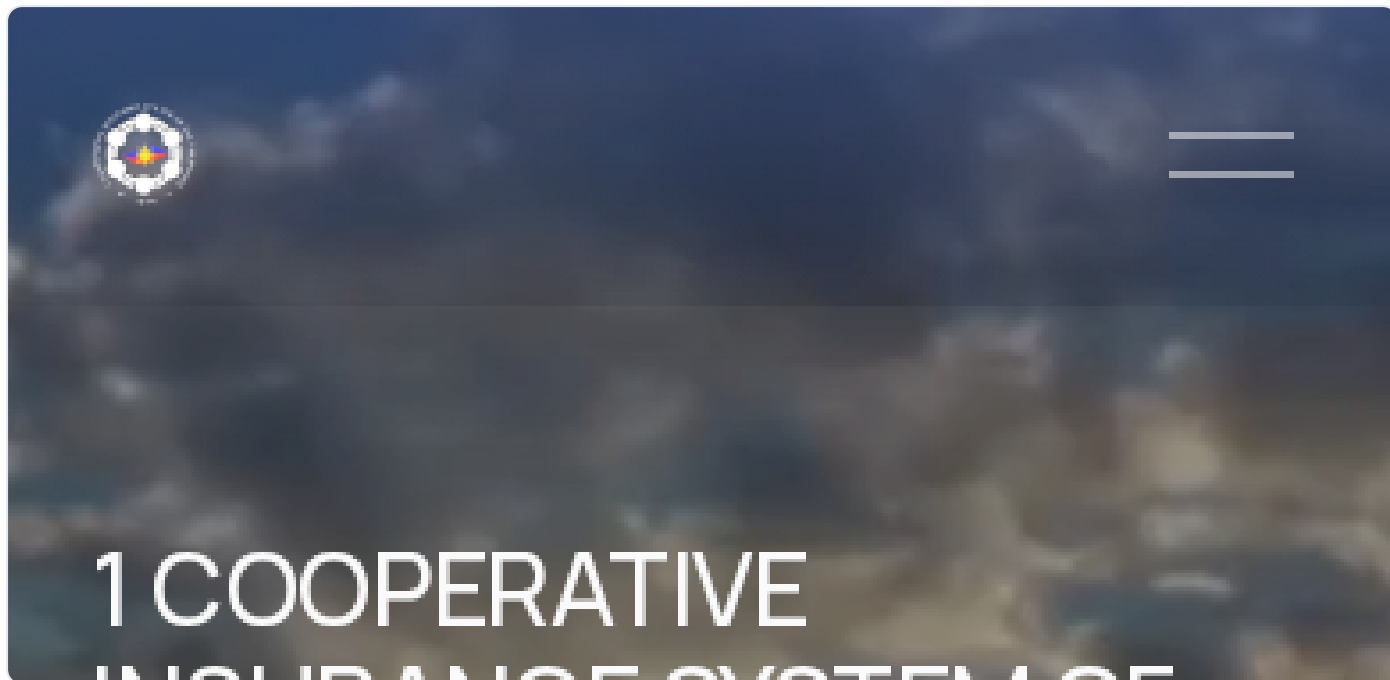
At a glance

The checks that decide most of this verdict.

Malware engines	2 flagged it VirusTotal	RISK
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	15% confidence AbuseIPDB, 9 reports; shared hosting inflates reports	CLEAR
Domain age	5.2 years old Registered history	CLEAR
Web archive	Archived since 2021 21 snapshots	CLEAR
Certificate	Encrypted connection Issued by YR2	NOTED

The page as captured

<https://www.1cisp.coop/>



What 1cisp.coop 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 flagged this site in external intelligence checks, indicating elevated compromise/scam exposure that requires immediate caution.

The website presents itself as 1 Cooperative Insurance System of the Philippines (1CISP), a membership-based cooperative insurer offering life and general insurance products and services, together with organizational information, governance materials, annual-report references, and member-oriented contact content.

Scam/Impersonation Risk

The site's on-page presentation is coherent and contains no detected login form, hidden sensitive form, wallet functionality, or explicit brand-impersonation indicators. However, that benign presentation is materially outweighed by external threat intelligence identifying two malicious detections, a Fortinet detection, and confirmed blacklist status from multiple sources. The global reputation service also returned no malicious result for Google Safe Browsing, so the evidence is not uniformly negative; nevertheless, the corroborated blacklist and malicious detections create a serious contradiction requiring a security-forward posture. The nine abuse reports relate to shared Squarespace infrastructure rather than being uniquely attributable to the website, but

they remain part of the adverse external evidence. No separate identity inconsistency or on-page impersonation finding was observed.

EVIDENCE

- The homepage and site navigation identify the organization as 1CISP and contain corporate insurance content without a login or password form.
- External scanning recorded 2 malicious detections and a Fortinet threat detection for the assessed domain.
- The assessed domain is listed by an external blacklist; Google Safe Browsing returned false for malicious status.
- The domain was registered on 2021-06-02 and is 5.21 years old; archival records contain 21 snapshots spanning 2021-11-23 to 2025-11-06 across 5 tracked years.

Regulatory Verification Notes

The About, History, Directors & Management, Registry of Licensed Agents, Corporate Governance, Articles of Cooperation, By-Laws, Code of Conduct, and Annual Report sections provide substantial organizational and governance content. The available evidence does not independently verify the real-world operator identity, and no licensing authority or license number is recorded in the supplied analysis. That is a regulatory verification gap rather than, standing alone, proof of fraud; in this case, it must be considered alongside the confirmed external threat detections. No match was identified in the available broker-reputation dataset. The site's transport security is technically present, but domain-validated encryption does not establish regulatory authorization or operator identity.

EVIDENCE

- The site's legal and governance navigation includes Directors & Management, a Registry of Licensed Agents, Articles of Cooperation, By-Laws, governance codes, and a 2025 Annual Report reference.
- No license authority or license number is recorded in the site-analysis evidence, and independent identity verification remains unconfirmed.
- The site is served from AS53831, SQUARESPACE - Squarespace, Inc., US.
- TLS is issued by YR2 at DV validation level and is valid through 2026-11-05.

What to Verify Next

Before any account, credential, policy, premium, or other financial interaction, an institution should independently confirm 1CISP's legal existence and insurance authorization with the relevant Philippine regulatory or cooperative registry, using contact details obtained from that registry rather than relying solely on the website. The organization's official domain and contact channels should also be corroborated through an independent offline route, and any payment destination should be checked against the verified legal entity before funds are transferred. The external blacklist and malicious-detection findings should be escalated to the organization's security or fraud team for resolution before access is permitted.

EVIDENCE

- The site publishes Directors & Management, a Registry of Licensed Agents, and corporate governance materials that can be cross-checked against authoritative records.
- The site presents insurance products and member services, making licensing and payment-recipient validation directly relevant to prospective interactions.
- The available evidence records no independently verified identity signals linking the site to a confirmed real-world operator.

Summary Verdict

The website has a credible corporate presentation but an unacceptable trust posture for sensitive interaction because its coherent content is contradicted by corroborated external malicious and blacklist detections. Its apparent institutional identity remains unverified, and the available evidence does not support treating the site as suitable for login, credential, or financial activity.

Infrastructure Integrity

The site resolves to infrastructure operated by Squarespace, Inc., with four likely origin IPs and no separately detected CDN edge-IP layer. Squarespace is a mainstream hosting provider and the infrastructure is technically resolved, but hosting-provider legitimacy is only a mitigating technical characteristic and cannot offset the adverse reputation evidence.

Closing Assessment

Access should remain limited to passive review while the organization's identity, authorization, and the external threat findings are independently resolved; sensitive interaction and financial engagement should not proceed in the interim.

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 registration record withholds contact details for the operator.
Registration and ownership rule:KF_WHOIS_HIDDEN
- 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

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

- 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

Signals weighed against the site

- AbuseIPDB: 9 reports on hosting IP 198.49.23.144 (Squarespace, Inc., Content Delivery Network), 15% confidence. The reports are attributed to shared infrastructure, not specifically to this website.

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 1cisp.coop.

- The request stayed on 1cisp.coop. It was not redirected to another domain. [CLEAR](#)
- Registration is published under Domains.coop Limited. [CLEAR](#)
- DNS for this domain is served by yoursrs.com, across 2 name servers. [NOTED](#)
- The registration is paid up to 2027-06-02. [NOTED](#)
- The earliest public archive of this site is from 2021-11-23. [CLEAR](#)
- It is hosted on SQUARESPACE, from a server in US. [NOTED](#)

Domain intelligence

Registrar	Domains.coop Limited
Hosting	SQUARESPACE - Squarespace, Inc., US
Country	US
Server IP	198.49.23.144
Name servers	ns1.yoursrs.com, ns2.yoursrs.com
SSL issuer	YR2

SSL expiry	2026-11-05
Domain age	5.21 years (continuous registration)
Domain expiry	2027-06-02
Archive first seen	2021-11-23
Archive snapshots	21
Reputation	VirusTotal: 2 flagged AbuseIPDB: 15% confidence, 9 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about 1cisp.coop 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/1cisp.coop> · assessed 2026-08-18