

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

premcogroup.com

Verdict

0

OUT OF 100

CRITICAL RISK

premcogroup.com 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	Corporate homepage for Premco Rail Engineers Limited: presents company history (50+ years), services (rail infrastructure, private sidings, core industrial infrastructure, stalled project recovery, consulting), contact details, and corporate identifiers (CIN, address, phone, email).
------------------------------	---

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.

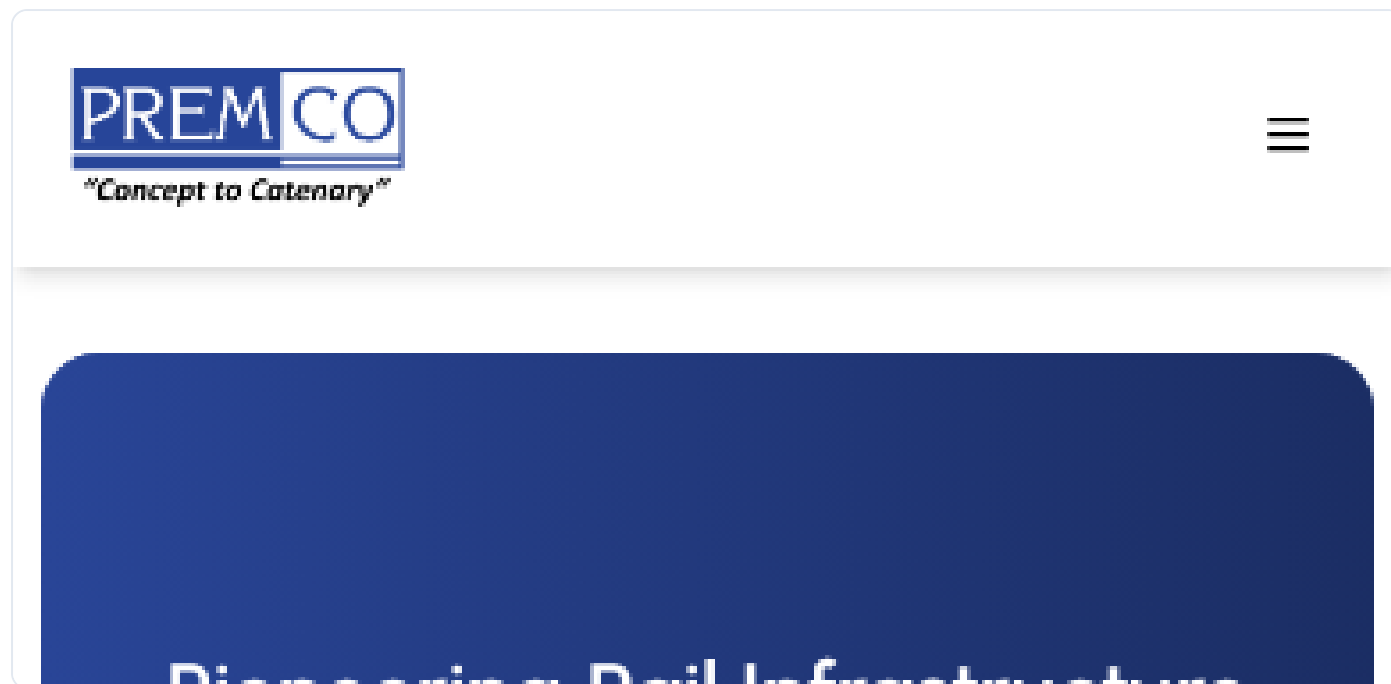
At a glance

The checks that decide most of this verdict.

Malware engines	17 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	22 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://premcogroup.com/>



What premcogroup.com 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

Security Alert

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

Premco Rail Engineers Limited's website is a corporate presentation for an Indian rail-infrastructure and industrial-construction business, describing more than 50 years of experience, work for Indian Railways and private industry, and services including civil works, electrification, signaling, telecommunications, private railway sidings, stalled-project recovery, and consulting.

Scam/Impersonation Risk

The site content itself presents a coherent corporate-services model and no page-level indicators of brand impersonation, phishing forms, or conflicting legal identities were identified. However, this benign presentation is materially contradicted by confirmed external security detections: the domain is blacklisted, and multiple major security providers classify it as malicious or suspicious. Under a security decision framework, those detections outweigh the professional appearance of the homepage and create a critical risk for sensitive interaction. No identity contradiction between distinct legal-entity names was observed, but the real-world operator remains independently unverified.

EVIDENCE

- External reputation assessment recorded 17 malicious and 1 suspicious detections, with threat flags from Fortinet, Kaspersky, and Sophos.
- The domain was confirmed on an external blacklist; Google Safe Browsing did not report a malicious result.
- Registration records show creation on 2004-11-25 and an age of 21.75 years.
- Historical records contain 57 archive snapshots spanning 2008–2026, with 19 years tracked.

Regulatory Verification Notes

The homepage identifies Premco Rail Engineers Limited and presents corporate identifiers, an address, telephone details, and contact information. It describes rail and industrial construction services for public and private clients, but no licensing authority or license number is disclosed in the supplied site content. That omission is a regulatory-transparency gap rather than proof of fraud; nevertheless, the external blacklist status requires the corporate claims and any proposed commercial relationship to be independently validated. No broker-related third-party match was identified.

EVIDENCE

- The homepage describes civil engineering, track repairs, electrification, signaling, telecommunications, private sidings, project recovery, and consulting.
- The homepage claims “50+ Years of Experience,” “Pan-India Presence,” and trust from Indian Railways and major industries.
- The site’s hosting infrastructure is identified as AS394695 operated by PUBLIC-DOMAIN-REGISTRY - PDR, US.
- Transport encryption uses a DV TLS certificate issued by YR2, valid until 2026-10-25.

What to Verify Next

Before any credential submission, financial commitment, document exchange, or contractual engagement, the claimed corporate identity should be checked against the relevant official corporate registry using the disclosed legal identifiers. Any claimed relationship with Indian Railways or major industrial clients should be confirmed through independently sourced institutional contact details, not solely through the website. Contact channels should also be validated through an offline or independently obtained route, and any security warning should be resolved with the relevant security provider before access is expanded beyond passive viewing.

EVIDENCE

- The homepage contains no login form or sensitive-data form.
- Automated interaction testing observed no external form submissions, wallet activity, or hidden forms.
- The site returned stable successful responses during both tested runs.
- The homepage provides corporate, service, and contact sections but no independently verified regulatory reference.

Summary Verdict

The website presents as a plausible corporate construction-services operation, but its overall trust posture is critical because confirmed external security contradictions materially undermine confidence in sensitive interaction. Identity verification remains incomplete, and the available evidence does not support treating the domain as suitable for login, credential handling, financial activity, or trusted business onboarding.

Infrastructure Integrity

The site has no detected CDN or WAF layer and resolves to two likely origin addresses rather than identifiable edge addresses. This direct hosting posture offers limited infrastructure-level mitigation and should not be treated as evidence of legitimacy.

Closing Assessment

Prospective users should restrict activity to passive review until the corporate identity, claimed affiliations, contact channels, and security detections have been independently resolved; credentials, documents, payments, and contractual commitments should not be submitted in the interim.

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, 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
- 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 premcogroup.com.

- The request stayed on premcogroup.com. It was not redirected to another domain. CLEAR
- Registration is published under PDR Ltd. d/b/a PublicDomainRegistry.com. CLEAR
- DNS for this domain is served by nudns.com, across 4 name servers. NOTED

- The registration is paid up to 2026-11-25. NOTED
- The earliest public archive of this site is from 2008-02-20. CLEAR
- It is hosted on PUBLIC-DOMAIN-REGISTRY, from a server in AE. NOTED

Domain intelligence

Registrar	PDR Ltd. d/b/a PublicDomainRegistry.com
Hosting	PUBLIC-DOMAIN-REGISTRY - PDR, US
Country	AE
Server IP	103.21.58.139
Name servers	NS1.NUDNS.COM, NS2.NUDNS.COM, NS3.NUDNS.COM, NS4.NUDNS.COM
SSL issuer	YR2
SSL expiry	2026-10-25
Domain age	21.75 years (continuous registration)
Domain expiry	2026-11-25
Archive first seen	2008-02-20
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 17 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about premcogroup.com 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/premcogroup.com> · assessed 2026-08-21