

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

pedalup.in

Verdict

0

OUT OF 100

CRITICAL RISK

pedalup.in 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 2026-08-20 by automated analysis. Classification confidence 55%.

WHAT THIS SITE APPEARS TO BE

Marketing landing page for PedalUp, a smart campus e-cycle mobility network targeting Indian residential campuses with early-access signups and pilot deployments. Content focuses on benefits (time-saving, low-cost, zero emissions), pilot campus names, and calls to secure early bird spots.

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	4 flagged it VirusTotal	RISK
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	0% confidence AbuseIPDB, 11 reports; shared hosting inflates reports	CLEAR
Domain age	3 months old Most scam domains are under a year old	RISK
Web archive	Archived since 2016 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YR2	NOTED

The page as captured

<https://www.pedalup.in/>

The logo for Pedal Up, featuring the words "Pedal Up" in a bold, dark green sans-serif font. A small green upward-pointing arrow is positioned above the letter 'p'.A dark green rounded rectangular button with the text "Early Access" in white, bold, sans-serif font. A small white right-pointing arrow is centered below the text.

What pedalup.in served when TrustSniffer captured it on 2026-08-20. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: less than 1 year (registration continuity).
- Public web-archive history exists since 2016.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

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

PedalUp is a marketing landing page for a proposed smart campus mobility service in India, presenting electric e-cycle fleets for residential university campuses. It promotes sustainable, affordable transport, early-access registration, pilot deployments, and campus-scale expansion under the PedalUp brand.

Scam/Impersonation Risk

The site's presentation is consistent with a conventional mobility start-up: the homepage describes campus e-cycles, early-access participation, pilot locations, sustainability benefits, and student affordability, with no observed login form, credential collection, wallet connection, or other sensitive interaction mechanism. However, this benign page content is outweighed by confirmed external threat contradictions: four malicious detections were recorded, including a Tier-1 detection from Sophos, and the domain is reported by two blacklist sources. No page-level brand impersonation or identity inconsistency was observed, so the principal concern is the externally confirmed threat reputation rather than a demonstrated imitation of another brand. The appropriate

posture is to treat sensitive interaction as unsafe and restrict activity to passive viewing unless the external findings are independently resolved.

EVIDENCE

- The homepage is a product-marketing page for PedalUp's campus e-cycle network and contains no login or sensitive submission form.
- External reputation assessment recorded 4 malicious detections from 9 effective evaluations, with Sophos among the flagged vendors.
- The domain was identified by both VT and an external blacklist source; no Google Safe Browsing malicious result was recorded.
- Archive records show first observation on 2016-05-12, last observation on 2018-01-09, and an archive-derived domain age of 10.272416153319645 years; the historical record does not independently establish the current operator.

Regulatory Verification Notes

The reviewed landing page presents PedalUp as a mobility service and names IIM Calcutta, BIT Mesra, BIT Sindri, and NIT Rourkela as pilot campuses, but those on-page references are not independent confirmation of institutional agreements or legal affiliation. The page does not state a legal operating entity, licensing authority, or license number. This is a material disclosure gap for a service seeking campus contracts, rentals, or early-access participation, although the absence of a stated license is a verification issue rather than standalone evidence of a scam. The available identity evidence remains insufficient to connect the website independently to a verified real-world operator.

EVIDENCE

- The homepage describes a campus mobility marketplace model involving campus deployments, rentals, and early-access participation.
- The homepage names four proposed pilot campuses but supplies no independently verifiable institutional endorsement in the reviewed content.
- The registration record lists GoDaddy.com, LLC as registrar and IIM B as the organization.
- The site's transport encryption uses a DV certificate issued by YR2, valid through 2026-10-23T22:21:27+00:00.

What to Verify Next

Before any account creation, payment, institutional engagement, or collection of personal information, the operator should be confirmed through an independent corporate or institutional channel rather than relying solely on the website. The named campuses should confirm the claimed pilot relationship through contact details published on their own official websites. Any proposed rental, deposit, subscription, or early-access arrangement should be supported by written terms identifying the contracting entity, refund conditions, data handling, and dispute process. The blacklist and malicious-detection findings should also be rechecked through current independent security channels before the site is reconsidered for sensitive use.

EVIDENCE

- The homepage contains an early-access call to action but no sensitive form was observed during interaction testing.
- The homepage provides product and campus claims without an identified legal contracting entity.
- The reviewed page contains no external links, social-domain references, structured organization data, or stated licensing authority.

Summary Verdict

The overall posture is **critical trust risk** with a sensitive-interaction warning. Although the website presents a coherent and apparently ordinary business concept, the confirmed external threat contradictions and unverified operator identity prevent a trustworthy legitimacy conclusion.

Infrastructure Integrity

The site is protected by CDN/WAF infrastructure, with observed edge hosting on AS16509 (Amazon-02 — Amazon.com, Inc., US); the origin server was not observable in this analysis. This provides some exposure mitigation but does not establish legitimacy or offset the external reputation findings. The 11 abuse reports associated with 64.29.17.65 were attributed to shared Vercel CDN infrastructure, with the address whitelisted and assigned zero confidence, so that specific signal is not treated as operator-specific evidence.

EVIDENCE

- Served from AS16509, Amazon-02 — Amazon.com, Inc., US; observed edge IP: 216.198.79.1.
- The site uses CDN/WAF edge infrastructure, with 1 observed edge IP and 0 origin candidates.
- TLS validation level is DV; certificate issuer is YR2 and validity ends 2026-10-23T22:21:27+00:00.

Closing Assessment

Prospective users should limit activity to passive viewing and should not submit credentials, personal information, or financial details until the operator, institutional relationships, and external threat findings have been independently validated.

Written analysis generated 2026-08-20 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

Signals weighed against the site

- AbuseIPDB: 11 reports on hosting IP 64.29.17.65 (Vercel, Inc, Content Delivery Network), 0% confidence. The reports are attributed to shared infrastructure, not specifically to this website.

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 pedalup.in.

- The request stayed on pedalup.in. It was not redirected to another domain. CLEAR
- Registration is published under GoDaddy.com, LLC. CLEAR
- DNS for this domain is served by domaincontrol.com, across 2 name servers. NOTED
- The registration is paid up to 2027-05-23. NOTED
- The earliest public archive of this site is from 2016-05-12. CLEAR
- It is hosted on AMAZON-02, from a server in US. NOTED

Domain intelligence

Registrar	GoDaddy.com, LLC
Hosting	AMAZON-02 - Amazon.com, Inc., US
Country	US
Server IP	64.29.17.65
Name servers	ns27.domaincontrol.com, ns28.domaincontrol.com
SSL issuer	YR2
SSL expiry	2026-10-23
Domain age	0.24 years (continuous registration)
Domain expiry	2027-05-23
Archive first seen	2016-05-12
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 4 flagged AbuseIPDB: 0% confidence, 11 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about pedalup.in 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/pedalup.in> · assessed 2026-08-20