

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

darcheni.com

Verdict

0

OUT OF 100

CRITICAL RISK

darcheni.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

Governance Risk

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

What this site appears to be

A mid-maturity online grocery storefront (darcheni.com) listing food products, categories, promotions, and standard ecommerce bells-and-whistles (cart, login, register). No explicit high-risk or crypto-related activity seen in the page content.

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.

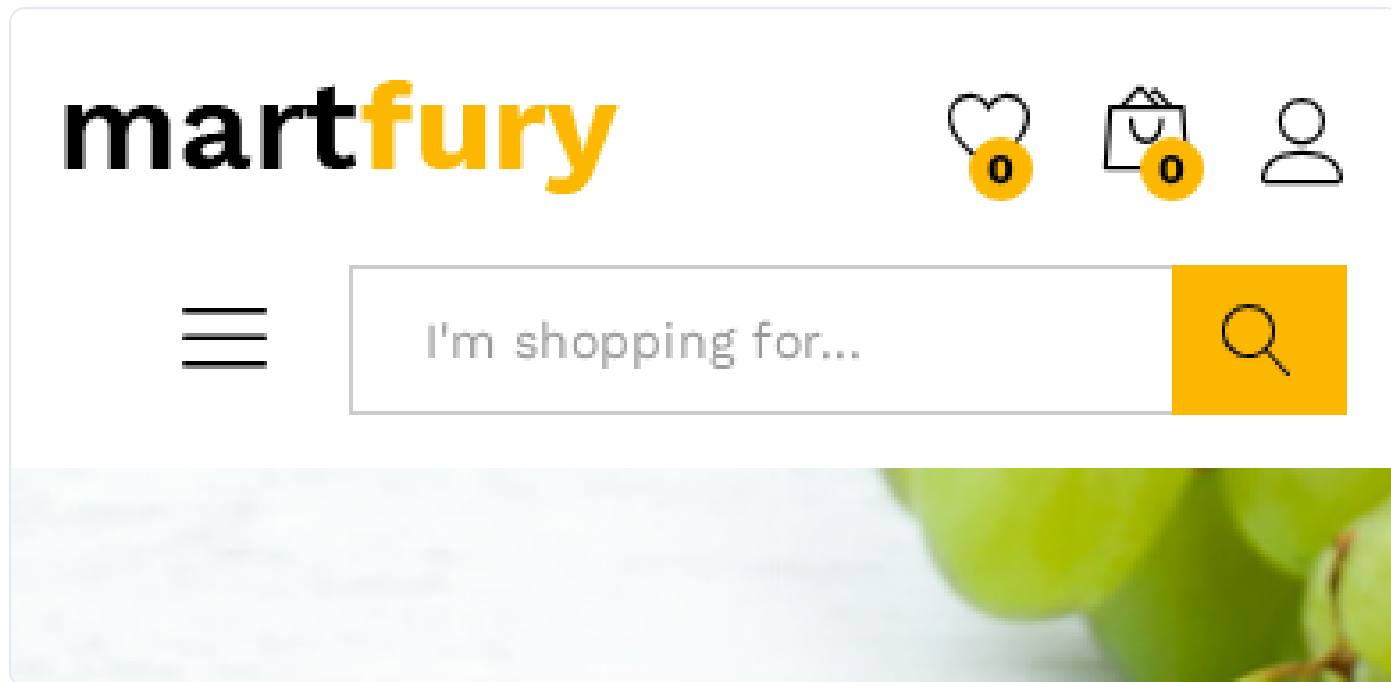
At a glance

The checks that decide most of this verdict.

Malware engines	12 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 months old Most scam domains are under a year old	RISK
Web archive	Archived since 2021 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YE2	NOTED

The page as captured

https://darcheni.com/



What darcheni.com 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 2021.
- 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.

darcheni.com presents itself as an online grocery storefront offering food products across categories such as fresh meats, vegetables, fruits, dairy, seafood, and prepared foods, supported by promotions, cart functionality, customer registration, and delivery-oriented ecommerce claims.

Scam/Impersonation Risk

The site's visible content is a conventional grocery shop and does not show cryptocurrency activity, credential-harvesting forms, brand impersonation, or conflicting legal identities. However, this benign presentation is outweighed by **confirmed blacklist status and multiple malicious threat detections**, creating a material risk for sensitive interaction despite the absence of an obvious abuse pattern in the rendered pages. The site should therefore be treated as unsuitable for login, credential submission, payment, or other financially consequential activity until the external detections are independently resolved. No identity contradiction or impersonation signal was observed. Evidence:

- The homepage contains grocery categories, product listings, promotional banners, cart functions, and login/register navigation rather than an overt high-risk financial proposition.
- External reputation checks recorded 12 malicious detections and confirmed blacklist status, including an external blacklist listing.
- The domain was registered in 2026 and is approximately 0.32 years old; the registrar is HOSTINGER operations, UAB.

Regulatory Verification Notes

The apparent business model is ordinary retail ecommerce, but the available site content does not establish the legal operator or demonstrate a verified licensing or registration basis. The presence of About, FAQs, and Contact navigation is not equivalent to independently verified corporate disclosure. The operator identity remains unverified, and governance transparency is unclear; these are verification gaps rather than proof of fraud. A separate broker-reputation dataset returned no match, which provides limited contextual information and does not constitute a licensing or regulatory determination. Evidence:

- The homepage identifies the storefront as “darcheni.com” and presents an “About Us,” “FAQs,” and “Contact” navigation structure without a verified legal-entity or license reference in the supplied content.
- The site publishes retail claims including free delivery above \$99, 90-day returns for faulty goods, secure payment, and 24/7 support; these commitments are not independently substantiated by the available evidence.
- The site is hosted on AS47583 (AS-HOSTINGER - Hostinger International Limited, CY), with TLS issued by YE2 at DV validation level and valid to 2026-09-22T04:28:29+00:00.

What to Verify Next

Before any sensitive interaction, an enterprise or prospective customer should independently confirm the operator's legal name, physical business details, return and delivery obligations, and payment-acquirer identity. Any claimed business registration or consumer-protection status should be checked against the relevant official registry, and contact channels should be validated through an independent route rather than relying solely on the website. If those checks cannot establish an accountable operator, interaction should remain limited to non-sensitive viewing. Evidence:

- The homepage exposes login and registration navigation, while the supplied form analysis found three forms consisting of search, login, and registration functions.
- The visible site content includes commercial assurances such as “Secure Payment” and “90 Days Return,” making independent confirmation of payment protection and returns material before purchase.
- The site's technical behavior showed no external posts, hidden forms, wallet activity, or clipboard-hijacking behavior during the observed runs, but this does not negate the external reputation findings.

Summary Verdict

The overall posture is **critical trust risk**. The site's conventional retail presentation and technically functional pages do not overcome the confirmed external threat detections and blacklist status, while the real-world operator identity remains unverified. Sensitive interaction is not supportable on the available evidence.

Infrastructure Integrity

The website is protected by a CDN/WAF layer, which provides some mitigation against direct exposure and common abuse techniques, but protective infrastructure is not evidence of legitimate ownership. The observed

infrastructure also includes Hostinger-hosted service and potential origin candidates behind the CDN, so the infrastructure should be treated as a mitigating control rather than a trust anchor. Evidence:

- CDN edge IPs observed: 13.248.169.48 and 76.223.54.146, both on AS16509.
- The resolved hosting infrastructure is AS47583, operated by AS-HOSTINGER - Hostinger International Limited, CY, in Germany.

Closing Assessment

Sensitive actions should be withheld unless independent operator, payment, and consumer-protection checks produce a clear and accountable basis for engagement; absent that confirmation, non-interactive viewing is the only proportionate use.

Written analysis generated 2026-08-20 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

02 Sensitive Interaction Risk

- The analysis matched a pattern TrustSniffer treats as a direct threat to a visitor.
Analysis engine signal:direct_threat
- The structure of the page changed sharply while it was loading.
Behaviour in a sandbox rule:BEHAV_DOM_DENSITY_SPIKE
- The page rewrote itself after it was interacted with, so what a visitor first sees is not what they end up on.
Behaviour in a sandbox rule:BEHAV_DOM_DIFF_AFTER_INTERACTION
- 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 darcheni.com.

- The request stayed on darcheni.com. It was not redirected to another domain. CLEAR
- Registration is published under HOSTINGER operations, UAB. CLEAR
- DNS for this domain is served by dns-parking.com, across 2 name servers. NOTED
- The registration is paid up to 2027-04-25. NOTED
- The earliest public archive of this site is from 2021-12-01. CLEAR
- It is hosted on AS-HOSTINGER, from a server in DE. NOTED

Domain intelligence

Registrar	HOSTINGER operations, UAB
Hosting	AS-HOSTINGER - Hostinger International Limited, CY
Country	DE
Server IP	2a02:4780:1:548:0:3455:b396:e
Name servers	APOLLO.DNS-PARKING.COM, ATHENA.DNS-PARKING.COM
SSL issuer	YE2
SSL expiry	2026-09-22
Domain age	0.32 years (continuous registration)
Domain expiry	2027-04-25
Archive first seen	2021-12-01
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 12 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about darcheni.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.