

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

mirashka.com

Verdict

0

OUT OF 100

CRITICAL RISK

mirashka.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 2026-08-21 by automated analysis. Classification confidence 75%.

What this site appears to be

Static coming-soon landing page for 'Mirashka' announcing a planned launch date (March 1, 2026). No forms, no social links, no monetization or transactional flows are present.

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	14 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	8.0 years old Registered history	CLEAR
Web archive	Archived since 2018 492 snapshots	CLEAR
Certificate	Encrypted connection Issued by YE1	NOTED

The page as captured

<https://mirashka.com/>



What mirashka.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: 3 to 10 years (registration continuity).
- Public web-archive history exists since 2018.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

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

Mirashka is a static coming-soon landing page presenting a brand introduction and announcing a planned launch in March 2026, with no visible commercial, account, or transactional functionality.

Scam/Impersonation Risk

The site presents no visible phishing form, login mechanism, payment flow, or brand-impersonation indicators, and its limited homepage content contains no overt fraud claims. However, this benign presentation is materially outweighed by confirmed external threat signals: the domain is blacklisted, and multiple threat-detection services identify malicious content or behavior associated with it, including Fortinet and Sophos. The available evidence therefore supports a **critical risk posture for sensitive interaction**, while the real-world operator remains unverified. No separate identity contradiction or direct impersonation finding was observed.

EVIDENCE

- The homepage is a static “Mirashka | Coming Soon” page with no forms, login fields, external links, or transactional elements.
- External threat intelligence recorded 14 malicious detections, with Fortinet and Sophos among the flagged vendors.
- The domain is listed on external blacklists; Google Safe Browsing did not report a malicious result.
- Domain registration continuity: registered 2018-08-25; approximately 7.99 years old.

Regulatory Verification Notes

The homepage identifies the project only as “Mirashka” and describes an intended digital presence; it does not provide a legal entity name, licensing information, registration number, or regulatory status. Because the site is only a launch placeholder, this is a disclosure and verification gap rather than standalone evidence of fraud. Any future financial, investment, or regulated-service functionality would require independent confirmation of the operator and the relevant authorization before engagement.

EVIDENCE

- The homepage provides a brand name, introductory description, and planned launch announcement but no legal or regulatory disclosure.
- The available page content contains no stated license authority or license number.
- No matching third-party broker profile was identified in the supplied reputational context.

What to Verify Next

Before any future login, credential submission, payment, download, or other sensitive interaction, the operator should be confirmed through an independent offline channel and any claimed corporate or regulatory status should be checked against the applicable official registry. The site should also be reassessed after launch, since the present page is too limited to establish how the announced service will operate.

EVIDENCE

- Browser testing completed 2 successful runs with 0 external XHR or fetch requests.
- The observed page exposed 0 sensitive forms, 0 wallet-provider detections, and 0 wallet-connection runs.
- The homepage returned stable content without detected cloaking, hidden forms, or suspicious inline scripts.

Summary Verdict

The website’s overall posture is critical, with sensitive interactions not supported by the available evidence. The current placeholder content does not explain or neutralize the confirmed external threat and blacklist signals, while operator identity remains unverified.

Infrastructure Integrity

The site is hosted by Hostinger International Limited through AS47583, with infrastructure registered in Ukraine and four likely origin addresses identified; no CDN or edge-IP layer was detected. Transport encryption is present, but it is a domain-validated certificate and therefore confirms encrypted delivery rather than organizational legitimacy.

EVIDENCE

- Served from AS47583 (AS-HOSTINGER – Hostinger International Limited, CY); server IP observed as 92.113.16.71 in Ukraine.
- TLS certificate issued by YE1 with DV validation, valid to 2026-11-02T06:09:17+00:00.
- Infrastructure resolution identified 4 unique IP addresses, 0 edge IPs, and 4 likely origin IPs; no CDN vendor was detected.

Closing Assessment

Sensitive interaction should not proceed unless the operator, intended service, and any applicable authorization are independently validated and the external threat status is resolved.

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, external reputation.

01 Governance Risk

- 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
- 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 mirashka.com.

- The request stayed on mirashka.com. It was not redirected to another domain. CLEAR
- Registration is published under BigRock Solutions Ltd.. CLEAR
- DNS for this domain is served by dns-parking.com, across 2 name servers. NOTED
- The registration is paid up to 2027-08-25. NOTED
- The earliest public archive of this site is from 2018-11-29. CLEAR
- It is hosted on AS-HOSTINGER, from a server in UA. NOTED

Domain intelligence

Registrar	BigRock Solutions Ltd.
Hosting	AS-HOSTINGER - Hostinger International Limited, CY
Country	UA
Server IP	2a02:4780:44:7325:a953:3ad6:b63c:7ddf
Name servers	NS1.DNS-PARKING.COM, NS2.DNS-PARKING.COM
SSL issuer	YE1
SSL expiry	2026-11-02
Domain age	7.99 years (continuous registration)
Domain expiry	2027-08-25
Archive first seen	2018-11-29
Archive snapshots	492
Reputation	VirusTotal: 14 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

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