

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

hordelo.kz

Verdict

0

OUT OF 100

CRITICAL RISK

hordelo.kz 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 75%.

What this site appears to be

Regional Russian/Kazakh bilingual (primarily Russian) newspaper site featuring local news, sports, announcements, classifieds, advertising information, contacts, and newsletter signup. Provides editorial content and advertising ordering details; contains login/registration for site users.

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	8 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	12 years old Registered history	CLEAR
Web archive	Archived since 2014 205 snapshots	CLEAR
Certificate	Encrypted connection Issued by YR1	NOTED

The page as captured

https://hordelo.kz/



What hordelo.kz served when TrustSniffer captured it on 2026-08-20. 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 2014.
- 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.

This website is a regional Russian/Kazakh bilingual newspaper platform presenting local news, sports coverage, announcements, classifieds, advertising services, radio partnerships, employment listings, and newsletter or user-account functions. Its apparent business model is local-media publishing supported by advertising placements, paid classifieds, promotional services, and related subscriptions.

Scam/Impersonation Risk

The site's visible content is consistent with a local newspaper and contains no page-level indicators of brand impersonation, phishing design, cryptocurrency activity, wallet interaction, or suspicious sensitive forms. However, this benign presentation is outweighed by confirmed external threat detections and a confirmed blacklist status, including malicious classifications from multiple evaluated sources. The site should therefore be treated as presenting a material risk for sensitive interaction, particularly login, credential submission, or financial activity. No identity contradiction between distinct legal-entity names was observed.

EVIDENCE

- The homepage presents local news, sports reporting, announcements, classifieds, advertising services, and radio-related content rather than a financial or investment offering.
- The homepage contains login, registration, and subscription/contact forms; analysis found no hidden forms, externally posted password forms, wallet-drainer activity, or external XHR activity.
- The domain has been registered since 2013 and is approximately 12.37 years old.
- Archive records show 205 snapshots from 2014-04-07 through 2025-12-04, spanning 12 tracked years with a maximum recorded gap of 1 year.

Regulatory Verification Notes

The site's apparent activity is local-media publishing and advertising rather than an explicitly regulated financial service. Its navigation includes "About the publication," history, mission, team, distribution, advertising tariffs, payment details, contacts, and related operational pages, but the supplied evidence does not establish an independently verified legal operator or regulatory status. This is an identity and governance verification gap, not a standalone finding of fraud. The absence of a matched broker signal provides no additional adverse broker-specific context, while the confirmed external blacklist remains the decisive reputational concern.

EVIDENCE

- The site navigation includes publication history, mission, team, distribution, advertising tariffs, payment details, contacts, and rules for commenting.
- The business-model evidence characterizes the service as a local newspaper funded through advertising placements, paid classifieds, radio partnerships, and promotional services.
- The site's transport encryption uses a DV certificate issued by YR1, valid through 2026-11-01.
- The site is served from AS202958, operated by Hoster-ALM - LLP _Kompaniya Hoster.KZ_, KZ.

What to Verify Next

Before any sensitive interaction, an institution should independently confirm that the domain is the intended official publication through a trusted offline contact or a separately sourced local-media reference. Any login or registration flow should be validated against the publication's independently confirmed support channels, and payment details for advertising or subscription services should be checked through a separately obtained business contact before funds are sent. If the site is being relied upon for business onboarding, its operating entity and applicable local registration or publishing requirements should be confirmed with the relevant official registry.

EVIDENCE

- The homepage provides links to “About the publication,” “Contacts,” advertising-order pages, payment details, and subscription/newsletter functions that can be checked against independently sourced contact information.
- The account surface includes both login and registration functionality, making independent confirmation of the intended service endpoint important before credentials are used.
- The site has a mid-level page-authority signal, but this is contextual evidence only and does not independently verify the operator.

Summary Verdict

The overall posture is **critical risk for sensitive interaction**. Although the website presents a coherent local-news business model and has a substantial historical web presence, the confirmed external threat and blacklist findings override those otherwise ordinary legitimacy signals. The operator’s real-world identity also remains unverified.

Infrastructure Integrity

The site resolves directly to a likely origin address rather than being placed behind a detected CDN or WAF edge network. This provides no protective CDN/WAF mitigation for the observed hosting posture; the infrastructure fact is a risk-management consideration, not proof of malicious intent.

Closing Assessment

Use should be limited to non-sensitive observation until the domain, operator, and relevant interaction channels have been independently confirmed; credentials, payments, and other sensitive actions should not be undertaken on the basis of the site’s presentation alone.

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, behaviour in a sandbox, 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
- 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 hordelo.kz.

- The request stayed on hordelo.kz. It was not redirected to another domain. [CLEAR](#)
- The earliest public archive of this site is from 2014-04-07. [CLEAR](#)
- It is hosted on Hoster-ALM, from a server in KZ. [NOTED](#)

Domain intelligence

Registrar	Not available
Hosting	Hoster-ALM - LLP _Kompaniya Hoster.KZ_, KZ
Country	KZ
Server IP	185.116.195.192
Name servers	Not available
SSL issuer	YR1
SSL expiry	2026-11-01
Domain age	12.37 years (continuous registration)
Domain expiry	Not available
Archive first seen	2014-04-07
Archive snapshots	205
Reputation	VirusTotal: 8 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about hordelo.kz 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/horde1o.kz> · assessed 2026-08-20