

Is pribregny.ru a scam? TrustSniffer's high-risk assessment: 5/100

pribregny.ru

Verdict

5

OUT OF 100

CRITICAL RISK

pribregny.ru 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 2026-08-22 by automated analysis. Classification confidence 55%.

What this site appears to be

Official site of KGBU SO 'Pribrezhny' — a regional state social-service boarding/pension home. Contains detailed service descriptions, admission rules, documents, contacts, news and links to regional portals and resources. Includes a contact form for inquiries.

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.

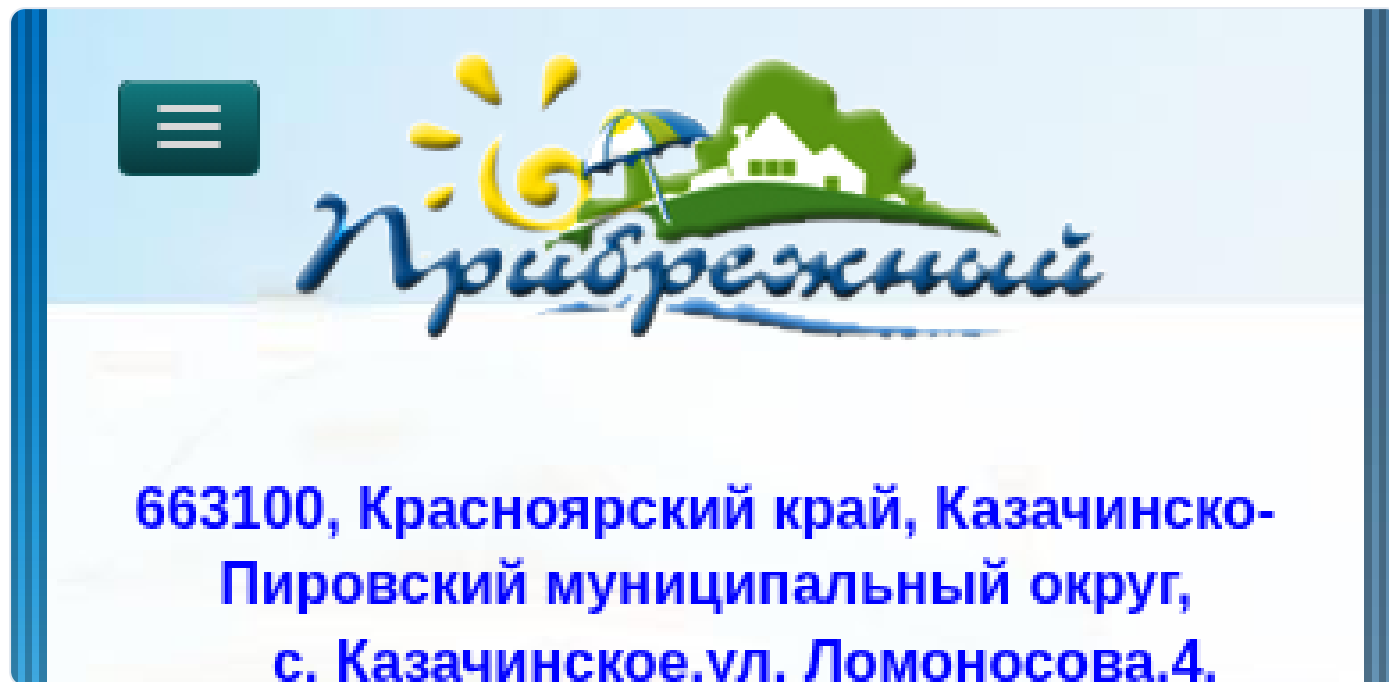
At a glance

The checks that decide most of this verdict.

Malware engines	6 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	10 years old Registered history	CLEAR
Web archive	Archived since 2016 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YR1	NOTED

The page as captured

<https://pribregny.ru/en/>



What pribregny.ru served when TrustSniffer captured it on 2026-08-22. 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 2016.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Overview

The website presents itself as the official site of KGBU SO "Pribrezhny," a regional state social-service boarding and pension institution in Krasnoyarsk Krai. It describes residential social, medical, and rehabilitative services, admission procedures, tariffs, paid accommodation, institutional documents, public reporting, contacts, and a contact form for inquiries.

Scam/Impersonation Risk

The site's institutional presentation is detailed and internally coherent, and the reviewed pages do not display a login form, payment interface, cryptocurrency function, or apparent brand-impersonation language. However, this positive page-level appearance is outweighed by confirmed external threat detections and a **blacklist** status associated with the domain. Behavioral testing also recorded suspected wallet-drainer activity in both successful runs, despite the absence of visible cryptocurrency content; this is a material technical contradiction that makes credentials, financial activity, and other sensitive interactions inappropriate. No conflicting legal-entity names or direct impersonation indicators were observed in the reviewed identity and legal content.

EVIDENCE

- External reputation assessment recorded 6 malicious and 2 suspicious detections from 8 evaluated results; the domain was also marked blacklisted.
- Behavioral testing recorded `wallet\_drainer\_runs: 2` and `wallet\_sensitive\_runs: 2`, while the homepage analysis identified no login form, hidden form, or cryptocurrency-related content.
- Domain registration records show registration on 2016-06-08 and an age of 10.21 years, through REGTIME-RU.

Regulatory Verification Notes

The services, documents, contacts, reports, tariffs, admission rules, and institutional governance materials presented on the site are consistent with a public social-service institution. Nevertheless, the reviewed content does not disclose a licensing authority or license number, and the real-world operator identity remains independently unverified. This is a regulatory and identity-verification gap rather than, by itself, proof of fraud; the decisive concern remains the external threat and blacklist evidence described above. Ownership opacity is also present, so the on-page institutional presentation should not be treated as independent proof of the operating entity.

EVIDENCE

- The services and documents sections provide admission rules, service contracts, tariffs, financial reporting, public-control materials, and institutional documents.
- The site's transport encryption uses a DV certificate issued by YR1, valid through 2026-10-24T23:14:18+00:00.
- The hosting infrastructure is served from AS50340, SELECTEL-MSK – JSC Selectel, RU, with the associated address located in RU.

What to Verify Next

Before any sensitive interaction, an independent offline or authoritative channel should confirm that the domain is genuinely operated by the named regional institution and that the published contact details are official. Any claimed authority to provide regulated social or medical services should be checked against the relevant regional government or service registry, and the domain should be excluded from credential, payment, document-upload, and financial workflows until the blacklist and behavioral findings have been resolved by the responsible security team.

EVIDENCE

- Confirm the institution's domain and contact channels through a regional government portal or independently obtained telephone number rather than relying solely on the website's contact page.
- Cross-check the institution's legal status, service authorization, and any applicable license information against the relevant official registry.
- Conduct a controlled technical review of the homepage, contact form, and linked resources before permitting access from enterprise accounts or sensitive networks.

Summary Verdict

The overall posture is critical, with a high risk of sensitive interaction and insufficient basis for trusting the domain with credentials, personal documents, payments, or other financial activity. The site’s credible institutional content does not offset the confirmed blacklist status and corroborating malicious and behavioral detections.

Infrastructure Integrity

The domain resolves directly to infrastructure operated by JSC Selectel rather than a detected CDN or WAF layer, with one resolved server address and no edge-IP layer identified. This provides no meaningful protective mitigation against the external reputation and behavioral findings.

Closing Assessment

Restrict use to passive, read-only review while independent ownership and security remediation are established; sensitive interaction should remain blocked.

Written analysis generated 2026-08-22 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 page behaved in a way consistent with a crypto wallet drainer.
Behaviour in a sandbox rule:BEHAV_WALLET_DRAINER_SUSPECT
 - 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 pribregny.ru.

- The request stayed on pribregny.ru. It was not redirected to another domain. CLEAR
- Registration is published under REGTIME-RU. CLEAR
- DNS for this domain is served by ru., across 4 name servers. NOTED
- The registration is paid up to 2027-06-08. NOTED
- The earliest public archive of this site is from 2016-03-09. CLEAR
- It is hosted on SELECTEL-MSK, from a server in RU. NOTED

Domain intelligence

Registrar	REGTIME-RU
Hosting	SELECTEL-MSK - JSC Selectel, RU
Country	RU
Server IP	81.90.181.103
Name servers	ns1.hostiman.ru., ns2.hostiman.ru., ns3.hostiman.com., ns4.hostiman.com.
SSL issuer	YR1
SSL expiry	2026-10-24
Domain age	10.21 years (continuous registration)
Domain expiry	2027-06-08
Archive first seen	2016-03-09
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 6 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about pribregny.ru 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.