

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

opticopt.ru

Verdict

0

OUT OF 100

CRITICAL RISK

opticopt.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 2026-08-21 by automated analysis. Classification confidence 55%.

What this site appears to be

Simple hosting provider default page in Russian stating the site opticopt.ru has been created and is ready to use. No services, payments, or contact information 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.

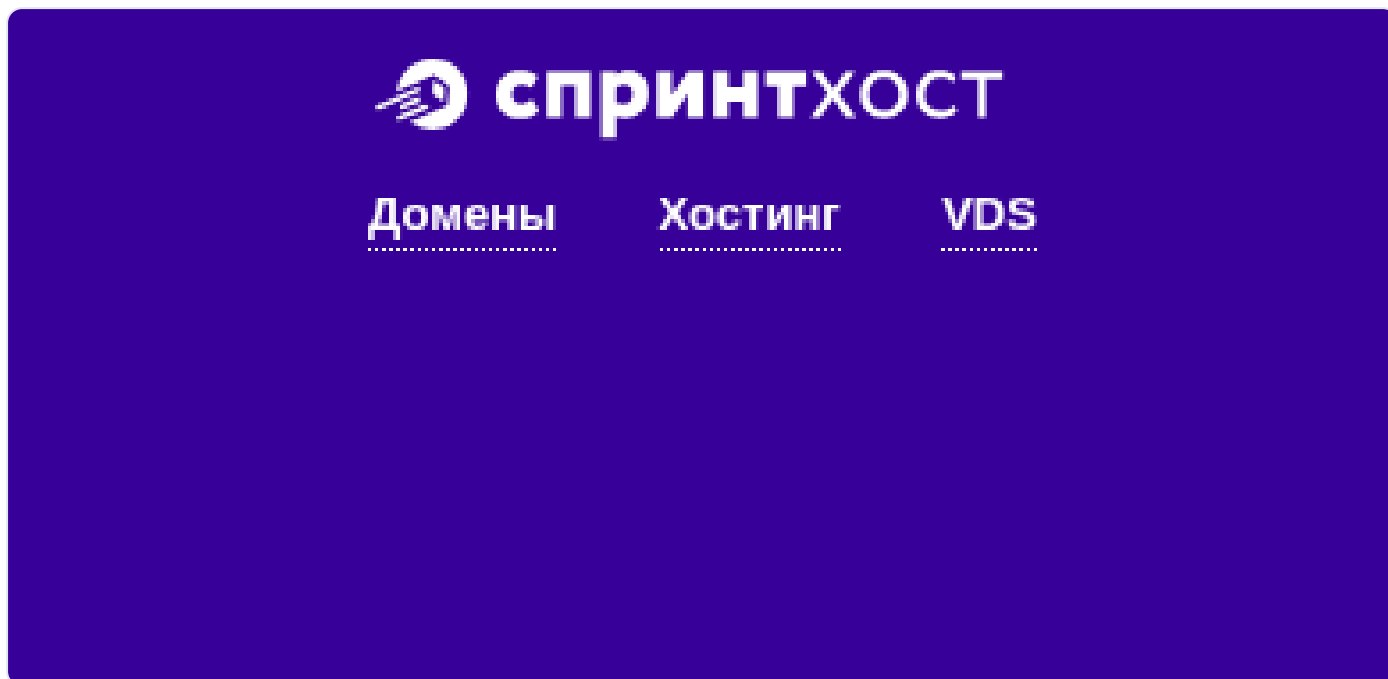
At a glance

The checks that decide most of this verdict.

Malware engines	5 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	1 months old Most scam domains are under a year old	RISK
Web archive	Archived since 2017 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YR1	NOTED

The page as captured

https://opticopt.ru/



What opticopt.ru served when TrustSniffer captured it on 2026-08-21. 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 2017.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Overview

opticopt.ru is a Russian-language placeholder website displaying a hosting-provider default page that says the site has been created and is ready for use; it presents no operating service, commercial offering, or evident business model to visitors.

Scam/Impersonation Risk

Confirmed external reputation contradictions make this a critical-risk site for sensitive interaction.

Multiple external detections classify the domain as malicious or suspicious, and the domain is present on external blacklists. The homepage itself does not show a login, payment flow, phishing form, brand impersonation, or active service; it is a minimal default page. That benign presentation does not resolve the external risk signals, particularly because the site provides no substantive identity or business context through which those signals could be explained. Archived records also show prior domain activity that conflicts with the current registration record, so continuity of control cannot be assumed.

EVIDENCE

- The domain was registered on 2026-07-07 and is recorded as approximately 0.12 years old.
- Historical records contain 23 snapshots spanning 2017–2021, covering 5 tracked years; the current registration record therefore does not by itself establish continuity with that earlier presence.
- External reputation evaluation recorded 5 malicious and 1 suspicious detections, with blacklist status confirmed by 2 external sources.
- The homepage is a Russian hosting default page with no login form, sensitive form, payment mechanism, service offering, or contact information.

Regulatory Verification Notes

The site does not present a legal entity, licensing claim, registration number, or clear governance disclosure. Its operator identity remains unverified, and the available ownership information is opaque for administrative purposes. Because the page is only a hosting placeholder, the absence of a license is a disclosure and verification gap rather than standalone proof of fraud; nevertheless, there is no on-site basis for treating the domain as a regulated or accountable service provider.

EVIDENCE

- The homepage identifies the domain as newly created and ready for use but does not identify an operating company or responsible legal entity.
- No license authority or license number is claimed in the available site content.
- The domain is registered through SPRINTNAMES-RU.
- TLS is issued by YR1 at DV validation level and is valid to 2026-10-05.

What to Verify Next

Before any sensitive interaction, an independent registry check should confirm whether a real operator exists and whether the proposed activity requires authorization. Any future claim of financial, investment, brokerage, or payment functionality should be matched to the named legal entity and verified directly with the relevant regulator. Contact and ownership details should be confirmed through an independently sourced channel rather than relying solely on information that may later appear on the domain.

EVIDENCE

- The available homepage contains no substantive business, legal, or contact disclosure to support independent attribution.
- The observed site state is a placeholder rather than an operational service, so any later change in business purpose should be assessed as a new interaction surface.
- The available identity evidence does not independently connect the domain to a verified real-world operator.

Summary Verdict

The overall posture is **critical trust risk**, with the domain unsuitable for login, credential submission, or financial interaction. The apparently inactive presentation does not offset the confirmed external reputation contradictions

or the absence of independently verified operator identity.

Infrastructure Integrity

The site is resolved directly to likely origin infrastructure, with no detected CDN or WAF layer providing meaningful edge mitigation. This reduces the protective value of the hosting arrangement and leaves the infrastructure posture dependent on the underlying provider.

EVIDENCE

- Hosted on AS35278, SPRINTHOST - SPRINTHOST.RU LLC, RU.
- Infrastructure facts record 2 unique IPs, 0 edge IPs, and 2 likely origin IPs.
- The resolved server IP is 141.8.192.186 in RU.

Closing Assessment

Sensitive interaction should not proceed unless the domain’s operator, purpose, and any applicable authorization are independently established through trusted offline or regulatory channels.

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, 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
- Most of what the page loaded came from other domains rather than from this one.
Behaviour in a sandbox rule:BEHAV_EXTERNAL_RATIO_HIGH
- The page exchanged network traffic with destinations TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_TRAFFIC
- The page sent data to a destination TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_POSTS
- The page made background requests to destinations TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_XHR
- 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 opticopt.ru.

- The request stayed on opticopt.ru. It was not redirected to another domain. CLEAR
- Registration is published under SPRINTNAMES-RU. CLEAR
- DNS for this domain is served by ru., across 4 name servers. NOTED
- The registration is paid up to 2027-07-07. NOTED
- The earliest public archive of this site is from 2017-05-06. CLEAR
- It is hosted on SPRINTHOST, from a server in RU. NOTED

Domain intelligence

Registrar	SPRINTNAMES-RU
Hosting	SPRINTHOST - SPRINTHOST.RU LLC, RU
Country	RU
Server IP	2a0a:2b42:101:ab04::
Name servers	ns1.sprinthost.ru., ns2.sprinthost.ru., ns3.sprinthost.net., ns4.sprinthost.net.
SSL issuer	YR1
SSL expiry	2026-10-05
Domain age	0.12 years (continuous registration)
Domain expiry	2027-07-07
Archive first seen	2017-05-06
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 5 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

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

This report online: <https://trustsniffer.com/report/opticopt.ru> · assessed 2026-08-21