

Is 2lo.ru safe? TrustSniffer's low-trust assessment: 25/100

2lo.ru

Verdict

25

OUT OF 100

LOW TRUST

2lo.ru is low-trust and potentially risky.

Several risk patterns were present. Do not send money or personal details until you have verified this business another way.

Sensitive Interaction Risk

Governance Risk

Assessed 2026-08-18 by automated analysis. Classification confidence 70%.

What this site appears to be

A Russian-language parked domain listing advertising the premium three-character domain 2lo.ru for sale, referencing REG.RU for purchase/transfer and showing a promo code. No forms or credential prompts 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.

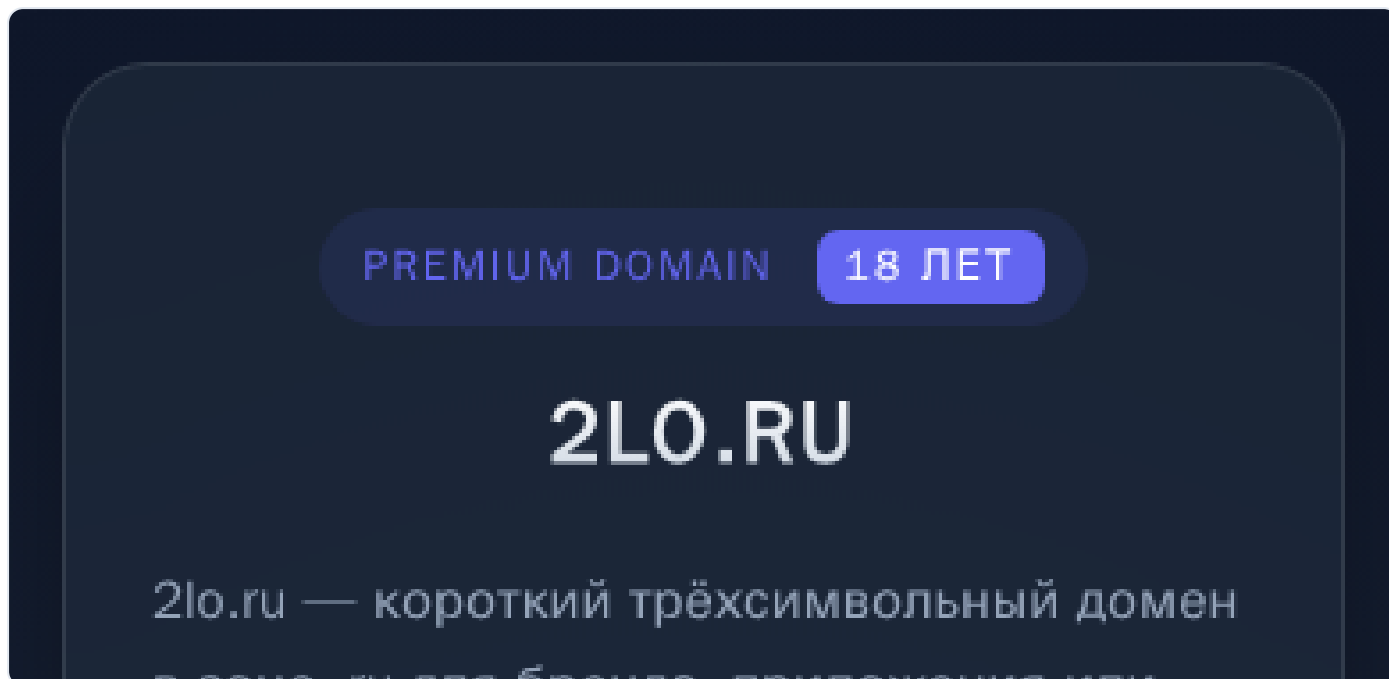
At a glance

The checks that decide most of this verdict.

Malware engines	4 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	6 months old Most scam domains are under a year old	RISK
Web archive	Archived since 2013 63 snapshots	CLEAR
Certificate	Encrypted connection Issued by YR2	NOTED

The page as captured

https://2lo.ru/



What 2lo.ru served when TrustSniffer captured it on 2026-08-18. 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 2013.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Overview

2lo.ru is a Russian-language parked-domain website offering the premium three-character .ru domain “2lo.ru” for sale, presenting potential branding uses and directing prospective buyers to REG.RU for purchase or transfer.

Scam/Impersonation Risk

The page itself presents a narrow domain-resale proposition rather than a credential-harvesting or financial-service interface: no login prompt, sensitive form, wallet connection, or active phishing mechanism was observed. However, the website is subject to a confirmed blacklist finding supported by multiple external threat detections, creating a material contradiction that outweighs the otherwise benign appearance of the parked listing. No specific brand impersonation was identified on the page, but the external reputation signal warrants treating sensitive interaction and payment activity as unsafe until the domain’s status and transaction path are independently resolved.

EVIDENCE

- Homepage: displays a premium-domain sale listing for “2lo.ru,” with no login form, credential prompt, or sensitive form.
- External reputation artifact: records a confirmed blacklist hit and malicious/suspicious detections for the domain.
- Historical domain record: 63 archive snapshots spanning 2013–2026, covering 14 tracked years; the archive-derived domain age is 13.256673511293634 years, while WHOIS records registration on 2026-02-22.

Regulatory Verification Notes

The website does not present a corporate legal entity, regulatory license, or registration number on the observed sale page. That omission is a transparency gap relevant to identifying the seller and establishing responsibility for the transaction, although the displayed business model is domain resale rather than an advertised regulated financial service. Ownership opacity remains material because the page’s commercial claims are not independently connected to a verified real-world operator. The reference to REG.RU provides a stated transaction route, but it is not proof that the seller, offer, or page is operated by that registrar.

EVIDENCE

- Homepage: identifies the asset as a premium three-character .ru domain and directs purchase or transfer through REG.RU.
- Registration record: registrar listed as REGRU-RU; creation date 2026-02-22T15:56:16Z and expiration date 2027-02-22T15:56:16Z.
- Hosting and transport telemetry: hosted on AS29182, RU-JSCIOT - JSC IOT, RU; TLS certificate issued by YR2 with DV validation, valid to 2026-10-27.

What to Verify Next

Before any sensitive interaction, an independent check should confirm that the purchase destination is the genuine registrar service and that the domain-transfer process is initiated through an independently obtained registrar channel rather than relying solely on the page’s embedded call-to-action. The prospective counterparty should also be required to provide verifiable seller identity, ownership authority, transfer terms, refund conditions, and payment-protection arrangements. Any payment or credential exchange should remain suspended until those checks reconcile the external reputation warning.

EVIDENCE

- Homepage purchase call-to-action: independently validate the destination and transaction sequence before following it.
- Domain-transfer offer: obtain documentary evidence of seller authority and confirm transfer mechanics with the registrar through an independently sourced channel.
- Commercial transaction: confirm payment protection, cancellation rights, and the responsible legal counterparty before funds are committed.

Summary Verdict

The site has a **low-trust posture with elevated sensitive-interaction risk**. Its limited, apparently benign page function does not overcome the confirmed external reputation contradiction, and the operator identity is not independently verified. The appropriate classification is therefore cautionary rather than trust-affirming.

Infrastructure Integrity

The domain resolves to one likely origin address and is not behind a detected CDN or WAF; the hosting infrastructure is RU-JSCIOT - JSC IOT, RU, on AS29182. This provides no meaningful edge-layer mitigation, so the infrastructure should be treated as a direct hosting arrangement rather than as evidence of legitimacy.

Closing Assessment

Treat the site as read-only until the blacklist status, seller identity, registrar transaction path, and payment protections have been independently validated; sensitive credentials and funds should not be committed beforehand.

Written analysis generated 2026-08-18 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
 - 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 2lo.ru.

- The request stayed on 2lo.ru. It was not redirected to another domain. CLEAR
- Registration is published under REGRU-RU. CLEAR
- DNS for this domain is served by ru., across 2 name servers. NOTED
- The registration is paid up to 2027-02-22. NOTED
- The earliest public archive of this site is from 2013-05-16. CLEAR
- It is hosted on RU-JSCIOT, from a server in RU. NOTED

Domain intelligence

Registrar	REGRU-RU
Hosting	RU-JSCIOT - JSC IOT, RU
Country	RU
Server IP	94.250.251.113
Name servers	ns1.reg.ru., ns2.reg.ru.
SSL issuer	YR2
SSL expiry	2026-10-27
Domain age	0.48 years (continuous registration)
Domain expiry	2027-02-22
Archive first seen	2013-05-16
Archive snapshots	63
Reputation	VirusTotal: 4 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about 2lo.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.