

Is fastingegoogru.vercel.app safe? TrustSniffer's low-trust assessment: 25/100

fastingegoogru.vercel.app

Verdict

25

OUT OF 100

LOW TRUST

fastingegoogru.vercel.app 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 2026-09-25 by automated analysis. Classification confidence 55%.

What this site appears to be

Russian-language page presenting a purported official video/player for a traffic-protocol record and guiding the user to download an APK and enable installation from unknown sources; lacks provenance and mirrors common malicious installer UX.

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.

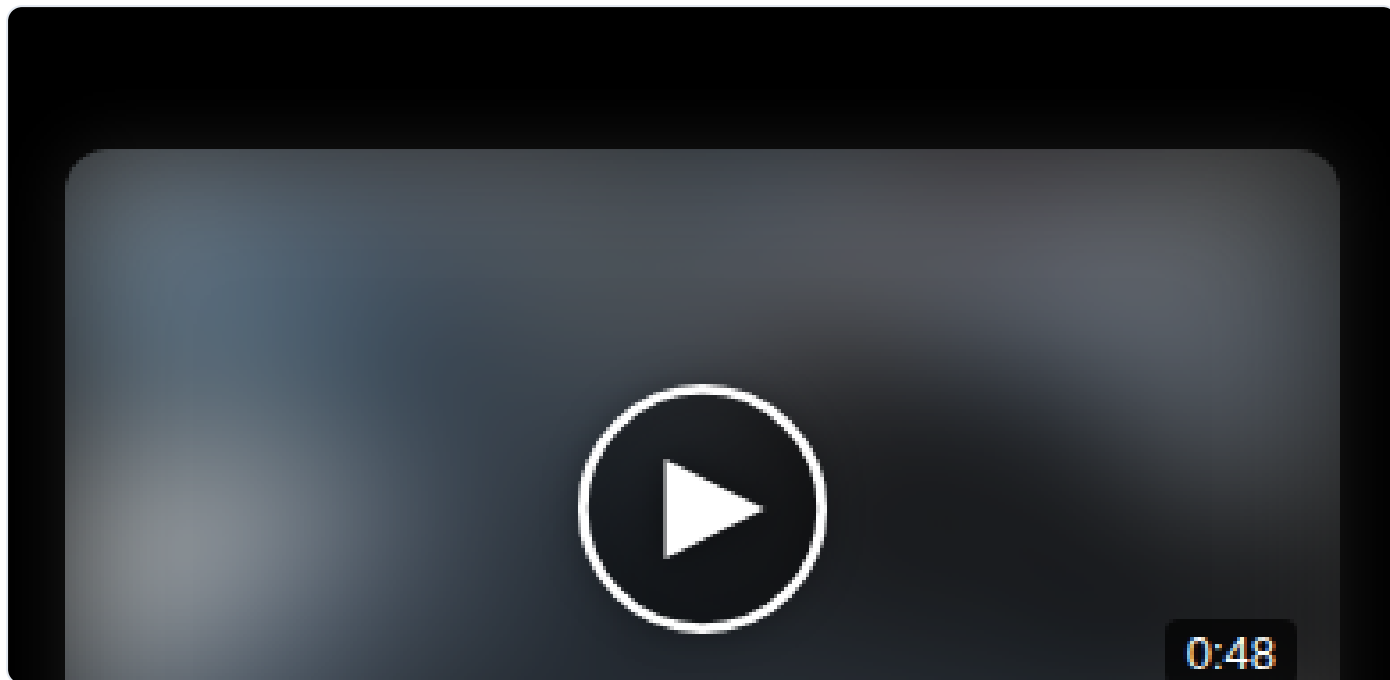
At a glance

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% confidence AbuseIPDB, 68 reports; shared hosting inflates reports	CLEAR
Domain age	Not available No registration record was returned	NOTED
Web archive	Never archived No public history of this site	WATCH
Certificate	Encrypted connection Issued by WR1	NOTED

The page as captured

<https://fastingegoogru.vercel.app/>



What fastingegoogru.vercel.app served when TrustSniffer captured it on 2026-09-25. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.
- The operator behind the site could not be independently connected to a real-world brand or person.

Full analysis

Security Alert

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

This Russian-language website presents itself as an official player for a traffic-protocol record and associated GLONASS/GPS video, but its apparent operating model is to prompt visitors to download an application package and enable installation from unknown sources rather than provide a transparent, verifiable service.

Scam/Impersonation Risk

The site presents a confirmed security concern. Its homepage claims that access to a traffic record and video is restricted, then directs the visitor through a download sequence that includes dismissing warnings and enabling installation from an unknown source. This is consistent with malicious installer or adware-distribution behavior, and external reputation checks recorded five malicious detections together with a confirmed blacklist hit. No distinct brand impersonation or conflicting legal-entity identity was identified; the principal concern is the combination of the installer workflow, absent provenance, and external malicious detections. A separate set of abuse reports concerns shared provider infrastructure and is not treated as evidence that this specific site generated those reports.

EVIDENCE

- The homepage, titled “Регистратор,” claims a verified traffic-protocol record and restricted GLONASS/GPS video access without identifying a responsible organization.
- The homepage instructs visitors to download a file, dismiss download warnings, and enable installation from an unknown source.
- External reputation checks recorded 5 malicious detections and a confirmed blacklist result for the site.

Regulatory Verification Notes

The website does not present a verifiable service identity, licensing authority, registration number, or clear legal basis for the purported official record. Its legal and governance disclosures are therefore insufficient for an organization making an official-record claim. This is a regulatory and transparency gap in its own right, while the malicious download behavior and external security findings remain the stronger basis for the overall risk assessment. The available evidence does not independently verify the real-world operator.

EVIDENCE

- The homepage provides no identified operator, responsible authority, license number, or registration detail alongside the purported official record.
- The site is served through AS16509, AMAZON-02 - Amazon.com, Inc., US.
- The site uses a DV TLS certificate issued by WR1, valid to 2026-11-27.
- The page contains no external links or independent provenance references for confirming the alleged traffic record.

What to Verify Next

Any downloaded file should remain unopened and should not be installed or granted elevated installation permissions. The alleged traffic record should be confirmed through an independently obtained official channel, such as a government or law-enforcement contact sourced separately from the website. If the file has already been opened, the affected device should be handled under established endpoint-isolation and malware-response procedures. Any future contact or support channel should be confirmed through an independent official source.

EVIDENCE

- The homepage provides only an internal download-and-install workflow for the purported record and no independent confirmation route.
- The page has no login form or sensitive data form, but its requested installation action creates a direct endpoint-security concern.
- The site’s stated purpose is not supported by a clearly identified product, organization, or accountable distribution channel.

Summary Verdict

The site has a low-trust posture with a material risk of harmful interaction. The available evidence is not sufficient to establish a legitimate operator, and the combination of contradictory security findings and unsafe

site behavior warrants treating the service as untrusted for sensitive activity.

Infrastructure Integrity

The site is protected by Cloudflare CDN/WAF infrastructure, and observed addresses are CDN edge servers rather than a directly exposed origin. The hosting arrangement includes Amazon and Vercel-associated edge infrastructure; this provides an infrastructure-layer mitigation but does not validate the site's content or operator. The 68 abuse reports associated with 216.198.79.195 are attributed to shared provider infrastructure, with a zero confidence score and a whitelist designation, so they are not independently assigned to this website.

EVIDENCE

- Cloudflare CDN/WAF protection was observed, with all six observed addresses classified as edge infrastructure and zero origin candidates identified.
- The hosting infrastructure resolves through Amazon and Vercel-associated providers.
- Abuse reporting for 216.198.79.195 is attributed to shared infrastructure rather than specifically to the website.

Closing Assessment

Prospective users and organizations should not conduct sensitive interactions with this site; any legitimate business requirement should be redirected through independently confirmed official channels and approved endpoint-security procedures.

Written analysis generated 2026-09-25 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.

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

Signals weighed against the site

- AbuseIPDB: 68 reports on hosting IP 216.198.79.195 (Vercel, Inc, Content Delivery Network), 0% confidence. The reports are attributed to shared infrastructure, not specifically to this website.

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 `fastingegoogru.vercel.app`.

- The request stayed on `fastingegoogru.vercel.app`. It was not redirected to another domain. CLEAR
- It is hosted on AMAZON-02, from a server in US. NOTED

Domain intelligence

Registrar	Not available
Hosting	AMAZON-02 - Amazon.com, Inc., US
Country	US
Server IP	216.198.79.195
Name servers	Not available
SSL issuer	WR1
SSL expiry	2026-11-27
Domain age	Not available (no registration date was returned)
Domain expiry	Not available
Archive first seen	Not available
Archive snapshots	0
Reputation	VirusTotal: 5 flagged AbuseIPDB: 0% confidence, 68 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about `fastingegoogru.vercel.app` 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.