

Is Ink.ua safe? TrustSniffer's moderate-trust assessment: 65/100

Ink.ua

Verdict

65

OUT OF 100

MODERATE TRUST

Ink.ua is moderately trusted.

Most signals looked ordinary, and some evidence was missing. Read the checks below before you pay or hand over personal details.

Governance Risk

Assessed 2026-08-20 by automated analysis. Classification confidence 50%.

What this site appears to be

Ukrainian-language URL shortening service (Ink.ua): offers free link shortening, analytics, API, QR generation, browser extensions, and paid features like custom domains. Security and anti-abuse policies are stated; Cloudflare CDN/protection mentioned.

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.

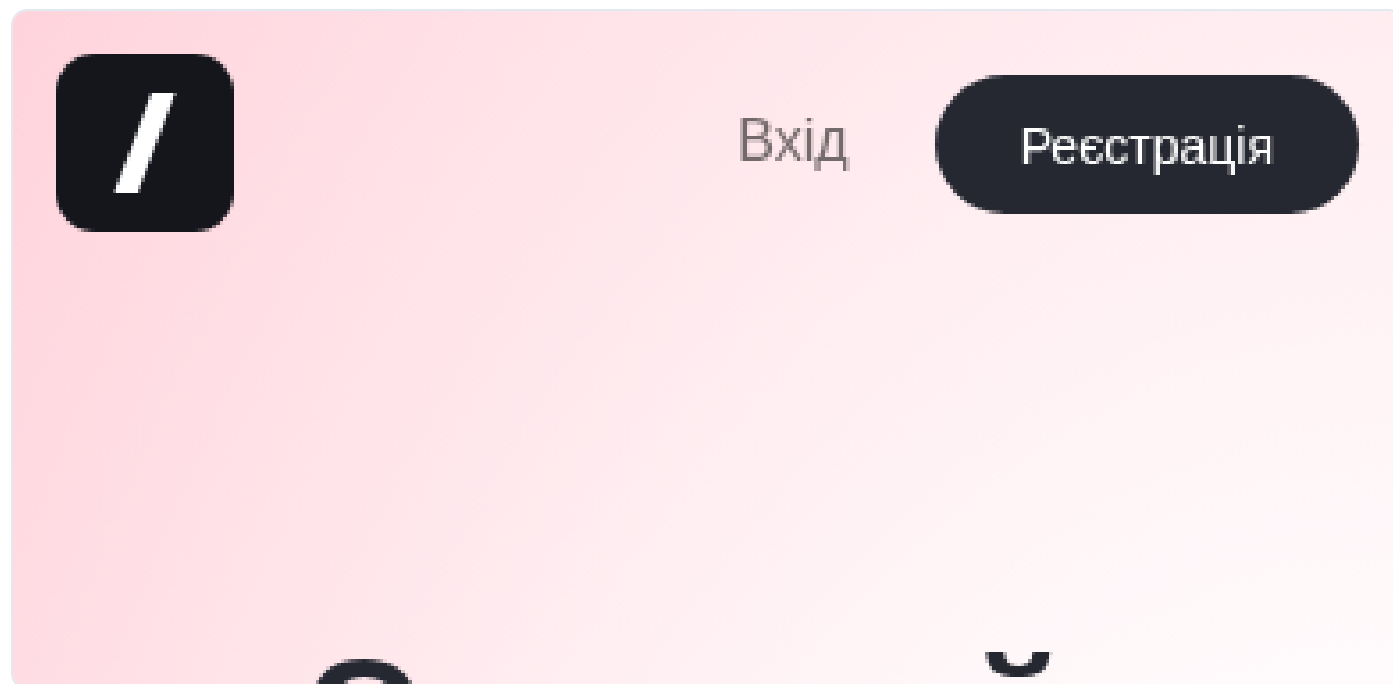
At a glance

The checks that decide most of this verdict.

Malware engines	None flagged it VirusTotal	CLEAR
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	0 reports AbuseIPDB; shared hosting inflates this count	NOTED
Domain age	2.0 years old Registered history	CLEAR
Web archive	Archived since 2024 Public history exists	CLEAR
Certificate	Encrypted connection Issued by WE1	NOTED

The page as captured

https://lnk.ua/ua



What lnk.ua served when TrustSniffer captured it on 2026-08-20. The page may look different now.

Key findings

- Automated classification: Governance Risk.
- Domain age: 1 to 3 years (registration continuity).
- Public web-archive history exists since 2024.
- No flags from the reputation services TrustSniffer consulted at assessment time.

Full analysis

Overview

lnk.ua is a Ukrainian-language URL-shortening SaaS that presents free link shortening alongside click analytics, API access, QR-code generation, browser extensions, password protection, and paid options such as custom domains and advanced analytics. Its apparent business model is subscription-based software and branded-link services for individuals, marketers, and integrations.

Scam/Impersonation Risk

No contradictions were observed. Available checks identified no confirmed malicious, phishing, impersonation, or abuse indicators, and the site's stated service model is coherent with its homepage content. The login, registration, and API-key functions are consistent with account-based SaaS operation; observed behavior showed no hidden forms, credential redirection, cloaking, wallet interaction, clipboard manipulation, or suspicious script activity. The evidence therefore supports an apparently legitimate service, while not independently proving the identity of its real-world operator.

EVIDENCE

- The homepage describes URL shortening, analytics, API integration, QR generation, browser extensions, and security or anti-abuse measures.
- The homepage includes login, registration, and API-key request functionality without an observed untrusted destination or sensitive external form.
- Behavioral testing recorded no cloaking, hidden forms, suspicious inline scripts, wallet activity, clipboard hijacking, or password submission to external forms.

Regulatory Verification Notes

The site is a software service rather than an identified regulated financial provider, and no licensing claim or license number is presented in the supplied material. Its legal-entity and governance disclosures are insufficient for independent confirmation of the operator, so legitimacy should be described as apparent and evidence-consistent rather than proven. This is a transparency and verification matter, not evidence of a scam. No adverse broker-reputation signal was identified, although that contextual result does not establish licensing or regulatory status.

EVIDENCE

- The domain registration record lists the registrar as ТОВ "Центр інтернет-імен України".
- The domain was registered on 2024-08-13 and is recorded as approximately 2.02 years old.
- The homepage provides a detailed SaaS description but does not supply a stated licensing authority or license number.

What to Verify Next

Before sensitive or high-value use, an organization should independently confirm the operating legal entity, applicable business registrations, and any licensing obligations relevant to the intended service. Account administrators should also review the site's terms, privacy, abuse-handling, and paid-service conditions, and confirm official support channels through an independently obtained source before relying on them for account recovery or payment matters.

EVIDENCE

- The operator identity remains independently unverified in the available evidence.
- The service offers account registration, API access, analytics, and paid features, creating a need to establish the responsible contracting entity before enterprise adoption.
- The homepage states that security and anti-abuse policies exist, making those policies appropriate documents for contractual and operational review.

Summary Verdict

The website presents a **moderate-trust posture**: its content, observed behavior, and external reputation signals are consistent with a functioning and apparently legitimate SaaS provider, but the available evidence does not independently verify the operator's real-world identity. No active scam or impersonation contradiction was identified.

Infrastructure Integrity

The site is protected by Cloudflare CDN/WAF infrastructure, with observed addresses limited to Cloudflare edge servers rather than a directly exposed origin. This reduces routine origin exposure and is a mitigating control, but it is not proof of operator legitimacy and can limit independent hosting verification. The transport layer uses a valid domain-validated certificate issued by WE1.

EVIDENCE

- Served from AS13335 (Cloudflare, Inc.; CLOUDFLARENET, US).
- TLS certificate validation level: DV; issuer: WE1; valid to 2026-11-17T20:53:17+00:00.
- Four observed IP addresses were identified as Cloudflare edge addresses; likely origin IP count: 0.

Closing Assessment

Ordinary, lower-sensitivity use is proportionate to the available evidence, while independent entity and regulatory checks should precede high-value commitments, privileged integrations, or other sensitive actions.

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 registration and ownership.

01 Governance Risk

- The public registration record for this domain is incomplete.
Registration and ownership rule:KF_WHOIS_INCOMPLETE

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 lnk.ua.

- The request stayed on lnk.ua. It was not redirected to another domain. CLEAR
- Registration is published under ТОВ "Центр інтернет-імен України". CLEAR
- DNS for this domain is served by cloudflare.com, across 2 name servers. NOTED
- The registration is paid up to 2027-08-13. NOTED
- The earliest public archive of this site is from 2024-09-09. CLEAR

- It is hosted on CLOUDFLARENET, from a server in US. NOTED

Domain intelligence

Registrar	TOB "Центр інтернет-імен України"
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US
Server IP	2606:4700:3031::ac43:a83b
Name servers	janet.ns.cloudflare.com, simon.ns.cloudflare.com
SSL issuer	WE1
SSL expiry	2026-11-17
Domain age	2.02 years (continuous registration)
Domain expiry	2027-08-13
Archive first seen	2024-09-09
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 0 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about lnk.ua 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/lnk.ua> · assessed 2026-08-20