

Is 2ur.jp a scam? TrustSniffer's high-risk assessment: 0/100

2ur.jp

Verdict

0

OUT OF 100

CRITICAL RISK

2ur.jp 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 2026-08-18 by automated analysis. Classification confidence 70%.

What this site appears to be

A straightforward URL shortener and QR code generator (2ur) with basic site pages (FAQ, Terms, Privacy) and social share links; no credential prompts or financial services detected.

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	14 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	2.0 years old Registered history	CLEAR
Web archive	Archived since 2024 140 snapshots	CLEAR
Certificate	Encrypted connection Issued by YR1	NOTED

The page as captured

https://2ur.jp/



Shorten URL

FAQs

Terms

Privacy

Contact us



What 2ur.jp served when TrustSniffer captured it on 2026-08-18. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: 1 to 3 years (registration continuity).
- Public web-archive history exists since 2024.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

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

What is presented is 2ur.jp, a utility website offering free URL shortening and QR-code generation. Its homepage describes shortened links, QR creation, click counting, newsletter registration, and supporting FAQ, Terms, Privacy, and Contact pages; its apparent business model is a general-purpose link utility potentially supported by advertising, analytics, or optional paid features.

Scam/Impersonation Risk

The site presents as a straightforward utility rather than a financial or credential-collection service, and no brand impersonation, phishing form, login prompt, or identity contradiction was observed in the supplied page analysis. However, the domain is **blacklisted** by multiple external sources and is associated with multiple malicious and suspicious detections, including confirmed threat detections from Fortinet, Kaspersky, and Sophos. That external reputation conflict is materially more significant than the benign appearance of the homepage and supports a clearly cautionary posture for sensitive interaction. The site's link-redirection function also means that shortened destinations should not be trusted solely because they originate from this service.

EVIDENCE

- External reputation telemetry recorded 14 malicious detections and 1 suspicious detection; Fortinet, Kaspersky, and Sophos were among the flagged vendors, and the domain was marked blacklisted by 2 external sources.
- The homepage and functional pages contain a URL-shortening form and newsletter form, but no login form, password field, hidden sensitive form, wallet connection, or financial-service mechanism.
- Domain registration telemetry records creation on 2024-09-03, with an age of 1.96 years.

Regulatory Verification Notes

The site provides Terms, Privacy, FAQ, and Contact pages, which is a positive structural disclosure signal, but the supplied content does not establish an independently verified legal operator or any applicable license or registration. The identity assessment remains likely rather than verified. The available technical controls show ordinary transport security and identifiable hosting, but neither establishes legitimacy or resolves the external reputation conflict.

EVIDENCE

- The archive records 140 snapshots spanning 2024-12-05 through 2026-05-16, covering 3 tracked years.
- The site is served from AS9370, SAKURA-B - SAKURA Internet Inc., JP.
- The TLS certificate is issued by YR1 at DV validation level and is valid to 2026-11-13.

What to Verify Next

Before any sensitive use, an organization should independently confirm the operator named in the site's legal materials and establish an offline or independently sourced contact route. Any shortened link should be expanded or inspected through a controlled security process before access to the destination, and browser or endpoint protections should remain active. If the service is being procured for enterprise use, its abuse-handling, data-retention, analytics, and destination-screening practices should be documented contractually.

EVIDENCE

- The Terms, Privacy, FAQ, and Contact pages provide the available locations for operator, data-processing, and abuse-handling verification.
- The homepage states that the service counts clicks and offers newsletter registration, making analytics and retention terms relevant to procurement review.
- The site's page analysis found no financial-service or credential-collection workflow, so verification should focus on link safety, data handling, and operator accountability.

Summary Verdict

The overall posture is **critical trust with sensitive-interaction risk**. Although the website has a coherent utility presentation and supporting informational pages, the confirmed external reputation contradictions prevent the available evidence from supporting ordinary trust in sensitive interactions. The real-world operator identity is likely connected to the site but is not independently verified.

Infrastructure Integrity

The site resolves directly to a single likely origin address, with no CDN or WAF detected and no edge-IP layer identified. Its hosting infrastructure is therefore identifiable but provides limited protective separation between the public service and its origin; infrastructure characteristics should be treated only as context, not as evidence of legitimacy.

Closing Assessment

The service should be limited to non-sensitive, read-only assessment until the operator, link-safety controls, and external reputation concerns have been independently resolved; credentials, financial activity, and other sensitive interactions should not be conducted through it.

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	LIKELY
Identity score	76/100
Identity verification confidence	76%

- Trusted social count=2

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 2ur.jp.

- The request stayed on 2ur.jp. It was not redirected to another domain. CLEAR
- DNS for this domain is served by ne.jp, across 2 name servers. NOTED
- The registration is paid up to 2026-09-30. NOTED
- The earliest public archive of this site is from 2024-12-05. CLEAR
- It is hosted on SAKURA-B, from a server in JP. NOTED

Domain intelligence

Registrar	Not available
Hosting	SAKURA-B - SAKURA Internet Inc., JP
Country	JP
Server IP	160.16.237.149
Name servers	ns1.dns.ne.jp, ns2.dns.ne.jp
SSL issuer	YR1
SSL expiry	2026-11-13
Domain age	1.96 years (continuous registration)
Domain expiry	2026-09-30
Archive first seen	2024-12-05
Archive snapshots	140
Reputation	VirusTotal: 14 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

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