

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

2ww.me

Verdict

0

OUT OF 100

CRITICAL RISK

2ww.me 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

Thai-language URL shortening service offering a bookmarklet, API, and simple stats (total hits, total URLs, today's URLs). No obvious financial or credential harvesting elements in visible content.

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	12 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	7.0 years old Registered history	CLEAR
Web archive	Archived since 2013 105 snapshots	CLEAR
Certificate	Encrypted connection Issued by WE1	NOTED

The page as captured

<https://2ww.me/>

เว็บย่อลิงค์

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

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: 3 to 10 years (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

Security Alert

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

The website is a Thai-language URL-shortening utility that offers visitors a bookmarklet, an API, and basic usage statistics, including total hits, total URLs, and URLs created today. Its apparent business model is to provide link-shortening infrastructure, potentially supported by advertising or analytics.

Scam/Impersonation Risk

The site's visible homepage content is a simple utility interface and does not show login forms, credential collection, financial services, or other obvious phishing mechanics. However, this benign presentation is outweighed by confirmed external security contradictions: the domain is blacklisted, 12 security evaluations classified it as malicious, one classified it as suspicious, and two security vendors generated threat detections. The absence of an apparent brand-impersonation pattern does not resolve the external reputation issue, and the deterministic assessment therefore treats sensitive interaction as unsafe. No separate identity inconsistency was observed across the supplied evidence.

EVIDENCE

- The homepage presents URL shortening, a bookmarklet, an API reference, and usage counters, with no sensitive form detected.
- External security telemetry recorded 12 malicious detections, 1 suspicious detection, and a confirmed blacklist status for the domain.
- The domain was registered on 2019-08-06 and has a recorded age of 7.04 years; the registrar is PDR Ltd. d/b/a PublicDomainRegistry.com.
- Historical records contain 105 snapshots spanning 2013–2026, with 14 years tracked.

Regulatory Verification Notes

The site exposes About, Terms and Conditions, Contact, and API navigation, but the supplied page evidence does not establish a clearly disclosed legal operator or verified regulatory status. No license is claimed or independently verified; for a URL-shortening service this is primarily a transparency and operator-identification matter rather than evidence of a regulated financial activity. Identity verification remains unconfirmed, so the site's apparent utility function should not be treated as proof of a known real-world operator. The separate broker-reputation dataset produced no match, which provides no affirmative regulatory assurance.

EVIDENCE

- The homepage navigation includes About, Terms and Conditions, Contact, API, and Bookmarklet sections, while the available disclosure state is unclear.
- The site is served through AS13335, CLOUDFLARENET - Cloudflare, Inc., US.
- The transport certificate is DV-validated, issued by WE1, and valid to 2026-10-24T10:19:40+00:00.
- No verified license authority or license number is presented in the supplied business-model evidence.

What to Verify Next

Before any interactive use, an enterprise security team should confirm the domain's current reputation and blacklist status through its own security controls and determine whether the shortened links resolve to destinations appropriate for the intended business purpose. The operator's legal identity and official support channels should be confirmed through an independent route, and any applicable registration or licensing position should be checked with the relevant jurisdictional registry. Until those checks are complete, use should remain limited to non-interactive observation rather than account access, credential submission, or financial activity.

EVIDENCE

- The homepage has no login form, hidden form, password submission, or detected sensitive form.
- Observed browser behavior recorded zero external XHR requests, zero suspicious inline scripts, no cloaking, and no wallet-provider activity across two successful runs.
- The site's visible content contains no stated license number or licensing authority.
- The displayed service is a link-shortening platform, making destination inspection material to assessing any proposed use.

Summary Verdict

The website presents a coherent, low-complexity utility interface, but the confirmed blacklist and malicious security detections establish a **critical trust posture**. Apparent technical stability and ordinary page content do not overcome those contradictions, and the operator’s real-world identity is not independently verified.

Infrastructure Integrity

Cloudflare CDN/WAF protection provides a mitigating layer against direct exposure of the service infrastructure, but it is not evidence of legitimacy. The observed infrastructure includes Cloudflare edge addresses and one potential origin candidate, so the protective layer should be viewed as an architectural control rather than a trust endorsement.

EVIDENCE

- Cloudflare edge IPs observed: 104.21.20.80, 172.67.191.251, 2606:4700:3037::6815:1450, and 2606:4700:3037::ac43:bffb.
- All four observed edge addresses are associated with AS13335; infrastructure resolution identified 5 unique addresses in total, including 1 likely origin candidate.

Closing Assessment

The appropriate institutional posture is to restrict activity to controlled, non-sensitive observation while the reputation status, destination behavior, and operator identity are independently investigated. No credentials, account access, payment details, or other sensitive actions should be permitted without a documented security exception and successful verification.

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, external reputation.

01 Governance Risk

- The registration record withholds contact details for the operator.
Registration and ownership rule:KF_WHOIS_HIDDEN
- 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
- 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	25%

- 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 2ww.me.

- The request stayed on 2ww.me. It was not redirected to another domain. CLEAR
- Registration is published under PDR Ltd. d/b/a PublicDomainRegistry.com. CLEAR
- The registration is paid up to 2027-08-06. NOTED
- The earliest public archive of this site is from 2013-03-01. CLEAR
- It is hosted on CLOUDFLARENET, from a server in US. NOTED

Domain intelligence

Registrar	PDR Ltd. d/b/a PublicDomainRegistry.com
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US
Server IP	2606:4700:3037::ac43:bff6
Name servers	Not available
SSL issuer	WE1
SSL expiry	2026-10-24
Domain age	7.04 years (continuous registration)
Domain expiry	2027-08-06
Archive first seen	2013-03-01
Archive snapshots	105
Reputation	VirusTotal: 12 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about 2ww.me 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/2ww.me> · assessed 2026-08-18