

Is dangbong.xyz a scam? TrustSniffer's high-risk assessment: 0/100

dangbong.xyz

Verdict

0

OUT OF 100

CRITICAL RISK

dangbong.xyz 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 2026-08-21 by automated analysis. Classification confidence 55%.

What this site appears to be

Very small page with ~3 characters of visible text. No metadata, links, forms, or social signals detected. Appears to be a login-only or placeholder page with no contextual information.

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.

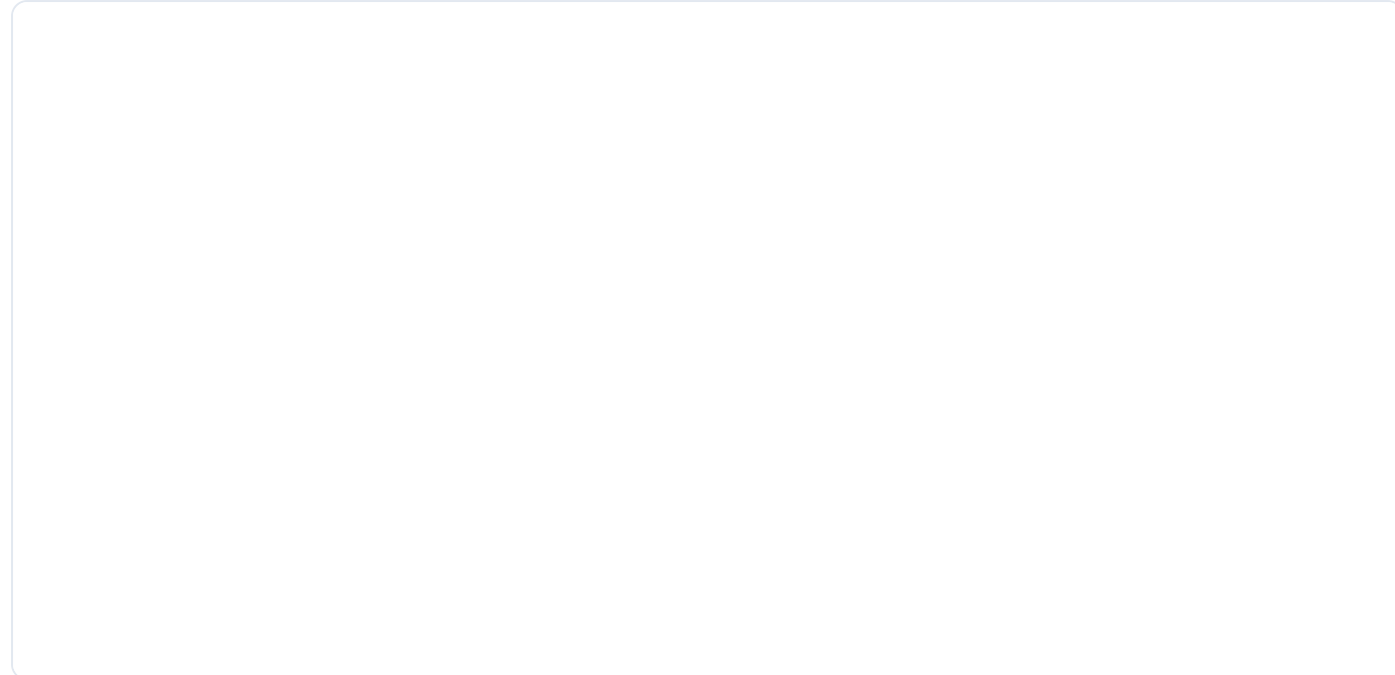
At a glance

The checks that decide most of this verdict.

Malware engines	11 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	3 months old Most scam domains are under a year old	RISK
Web archive	Archived since 2018 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YR2	NOTED

The page as captured

<https://bulsis.net/go/2781248>



What dangbong.xyz served when TrustSniffer captured it on 2026-08-21. 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 2018.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

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

The website is a minimal login-only or placeholder surface at dangbong.xyz. It presents approximately three visible characters, with no service description, business identity, navigation, metadata, or contextual explanation of its purpose or monetization.

Scam/Impersonation Risk

A confirmed **blacklist** contradiction and malicious threat detections create a critical risk posture for sensitive interaction. External assessment recorded 11 malicious and 2 suspicious detections, with Kaspersky and Sophos among the flagged vendors; this is materially stronger than an isolated reputation anomaly. The page also exhibits hidden forms, two suspicious inline scripts, and non-whitelisted external posts, while providing no context that would allow a visitor to establish what service is being accessed. No separate brand-impersonation finding or conflicting legal-entity identity was observed, but those absences do not offset the confirmed blacklist and malicious-detection evidence.

EVIDENCE

- Homepage: approximately 3 visible characters; classified as a login-only or unknown page with no service description or verifiable business identity.
- Page behavior: hidden forms detected in both observed runs, with 2 suspicious inline scripts and 2 non-whitelisted external posts.
- External reputation: 11 malicious and 2 suspicious detections; Kaspersky and Sophos were identified among the flagged vendors.
- Domain provenance: registered 2026-05-27 and recorded as approximately 0.24 years old; historical records contain 43 snapshots spanning 2018–2026, tracked across 9 years, which does not establish continuity of the current operator.

Regulatory Verification Notes

The operator identity is unverified and the available page content does not provide a meaningful legal, corporate, licensing, or governance disclosure. No license claim, licensing authority, or license number is present in the available business-model evidence. The historical record and transport certificate demonstrate technical or archival artifacts, not regulatory authorization or proof that the current operator is connected to any established entity. The appropriate interpretation is therefore a substantial verification gap rather than a licensing conclusion.

EVIDENCE

- Available site content: no company name, legal identity, licensing authority, registration number, or service disclosure was identified.
- Registration record: registrar listed as Dynadot Inc.; creation date 2026-05-27T02:57:04Z and expiration date 2027-05-27T23:59:59Z.
- Hosting infrastructure: served from AS24940, HETZNER-AS - Hetzner Online GmbH, DE.
- Transport encryption: TLS certificate issued by YR2, domain validation (DV), valid to 2026-11-15T23:20:07+00:00.

What to Verify Next

Before any sensitive interaction, an institution should independently confirm that the domain is an authorized endpoint for a known organization through an established, offline or previously trusted contact channel. Any claimed operator, license, or regulated activity should be matched against the relevant official corporate and regulatory registries using independently sourced organization details. Security teams should also preserve the page and browser-behavior evidence, block authentication attempts to the domain, and review endpoint or network telemetry for prior access.

EVIDENCE

- Homepage and login surface: insufficient information is available to identify the service or establish an accountable operator.
- Legal and business disclosure: no license claim or verifiable regulatory identity is present for independent registry matching.
- Browser behavior: hidden forms and suspicious inline scripts warrant retention of relevant security telemetry for investigation.
- Site transport: the certificate provides encrypted transport but does not authenticate the underlying business or operator.

Summary Verdict

The site warrants a **critical-trust posture** with elevated risk for credentials, authentication, and financial activity. The available evidence is not sufficient to establish a legitimate operator, and the combination of confirmed blacklist status, malicious detections, and a context-free login surface makes sensitive interaction inappropriate.

Infrastructure Integrity

The site uses CDN/WAF protection, with observed edge addresses on AS24940; the origin server was not observable in this analysis. This infrastructure provides some exposure mitigation, but it is only a protective technical control and cannot counter the site's external threat-reputation findings.

Closing Assessment

Prospective users and organizations should not authenticate, submit credentials, or conduct financial activity through this site; any required engagement should remain limited to controlled investigation and independently validated channels.

Written analysis generated 2026-08-21 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, page content, 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
- The page presents a sign-in form, and the operator behind it could not be independently verified.
Page content rule:PAGE_TYPE_LOGIN_UNVERIFIED

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
- The page sent data to a destination TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_POSTS
- The page carried inline scripts written in a style TrustSniffer treats as suspicious.
Behaviour in a sandbox rule:BEHAV_SUSPICIOUS_INLINE_SCRIPTS
- The page contained a form a visitor cannot see.
Behaviour in a sandbox rule:BEHAV_HIDDEN_FORMS
- 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 dangbong.xyz.

- The request for dangbong.xyz ended on bulsis.net, a different domain. WATCH
- Registration is published under Dynadot Inc. CLEAR
- DNS for this domain is served by park-my-domain.net, across 2 name servers. NOTED
- The registration is paid up to 2027-05-27. NOTED
- The earliest public archive of this site is from 2018-08-13. CLEAR
- It is hosted on HETZNER-AS, from a server in DE. NOTED

Domain intelligence

Registrar	Dynadot Inc
Hosting	HETZNER-AS - Hetzner Online GmbH, DE
Country	DE
Server IP	157.90.33.74

Name servers	NS1.PARK-MY-DOMAIN.NET, NS2.PARK-MY-DOMAIN.NET
SSL issuer	YR2
SSL expiry	2026-11-15
Domain age	0.24 years (continuous registration)
Domain expiry	2027-05-27
Archive first seen	2018-08-13
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 11 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about dangbong.xyz 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/dangbong.xyz> · assessed 2026-08-21