

Is a551008.cc a scam? TrustSniffer's high-risk assessment: 0/100

a551008.cc

Verdict

0

OUT OF 100

CRITICAL RISK

a551008.cc 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 2026-08-22 by automated analysis. Classification confidence 55%.

What this site appears to be

Landing page for an online casino/gambling brand offering live dealers and multiple mirror links/IP endpoints and urging users to download an app and register. Presents alternate domains and IP addresses to bypass blocks and encourages bookmarking.

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	17 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 Public history exists	CLEAR
Certificate	Encrypted connection Issued by WE1	NOTED

The page as captured

<https://a551008.cc/>



What a551008.cc served when TrustSniffer captured it on 2026-08-22. 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.

The website is a gambling and mirror-link landing page presenting live dealers, sports betting, electronic games, esports, fishing and card games under the “K8” and “Phoenix Sports” branding. Its apparent purpose is to direct visitors toward registrations, app downloads, alternate domains and direct IP endpoints for gambling platforms, with monetisation dependent on user deposits, referrals or related sign-ups.

Scam/Impersonation Risk

The site presents a confirmed **blacklist-based contradiction** and should be treated as high risk for sensitive interaction. External security detections include 17 malicious classifications, including detections from Fortinet, Kaspersky and Sophos, and the domain is listed by external blacklist sources. The landing page compounds that concern by directing visitors through multiple mirror domains and direct IP endpoints, encouraging bookmarking of alternate routes, promoting an app download, and using a privacy-related warning that advises against using the site on the same device as the “国家反诈中心” application. Its stated assurances, including “international major brand” positioning and “large-amount worry-free” claims, are not supported by identifiable

evidence on the page. No identity-name conflict was observed, but the confirmed blacklist and malicious detections are sufficient to establish a material security concern.

EVIDENCE

- The homepage displays six external destinations, including two direct IP endpoints, alongside “main,” “recommended” and “backup” routes.
- The homepage urges visitors to register, download an application and bookmark both the alternate route and the landing page.
- The homepage carries the claims “K8凯发-国际大品牌 信誉保障 大额无忧” and “凤凰体育(中国)官方网站” without supporting corporate or operational evidence.
- The domain is recorded as registered on 2026-06-24, with an age of 0.16 years.

Regulatory Verification Notes

The available landing page does not state a licensing authority, license number, legal entity or verifiable operating address. That is a regulatory transparency gap rather than independent proof of fraud, but it is significant because the site solicits gambling registrations and deposits while routing visitors through alternate destinations. The published business model includes deposit-before-service, opaque value flow, unsupported claims and an unverifiable contact or address position. A separate broker-reputation dataset produced no matching record; this is only contextual and does not establish licensing or regulatory standing.

EVIDENCE

- The homepage describes live-dealer, sports, electronic, esports, fishing and card-gaming services but provides no visible licensing authority or license number.
- The homepage routes registration and app-download activity to alternate domains and IP endpoints rather than presenting a clearly identified operating entity.
- Hosting infrastructure is served from AS13335, CLOUDFLARENET — Cloudflare, Inc., US.
- The site's TLS certificate is issued by WE1 at DV validation level and is valid to 2026-10-14.

What to Verify Next

Before any interaction involving registration, application installation, credentials or funds, an independent gambling regulator should confirm the operator's legal entity, domain and license status through its official registry. The advertised payment and withdrawal arrangements should be validated independently, including the beneficiary identity, dispute process and availability of consumer protections. Contact details and official support channels should be confirmed through an offline or independently sourced route, and any application should be obtained only from an official, verifiable distribution channel rather than from the landing page or its mirrors.

EVIDENCE

- The homepage provides no license number or regulator that can be checked directly.
- The homepage relies on alternate domains, direct IP endpoints and an app-download call to action.
- The page-level assessment identifies deposit-before-service, opaque value flow, claim-evidence dissonance and unverifiable contact or address signals.

Summary Verdict

The overall posture is **critical trust risk**, with the available evidence supporting avoidance of sensitive interaction. The site’s apparent gambling function, routing model and external threat reputation do not provide a defensible basis for account, credential or financial engagement.

Infrastructure Integrity

Cloudflare CDN/WAF protection provides a mitigating layer against direct exposure of the underlying service, but it does not establish operator legitimacy. All observed addresses are Cloudflare edge infrastructure, including 104.21.35.188 and the associated IPv4 and IPv6 edge addresses; no origin candidate was identified.

Closing Assessment

The appropriate institutional action is to block or isolate the domain and prevent downloads, registrations, credential submission and financial transactions until independent regulatory, ownership and payment-channel validation has been completed.

Written analysis generated 2026-08-22 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, page content, external reputation.

01 Governance Risk

- The registration record withholds contact details for the operator.
Registration and ownership rule:KF_WHOIS_HIDDEN
- Registration details are held behind a privacy service, so no operator is named publicly. This is common and legal, and it also means there is nobody to check.
Registration and ownership rule:KF_WHOIS_PRIVATE

02 Sensitive Interaction Risk

- The analysis matched a pattern TrustSniffer treats as a direct threat to a visitor.
Analysis engine signal:direct_threat
- A form on the page submits to a destination TrustSniffer could not verify.
Page content rule:PAGE_FORM_UNTRUSTED_DEST
- 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 a551008.cc.

- The request stayed on a551008.cc. It was not redirected to another domain. CLEAR
- Registration is published under DYNADOT LLC. CLEAR
- DNS for this domain is served by cloudflare.com, across 2 name servers. NOTED
- The registration is paid up to 2027-06-24. NOTED
- The earliest public archive of this site is from 2024-08-07. CLEAR
- It is hosted on CLOUDFLARENET, from a server in US. NOTED

Domain intelligence

Registrar	DYNADOT LLC
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US
Server IP	2606:4700:3030::6815:23bc
Name servers	DEVIN.NS.CLOUDFLARE.COM, MELISSA.NS.CLOUDFLARE.COM
SSL issuer	WE1
SSL expiry	2026-10-14
Domain age	2.04 years (continuous registration)
Domain expiry	2027-06-24
Archive first seen	2024-08-07
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 17 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about a551008.cc 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.

