

Is dd365g.cc a scam? TrustSniffer's high-risk assessment: 0/100

dd365g.cc

Verdict

0

OUT OF 100

CRITICAL RISK

dd365g.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 2026-08-20 by automated analysis. Classification confidence 55%.

What this site appears to be

A short Chinese-language landing/portal page offering two access lines to 3652aa.com and an online customer service link. No forms, no contact details, and no clear monetization or regulatory signals.

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.

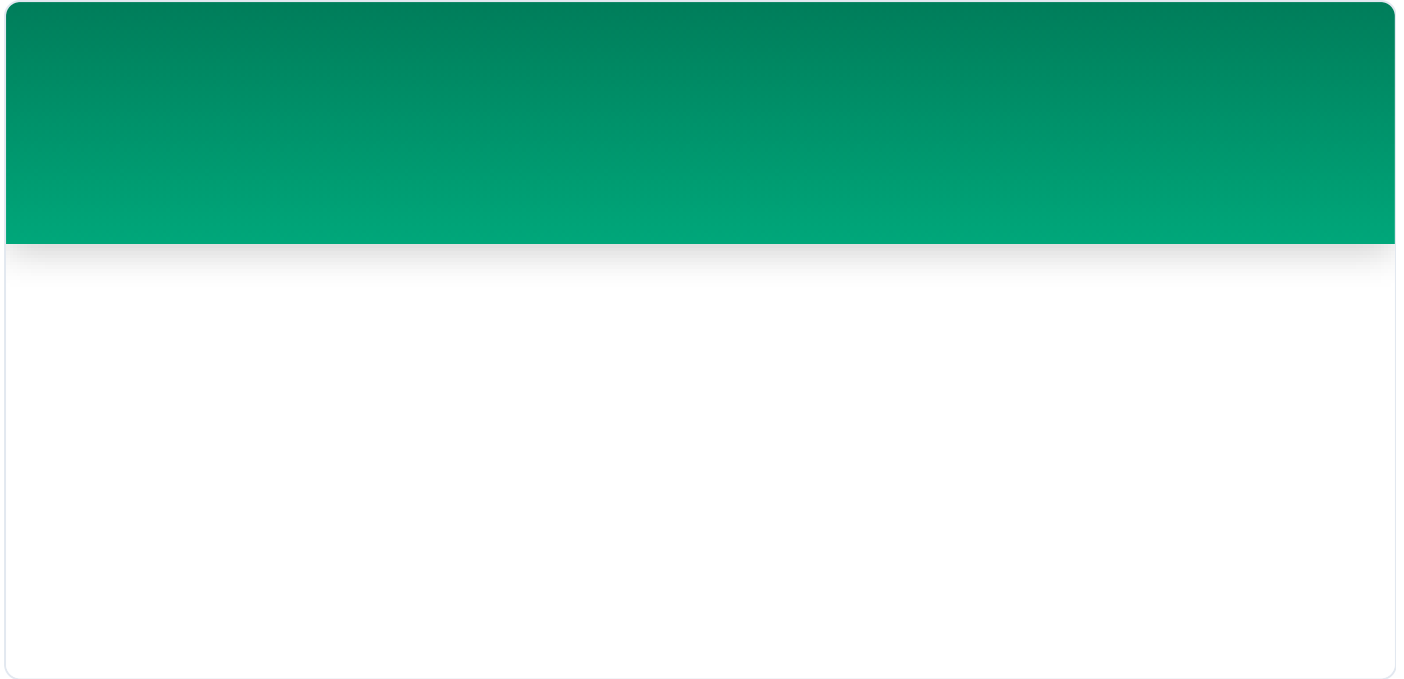
At a glance

The checks that decide most of this verdict.

Malware engines	15 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	7.1 years old Registered history	CLEAR
Web archive	Archived since 2021 Public history exists	CLEAR
Certificate	Encrypted connection Issued by ZeroSSL RSA DV SSL CA 2	NOTED

The page as captured

https://14.128.54.125:8889/



What dd365g.cc served when TrustSniffer captured it on 2026-08-20. 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 2021.
- 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 Chinese-language landing and redirect portal that presents two alternate access routes to 3652aa.com and an online customer-service link. Its apparent function is to direct visitors to another website rather than provide a clearly identified standalone commercial service.

Scam/Impersonation Risk

The site presents a **critical sensitive-interaction risk** because external threat-intelligence assessments recorded malicious detections and a confirmed blacklist status from multiple sources. This is the decisive contradiction in the assessment and outweighs the otherwise limited page-level indicators, which found no login form, payment flow, or explicit brand-impersonation language on the landing page. The portal's very limited content and redirection function also provide little context for establishing who operates it or why the alternate routes should be trusted. No identity contradiction involving two distinct legal-entity names was observed. The published destination reference is 3652aa.com, while the assessed domain is dd365g.cc; that relationship should not be treated as proof of common ownership.

EVIDENCE

- External assessments recorded 15 malicious detections and 1 suspicious detection, with the domain flagged by Kaspersky and Sophos.
- The external reputation record marks the domain as blacklisted and activates a security response based on the malicious detections.
- The homepage is classified as a landing/redirect portal and contains only approximately 95 characters of visible text, with two access links and an online-service link.

Regulatory Verification Notes

The site does not present a clear legal entity, licensing statement, registration number, or regulatory authority on the examined landing page. That is a regulatory-disclosure gap rather than independent proof of fraud, but it prevents meaningful confirmation of the operator, jurisdiction, or accountability framework behind the service being promoted. The site's business purpose is also not sufficiently explained to establish whether it is merely an access portal, an affiliate channel, or part of a regulated activity. The available evidence does not independently verify the real-world operator identity.

EVIDENCE

- The homepage provides no clear company name, license reference, registration number, or regulatory disclosure.
- The domain was registered on 2019-07-01 and is approximately 7.14 years old; the registrar is NameSilo, LLC.
- Hosted on AS396982 (Google Cloud Platform / Google LLC, US).
- TLS certificate issued by ZeroSSL RSA DV SSL CA 2 at DV validation level, valid to 2026-10-03T23:59:59+00:00.

What to Verify Next

Before any sensitive interaction, an enterprise should independently establish the legal operator of both the assessed domain and the referenced destination, confirm whether the underlying service requires authorization in the relevant jurisdiction, and validate that any customer-service channel is published through an independently confirmed official source. Security teams should also check whether endpoint, DNS, and web-proxy controls block the assessed domain and should preserve the observed redirect configuration for incident-response comparison.

EVIDENCE

- The homepage contains no forms or payment fields, so any later request for credentials, wallet authorization, payment, or software installation would represent a material change in interaction risk.
- The site offers alternate "lines" to another domain without explaining the ownership or operational relationship between the two domains.
- The page lacks a title, metadata description, and structured identity information, limiting independent validation of its purpose.

Summary Verdict

The overall posture is **critical and unsuitable for sensitive interaction**. The confirmed external threat detections, blacklist status, minimal identity substance, and unverified operator relationship do not support treating the site as a trusted access channel. Any legitimacy suggested by ordinary hosting or transport controls is insufficient to overcome the security contradiction.

Infrastructure Integrity

The site is protected by Cloudflare CDN/WAF infrastructure, and the observed address is an edge address rather than an independently exposed origin. This provides a mitigating layer against direct infrastructure exposure but does not establish legitimacy and may limit independent verification of the underlying host.

Closing Assessment

The assessed domain should be blocked or isolated from credential, financial, authentication, and software-download workflows pending independent confirmation of the operator and the referenced service through trusted offline or previously established channels.

Written analysis generated 2026-08-20 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
 - 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
 - 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 dd365g.cc.

- The request for dd365g.cc ended on 14.128.54.125, a different domain. WATCH
- Registration is published under NameSilo, LLC. CLEAR
- DNS for this domain is served by cloudflare.com, across 2 name servers. NOTED
- The registration is paid up to 2027-07-01. NOTED
- The earliest public archive of this site is from 2021-12-01. CLEAR
- It is hosted on GOOGLE-CLOUD-PLATFORM, from a server in US. NOTED

Domain intelligence

Registrar	NameSilo, LLC
Hosting	GOOGLE-CLOUD-PLATFORM - Google LLC, US
Country	US
Server IP	34.85.99.0
Name servers	CLAYTON.NS.CLOUDFLARE.COM, FATIMA.NS.CLOUDFLARE.COM
SSL issuer	ZeroSSL RSA DV SSL CA 2
SSL expiry	2026-10-03
Domain age	7.14 years (continuous registration)
Domain expiry	2027-07-01
Archive first seen	2021-12-01
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 15 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about dd365g.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.