

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

cortanaassistant.com

Verdict

0

OUT OF 100

CRITICAL RISK

cortanaassistant.com 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

GPT summary status=skipped | No usable content for GPT summary (clean/dom/html all empty)

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	4.3 years old Registered history	CLEAR
Web archive	Archived since 2024 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YR2	NOTED

The page as captured

No screenshot is retained for this report.

Key findings

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

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

This website is the domain cortanaassistant.com, but the supplied site evidence does not establish a substantiated service, operator, or business model for visitors. Its apparent purpose therefore remains unverified, and the available technical and external-reputation evidence warrants a security-first assessment.

Scam/Impersonation Risk

The domain presents a critical sensitive-interaction risk because external threat intelligence recorded a confirmed blacklist hit and malicious detections associated with the domain. The available evidence does not establish a conflicting legal identity or a confirmed impersonation of a named organization; however, the external detections are sufficiently serious to outweigh otherwise ordinary technical indicators. Behavioral analysis also identified suspicious network activity and a mismatch involving the final destination, while both observed execution runs failed to complete successfully. Login, credential submission, and financial interaction should not be undertaken on this basis.

EVIDENCE

- External reputation checks recorded 12 malicious detections and 1 suspicious detection; a Tier-1 threat detection was attributed to Sophos.
- The domain was confirmed on external blacklists, with blacklist sources recorded as VT and EXTERNAL_BLACKLIST.
- Behavioral analysis recorded 2 runs, with 2 failed runs, 4 external XHR requests, 4 external POST requests, and a maximum external-activity proportion of 64.7%.
- Domain registration evidence records 19 May 2022; the reconciled domain age is 4.26 years.

Regulatory Verification Notes

The available evidence does not independently verify the real-world operator or establish a regulated entity behind the website. Licensing, registration, and responsible-operator disclosures are not confirmed, so any financial, investment, trading, or payment-related representation would require validation through the relevant official registry before engagement. The domain uses a privacy-associated ownership record through Whois Privacy Corp. and is registered through Internet Domain Service BS Corp.; this is an administrative registration

detail, not proof of either legitimacy or misconduct. Historical analysis did not identify a confirmed semantic repurposing conflict, but it does not overcome the external threat findings.

EVIDENCE

- The registrar is Internet Domain Service BS Corp.; the recorded registrant organization is Whois Privacy Corp.
- Historical records span 2024–2026, with 22 archive snapshots across 3 years tracked.
- The site is hosted on AS24940, HETZNER-AS (Hetzner Online GmbH, DE).
- The transport certificate is DV-validated, issued by YR2, and valid until 2026-10-01T06:59:23+00:00.

What to Verify Next

Before any engagement, an independent party should confirm the operator's legal name, address, and beneficial ownership through authoritative corporate records, and confirm any claimed authorization directly with the applicable financial or payments regulator. Contact details and support channels should be validated through an independently sourced route rather than relying solely on the website. Security teams should also compare the domain against current blocklists and inspect any redirected destination in a controlled environment; until those checks are resolved, access should remain limited to non-interactive review.

EVIDENCE

- The operator identity remains independently unverified.
- The on-page disclosure state is unclear, and no authoritative regulatory source is identified.
- The decisive adverse signals are external malicious detections and confirmed blacklist status.
- The available behavioral record shows suspicious network interpretation and failed execution runs.

Summary Verdict

The website has a critical trust posture and should be treated as unsuitable for sensitive interaction. Available evidence is materially inconsistent with safe use for authentication, credential handling, or financial activity, and the operator's legitimacy remains unverified.

Infrastructure Integrity

The site is protected by a CDN/WAF layer, and all observed addresses were CDN edge servers rather than an identifiable origin. This provides some defensive separation and may reduce direct origin exposure, but it is only a mitigating infrastructure characteristic and does not offset the external threat detections.

EVIDENCE

- Four observed edge IP addresses were associated with AS24940; no origin candidate was identified.
- Hosting infrastructure is provided by HETZNER-AS - Hetzner Online GmbH, DE.
- The CDN/WAF posture was assessed as present, with trusted-CDN status recorded.

Closing Assessment

Prospective users and organizations should suspend sensitive interaction until independent identity, regulatory, and destination-integrity checks produce satisfactory results; any necessary investigation should be performed

through isolated, non-authenticated tooling.

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, behaviour in a sandbox, external reputation.

01 Governance Risk

- 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 large share of what the page loaded came from other domains.

Behaviour in a sandbox rule:BEHAV_EXTERNAL_RATIO_MODERATE

- 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	UNKNOWN
Identity score	50/100
Identity verification confidence	15%

- AI page analysis unavailable (page captured; identity not AI-verified)

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 cortanaassistant.com.

- The request stayed on cortanaassistant.com. It was not redirected to another domain. CLEAR
- Registration is published under Internet Domain Service BS Corp.. CLEAR
- DNS for this domain is served by ndsplitter.com, across 2 name servers. NOTED
- The registration is paid up to 2027-05-19. NOTED
- The earliest public archive of this site is from 2024-01-21. CLEAR
- It is hosted on HETZNER-AS, from a server in DE. NOTED

Domain intelligence

Registrar	Internet Domain Service BS Corp.
Hosting	HETZNER-AS - Hetzner Online GmbH, DE
Country	DE
Server IP	159.69.83.207
Name servers	NS1.NDSPLITTER.COM, NS2.NDSPLITTER.COM
SSL issuer	YR2
SSL expiry	2026-10-01
Domain age	4.26 years (continuous registration)
Domain expiry	2027-05-19
Archive first seen	2024-01-21
Archive snapshots	Not counted (archive lookup incomplete)
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 cortanaassistant.com 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/cortanaassistant.com> · assessed 2026-08-22