

Is bachusardar.com a scam? TrustSniffer's high-risk assessment: 5/100

bachusardar.com

Verdict

5

OUT OF 100

CRITICAL RISK

bachusardar.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

A family/genealogy website (Bachusardar.com) hosting memoirs, photo albums, reunion details and memorial content. Contact email and Facebook link present. No financial, login, or transactional features detected.

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.

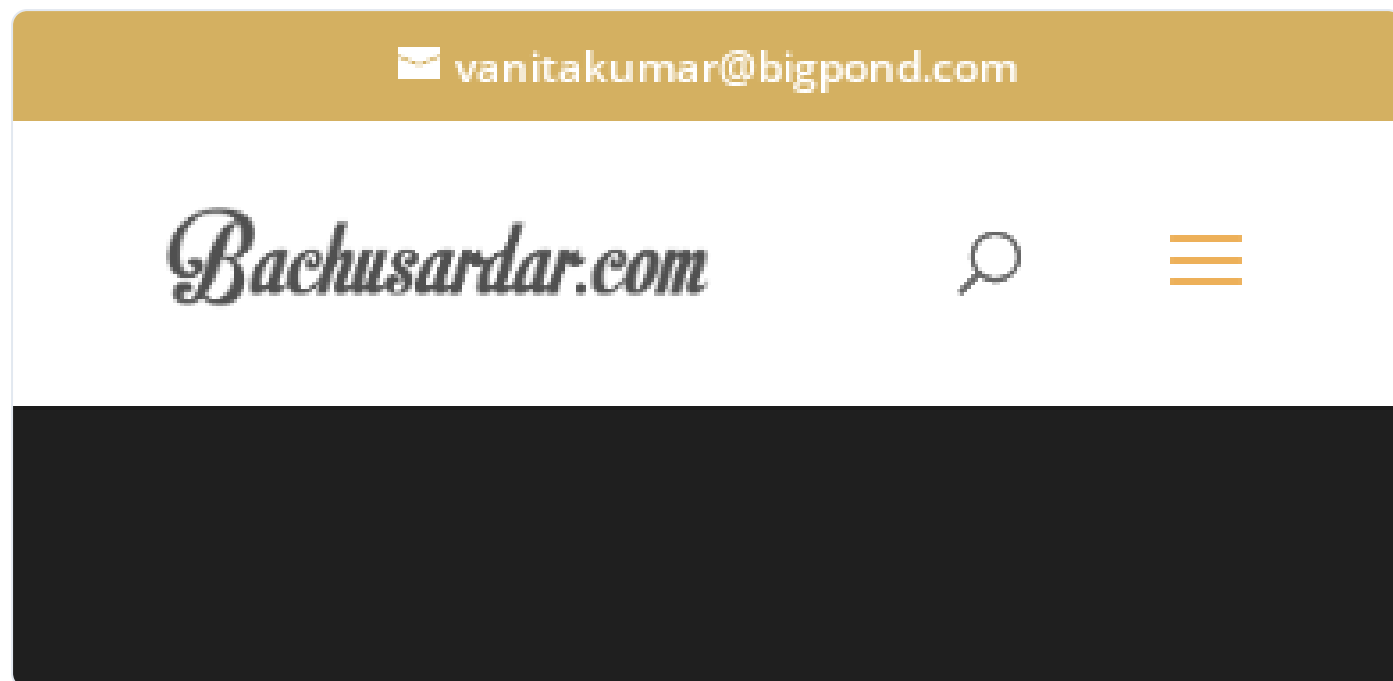
At a glance

The checks that decide most of this verdict.

Malware engines	6 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	19 years old Registered history	CLEAR
Web archive	Archived since 2011 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YR1	NOTED

The page as captured

<https://bachusardar.com/>



What bachusardar.com served when TrustSniffer captured it on 2026-08-22. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: more than 10 years (registration continuity).
- Public web-archive history exists since 2011.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Overview

Bachusardar.com presents itself as a non-commercial family and genealogy archive for the Bachu extended family, containing memoirs, photo albums, memorial material, reunion information from 2008, videos, and a link to Facebook; its apparent purpose is preservation of family history rather than commerce or financial activity.

Scam/Impersonation Risk

The site's visible content is consistent with a personal family archive: it has no login function, payment flow, financial service, cryptocurrency feature, or transactional form, and no page-level brand-impersonation or phishing indicators were identified. However, this benign presentation is outweighed by confirmed external threat detections: the domain is listed by external reputation sources, including six malicious detections in one evaluated source. This is a direct contradiction to the site's otherwise ordinary content and supports a clearly cautionary posture for sensitive interaction. The site's identity is only likely rather than independently verified, so its historical or personal presentation should not be treated as proof of the current operator's identity. No identity contradiction between distinct legal entities was observed.

EVIDENCE

- The homepage and family archive pages describe memoirs, albums, memorials, and the 2008 family reunion, with no financial or transactional functionality observed.
- The homepage's form analysis identified one search form and no login form, hidden sensitive form, or external password submission.
- External reputation assessment recorded 6 malicious detections and a confirmed external blacklist hit; Google Safe Browsing was not malicious.
- Domain registration telemetry: created 2007-05-07 and currently approximately 19.3 years old; archival records span 2011-02-01 to 2026-04-22 across 16 tracked years, with incomplete archival coverage.

Regulatory Verification Notes

The website appears personal and non-commercial, so no financial-service licensing claim would ordinarily be expected from the visible content. Nevertheless, the available material does not establish the legal identity of the current operator or provide an independently verified regulatory basis for any sensitive engagement. The domain registration uses Key-Systems GmbH and registrant details are privacy-protected; this is an administrative limitation rather than evidence of an identity contradiction. The low page-authority signal and missing structured metadata provide additional context about the site's limited formal web presence, but do not independently determine legitimacy. The external reputation warning remains a reputational signal with material security significance, not a regulatory finding.

EVIDENCE

- The homepage identifies the site as created to preserve the Bachu family history and commemorate a family reunion, without presenting a company, financial service, or license claim.
- Registration telemetry: registrar Key-Systems GmbH; creation date 2007-05-07; expiration date 2027-05-07; registrant and organization fields are REDACTED FOR PRIVACY.
- Hosting telemetry: served from AS63956, INT-5GN-AS-AP – 5G NETWORK OPERATIONS PTY LTD, Australia.
- Transport telemetry: TLS certificate issued by YR1 using domain validation (DV), valid through 2026-10-23.

What to Verify Next

Before any credential, payment, download, or other sensitive interaction is permitted, the domain's current reputation status should be checked through the organization's approved security controls and the site should be reached only through a known-good, independently confirmed channel. The current operator should be corroborated through an offline or independently sourced family contact rather than relying solely on the website or its social link. Any unexpected redirection, request for account details, software installation, or change from archival content to commercial activity should be treated as a material change requiring renewed assessment.

EVIDENCE

- The visible site contains no sensitive form, wallet connection, password submission, or transaction flow, so any such later request would represent a significant change in observed behavior.
- The site links externally to Facebook and otherwise exposes a small, primarily internal page set consisting of the homepage, albums, memoirs, reunion information, and videos.
- Behavioral testing recorded two successful runs, no external XHR or external POST activity, no clipboard writes, no wallet-provider detection, and no hidden forms.
- Behavioral testing also recorded 2 suspicious inline scripts and a maximum post-interaction DOM difference of 1,198, which should be considered when validating any future interactive behavior.

Summary Verdict

The overall posture is **critical trust with sensitive-interaction risk**. Although the site's visible purpose and content are non-commercial and personally themed, the confirmed external reputation contradiction prevents the domain from being treated as trustworthy for credentials, financial activity, or other sensitive actions. The real-world operator identity remains likely but not independently verified.

Infrastructure Integrity

The domain resolves directly to a single identified origin in Australia rather than through a detected CDN or WAF. Hosting is provided by INT-5GN-AS-AP – 5G NETWORK OPERATIONS PTY LTD on AS63956; the site uses a valid DV TLS certificate issued by YR1, which protects transport confidentiality but does not establish the operator's legitimacy or offset the external reputation warning.

Closing Assessment

The appropriate enterprise disposition is to restrict the domain from sensitive use and permit only controlled, non-interactive viewing if operationally necessary, subject to monitoring for changes in content, behavior, or reputation.

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

- 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
- The page carried inline scripts written in a style TrustSniffer treats as suspicious.
Behaviour in a sandbox rule:BEHAV_SUSPICIOUS_INLINE_SCRIPTS
- The structure of the page changed sharply while it was loading.
Behaviour in a sandbox rule:BEHAV_DOM_DENSITY_SPIKE
- 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	LIKELY
Identity score	73/100
Identity verification confidence	37%

- Trusted social count=1

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 bachusardar.com.

- The request stayed on bachusardar.com. It was not redirected to another domain. CLEAR
- Registration is published under Key-Systems GmbH. CLEAR
- DNS for this domain is served by digitalhost.com, across 3 name servers. NOTED
- The registration is paid up to 2027-05-07. NOTED
- The earliest public archive of this site is from 2011-02-01. CLEAR
- It is hosted on INT-5GN-AS-AP, from a server in AU. NOTED

Domain intelligence

Registrar	Key-Systems GmbH
Hosting	INT-5GN-AS-AP - 5G NETWORK OPERATIONS PTY LTD, AU
Country	AU
Server IP	103.127.41.4
Name servers	DNS1.DIGITALHOST.COM, DNS2.DIGITALHOST.COM, DNS3.DIGITALHOST.COM
SSL issuer	YR1
SSL expiry	2026-10-23

Domain age	19.30 years (continuous registration)
Domain expiry	2027-05-07
Archive first seen	2011-02-01
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 6 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about bachusardar.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/bachusardar.com> · assessed 2026-08-22