

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

bigbauer.com

Verdict

0

OUT OF 100

CRITICAL RISK

bigbauer.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 2026-08-21 by automated analysis. Classification confidence 50%.

What this site appears to be

A German-language login page labeled GMX.NET that asks for GMX email address and password with links to register, password reset, imprint, terms, and privacy. The page is primarily a credential entry screen without additional service description.

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	None flagged it VirusTotal	CLEAR
Google Safe Browsing	Listed as unsafe Google	RISK
Abuse reports on the host	0 reports AbuseIPDB; shared hosting inflates this count	NOTED
Domain age	26 years old Registered history	CLEAR
Web archive	Archived since 2001 Public history exists	CLEAR
Certificate	Encrypted connection Issued by Sectigo Public Server Authentication CA DV R36	NOTED

The page as captured

<https://bigbauer.com/>

Login

Bitte melden Sie sich hier mit Ihrer GMX E-Mail-Adresse und Ihrem Passwort an.

GMX E-Mail-Adresse

What bigbauer.com served when TrustSniffer captured it on 2026-08-21. 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 2001.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Overview

The website at bigbauer.com presents a German-language page branded “GMX.NET” that functions primarily as an email-service login screen, requesting a GMX email address and password while offering registration, password-reset, imprint, terms, and privacy links. Its apparent purpose is to obtain user authentication credentials, but the captured page provides no surrounding service, corporate, or operational context.

Scam/Impersonation Risk

The site presents a high-risk sensitive-interaction profile. The homepage is login-only, contains a single credential form, and supplies minimal context beyond the GMX.NET label; this combination creates a substantial evidence gap for a page requesting authentication. Independent external detections include a Google Safe Browsing malicious result and a confirmed blacklist record from another external source. These are direct contradiction signals, although the supplied page analysis does not independently classify the page as brand impersonation or phishing. No additional contradiction involving multiple legal-entity names was observed.

EVIDENCE

- The homepage contains a German-language login form requesting a GMX email address and password, with no substantive service description.
- External reputation telemetry records `gsb\_malicious: true` and `external\_blacklist: true`; the associated threat type is recorded as social engineering.
- Domain registration telemetry records creation on 2000-10-19, with an age of 25.85 years.
- Archive telemetry records 24 snapshots spanning 2001–2026, covering 26 tracked years.

Regulatory Verification Notes

The page exposes links labelled Impressum, AGB, and Datenschutz, but the supplied capture does not establish an independently verified operator, regulated affiliation, or licensing basis. No license claim or license number is present in the available page content, so the legal and regulatory position remains unresolved rather than validated. The absence of a broker-dataset match provides limited contextual information only and is not a licensing determination. The domain uses a long-standing registration through IONOS SE, but that infrastructure fact does not overcome the page-level and external-reputation contradictions.

EVIDENCE

- The homepage links to an imprint, terms, and privacy information, but the captured content does not provide verified operator or licensing details.
- Hosting telemetry identifies AS8560, IONOS-AS - IONOS SE, DE.
- The transport certificate is issued by Sectigo Public Server Authentication CA DV R36, uses domain validation, and is valid through 2026-11-10.
- The supplied broker-reputation dataset reports no match.

What to Verify Next

Credential submission should be withheld unless the service is reached through an independently known official GMX channel, such as a trusted bookmark or separately verified corporate route. Any purported operator or affiliation should be checked against authoritative corporate and regulatory records, and the imprint and terms should be reviewed for a consistent legal entity and enforceable contact details. If access is necessary for an existing account, password-reset and account-recovery activity should be initiated only through the independently verified official service.

EVIDENCE

- The homepage title is “Login - GMX.NET” and identifies the page as a login-only / unknown service.
- The page contains one sensitive login form and offers no external links or broader service context.
- The captured page includes only a short body of 274 characters focused on login, registration, password recovery, imprint, terms, and privacy.

Summary Verdict

The website has a **critical sensitive-interaction risk posture**. The convergence of a credential-focused page with minimal context and confirmed external blacklist detections makes the site unsuitable for normal

authentication or other sensitive engagement. The real-world operator identity also remains unverified.

Infrastructure Integrity

A CDN/WAF layer is present, and the observed addresses are associated with AS8560 and IONOS-AS - IONOS SE in Germany; no origin candidate was observable in the supplied infrastructure analysis. This edge protection may reduce direct exposure of the underlying host, but it is only a mitigating technical characteristic and provides no assurance that the website or its operator is legitimate.

Closing Assessment

Enterprise controls should block or isolate this domain for credential-related activity, and any required account access should be redirected to an independently verified official service through established recovery procedures.

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, 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
 - 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
 - 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 bigbauer.com.

- The request stayed on bigbauer.com. It was not redirected to another domain. CLEAR
- Registration is published under IONOS SE. CLEAR
- DNS for this domain is served by ui-dns.de, across 4 name servers. NOTED
- The registration is paid up to 2026-10-19. NOTED
- The earliest public archive of this site is from 2001-07-20. CLEAR
- It is hosted on IONOS-AS, from a server in DE. NOTED

Domain intelligence

Registrar	IONOS SE
Hosting	IONOS-AS - IONOS SE, DE
Country	DE
Server IP	2001:8d8:100f:f000::253
Name servers	NS1034.UI-DNS.DE, NS1059.UI-DNS.ORG, NS1066.UI-DNS.COM, NS1123.UI-DNS.BIZ
SSL issuer	Sectigo Public Server Authentication CA DV R36
SSL expiry	2026-11-10
Domain age	25.85 years (continuous registration)
Domain expiry	2026-10-19
Archive first seen	2001-07-20
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 0 flagged AbuseIPDB: 0 reports Google Safe Browsing: 1 match

About this assessment

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