

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

mekblue.com

Verdict

0

OUT OF 100

CRITICAL RISK

mekblue.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

MEKBLUE corporate site for a chemical/industrial liquids manufacturer (AdBlue®, antifreeze, windshield washer fluid, demineralized water). Provides product categories, quality documents, contact details, address and phone numbers. Contains a contact form for inquiries and order requests.

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.

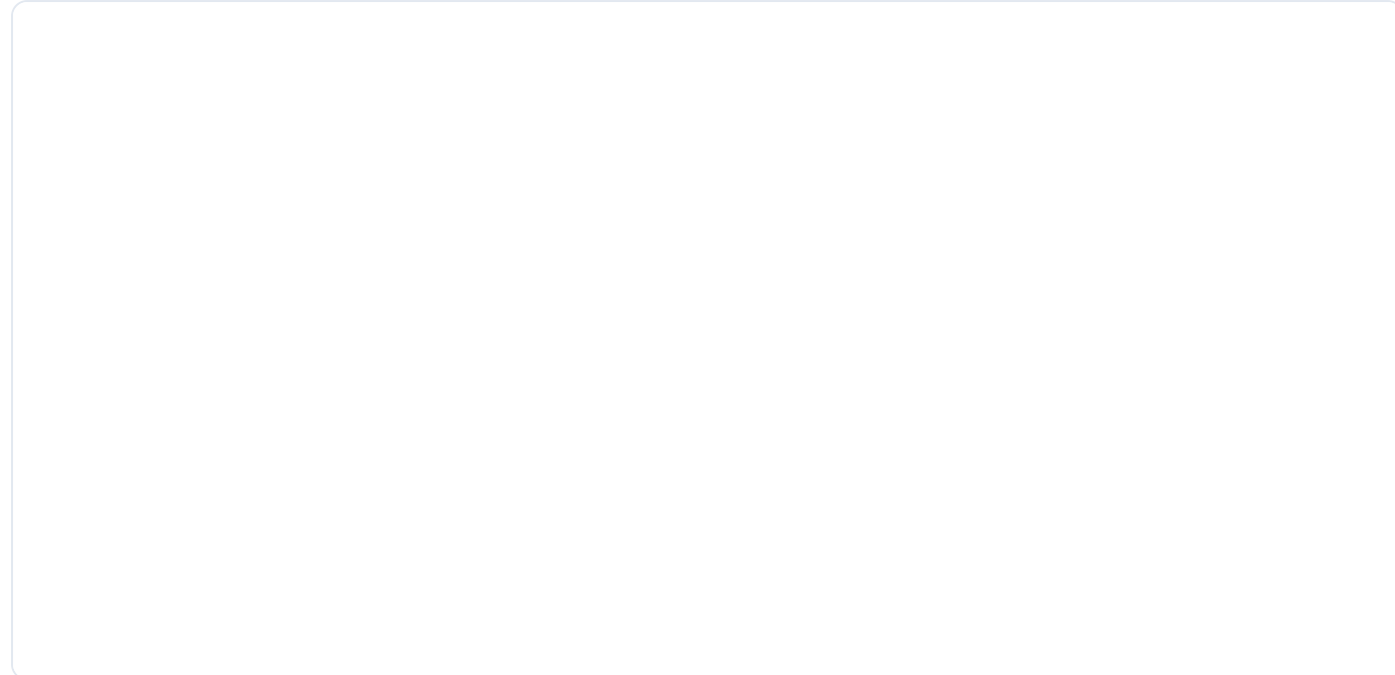
At a glance

The checks that decide most of this verdict.

Malware engines	7 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	10 years old Registered history	CLEAR
Web archive	Archived since 2017 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YR1	NOTED

The page as captured

<https://www.mekblue.com/>



What mekblue.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 2017.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

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

MEKBLUE is a Turkish corporate website presenting itself as a manufacturer and seller of industrial liquids, including AdBlue®, antifreeze, windshield washer fluid, demineralized water, chemicals, and related equipment. It presents product information, catalogs, laboratory and quality documentation, corporate material, and contact channels intended to support business inquiries and product orders.

Scam/Impersonation Risk

The site's ordinary manufacturing presentation and absence of visible credential-harvesting or brand-impersonation content do not reconcile the stronger external warning signals. The domain is reported as **blacklisted** by two sources, with seven malicious detections, including detections associated with Sophos and Fortinet. Behavioral analysis also recorded hidden forms in both observed runs and a substantial DOM change after interaction, although no password form, wallet connection, external form destination, or external network submission was identified. The available evidence therefore supports a clearly cautionary posture for sensitive interaction; it does not establish a conflicting legal identity or prove that the site is impersonating a named brand.

EVIDENCE

- External reputation records show blacklist status and 7 malicious detections; Sophos and Fortinet were among the flagged vendors.
- The behavioral sensor recorded 2 hidden forms across 2 runs and a maximum post-interaction DOM difference of 2398.
- Domain registration records show creation on 2016-07-29 and an age of 10.07 years.
- Archive telemetry records 64 snapshots spanning 2017-02-07 through 2026-05-15, with 10 years tracked.

Regulatory Verification Notes

The corporate and contact pages identify MEKBLUE as operating under Mekser Mühendislik and provide an industrial address, telephone numbers, product catalogs, laboratory material, test reports, and quality-document sections. These disclosures make the business model specific and commercially coherent, but the available material does not provide a verified license or registration number for the relevant manufacturing or chemical activities. That is a regulatory verification gap rather than, by itself, proof of fraud. Independent identity linkage remains only likely rather than verified, and the external blacklist signal materially outweighs the site's otherwise substantial corporate content. The domain is registered through Isimtescil Bilisim A.S.; its transport security is provided by a currently valid DV certificate, which confirms encryption but not legal authorization.

EVIDENCE

- The corporate pages state that MEKBLUE operates under Mekser Mühendislik and provide product, laboratory, quality, and occupational-safety documentation sections.
- WHOIS records identify Isimtescil Bilisim A.S. as registrar, with registration from 2016-07-29 to 2027-07-29.
- Hosting telemetry identifies AS42846, guzelhosting – GNET Internet Telekomunikasyon A.S., Türkiye.
- The site's TLS certificate is issued by YR1 at DV validation level and is valid until 2026-09-23.

What to Verify Next

Before any commercial engagement, an independent corporate-registry check should confirm the legal entity named on the corporate pages and its authority to contract and sell the stated products. Applicable chemical, manufacturing, environmental, and quality certifications should be validated directly with the issuing bodies rather than relying solely on documents hosted by the site. Any order, payment instruction, or change to contact details should be confirmed through an independently sourced business channel, and the contact form should not be used to submit credentials, identity documents, payment data, or other sensitive information. Security teams should also preserve the external detections and behavioral indicators for internal blocking and incident-triage decisions.

EVIDENCE

- The corporate and contact pages provide the stated legal-business relationship, premises details, and telephone channels for independent confirmation.
- Product and document sections provide the specific certification and laboratory materials requiring issuer-side validation.
- The site exposes one contact form for inquiries and order requests; behavioral testing recorded hidden forms during both observed runs.

Summary Verdict

The overall posture is **critical trust risk** because authoritative external threat detections and blacklist signals create a material contradiction that the site's coherent corporate content and established registration history cannot resolve. The site may represent a real industrial business, but the available evidence does not support treating it as suitable for sensitive interaction or financial reliance.

Infrastructure Integrity

The site resolves directly to two likely origin addresses, with no detected CDN or WAF layer and no edge-IP posture identified. Direct hosting through guzelhosting – GNET Internet Telekomunikasyon A.S. provides a concrete technical location but does not offer the protective buffering or legitimacy assurance associated with independently verified defensive infrastructure.

Closing Assessment

The appropriate enterprise posture is to restrict the site to controlled, non-sensitive review while withholding credentials, confidential information, and payment activity unless the independent identity, regulatory, and reputation checks above produce satisfactory results.

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

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 rewrote itself after it was interacted with, so what a visitor first sees is not what they end up on.

Behaviour in a sandbox rule:BEHAV_DOM_DIFF_AFTER_INTERACTION

- The page contained a form a visitor cannot see.

Behaviour in a sandbox rule:BEHAV_HIDDEN_FORMS

- 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	79/100
Identity verification confidence	39%

- Trusted social count=3

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 mekblue.com.

- The request stayed on mekblue.com. It was not redirected to another domain. [CLEAR](#)
- Registration is published under Isimtescil Bilisim A.S. [CLEAR](#)
- DNS for this domain is served by guzelhosting.com, across 2 name servers. [NOTED](#)
- The registration is paid up to 2027-07-29. [NOTED](#)
- The earliest public archive of this site is from 2017-02-07. [CLEAR](#)
- It is hosted on guzelhosting, from a server in TR. [NOTED](#)

Domain intelligence

Registrar	Isimtescil Bilisim A.S
Hosting	guzelhosting - GNET Internet Telekomunikasyon A.S., TR
Country	TR
Server IP	2a06:41c0:1:e::89
Name servers	NS1.GUZELHOSTING.COM, NS2.GUZELHOSTING.COM

SSL issuer	YR1
SSL expiry	2026-09-23
Domain age	10.07 years (continuous registration)
Domain expiry	2027-07-29
Archive first seen	2017-02-07
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 7 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

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