

Is plasmatech.ir safe? TrustSniffer's low-trust assessment: 40/100

plasmatech.ir

Verdict

40

OUT OF 100

LOW TRUST

plasmatech.ir is low-trust and potentially risky.

Several risk patterns were present. Do not send money or personal details until you have verified this business another way.

Sensitive Interaction Risk

Governance Risk

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

What this site appears to be

Persian-language corporate site for Plasmatech, an engineering company providing surface treatment services. Contact email and phone shown. Standard service listings and resources. Page contains an unusual 'verification' block instructing the user to perform keyboard actions, which appears deceptive.

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.

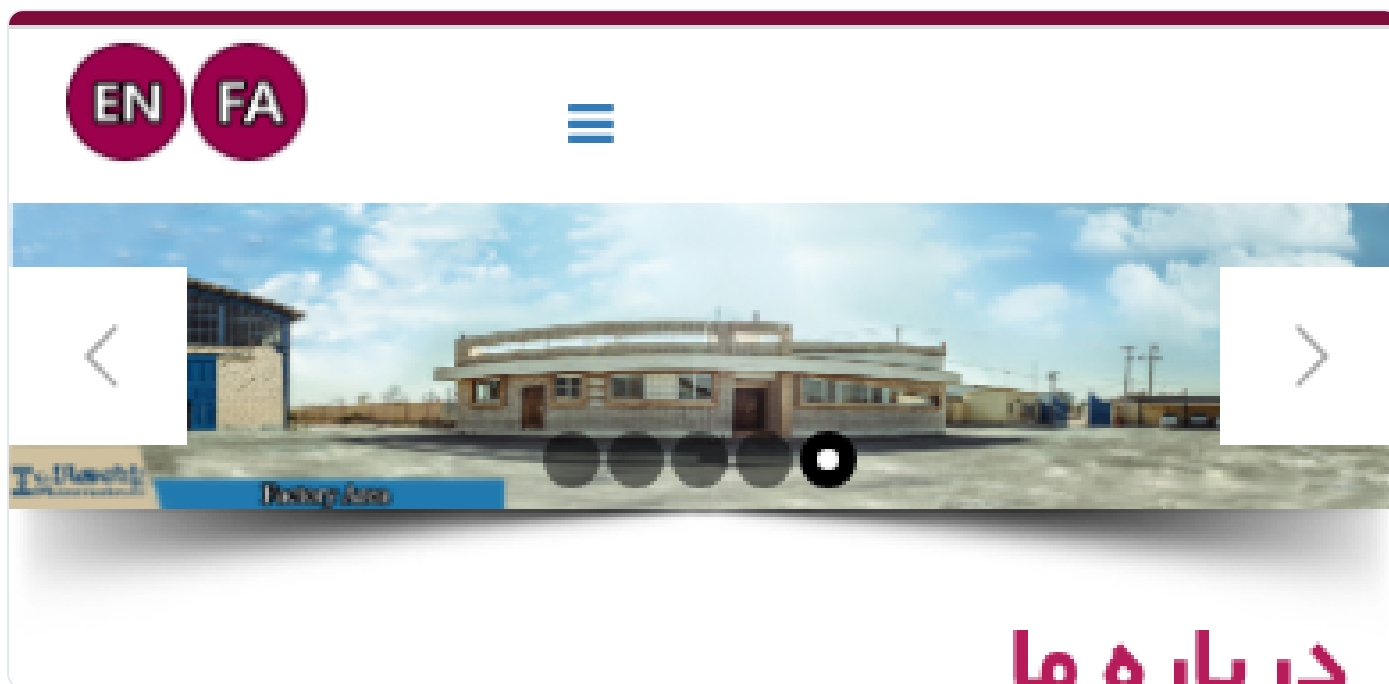
At a glance

The checks that decide most of this verdict.

Malware engines	3 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	21 years old Registered history	CLEAR
Web archive	Archived since 2005 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YR2	NOTED

The page as captured

<https://plasmatech.ir/fa/>



What plasmatech.ir served when TrustSniffer captured it on 2026-08-20. 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 2005.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Overview

Plasmatech is a Persian-language corporate business-to-business website presenting an engineering company that provides surface-treatment services, including plasma nitriding, thermal spraying, physical vapour deposition, cladding, and lapping, for industrial sectors such as oil and gas, steel, textiles, and wood and paper.

Scam/Impersonation Risk

The site has a **high-risk interaction posture** because external reputation checks recorded a confirmed blacklist hit, including multiple malicious detections. The homepage also contains deceptive “verification” instructions directing visitors to press the Windows key and run a pasted command sequence, which is inconsistent with a normal CAPTCHA and creates a material risk of social-engineering or malicious execution. No separate identity contradiction or brand-impersonation finding was observed, but the blacklist result and deceptive browser instructions are sufficient to make sensitive interaction inappropriate.

EVIDENCE

- The homepage contains a “Complete these Verification Steps” block instructing visitors to press Windows+R, paste content, and press Enter.
- External reputation checks recorded a blacklist hit, with 3 malicious and 1 suspicious detections.
- Authoritative domain continuity is 20.802190280629706 years; archival records span 2005-10-30 to 2025-06-13, covering 21 years.

Regulatory Verification Notes

The available pages present Plasmatech as an engineering-services company, but the site’s legal and governance disclosures are unclear and the real-world operator identity remains unverified. No licence, registration number, or regulatory authority is claimed in the supplied business content. This is a disclosure gap requiring independent confirmation rather than a standalone determination of fraud. The site’s ordinary B2B service presentation is not sufficient to offset the separate reputation and interaction concerns identified above.

EVIDENCE

- The homepage and about section identify the business as Plasmatech and describe engineering and industrial-service activities.
- The supplied business content contains no claimed licence authority or licence number.
- Domain registration is recorded through IRNIC.

What to Verify Next

Before any commercial engagement, an independent business registry or relevant industry authority should be used to confirm the legal entity, operating address, and responsible representatives. Any quotation, purchase order, or payment instruction should be validated through independently sourced contact channels and against documented contractual terms. The unusual browser-verification mechanism should not be followed; the official site should be accessed only through a clean browser session, with endpoint monitoring applied where organizational policy requires it.

EVIDENCE

- The about and contact pages provide the stated company identity and contact routes for independent cross-checking.
- The site includes catalogues, cooperation forms, customer-satisfaction forms, and service information that can be compared with independently obtained commercial documentation.
- The deceptive verification block is visible on the homepage and should be treated as a browser-interaction control rather than a legitimate identity check.

Summary Verdict

The available evidence supports a low-trust classification with elevated risk for sensitive interaction. The site may represent a genuine engineering-services business, but legitimacy and operator identity are not independently established, while confirmed external reputation concerns and deceptive on-page behaviour materially weaken confidence.

Infrastructure Integrity

The website is protected by CDN/WAF infrastructure, which provides a mitigating layer against direct exposure but does not establish legitimacy or remove the reputation concerns. The observed infrastructure resolves through OVH SAS in France, with the origin not observable in this analysis.

EVIDENCE

- Served from AS16276 (OVH - OVH SAS, FR), observed edge IP 5.39.23.50.
- TLS certificate issuer: YR2; validation level: DV; valid to 2026-10-07T04:26:33+00:00.
- CDN/WAF protection is present, with 1 observed edge IP and 0 observed origin candidates.

Closing Assessment

The appropriate institutional posture is to limit activity to passive review until the operator, business credentials, and transaction channels have been independently validated; login, credential submission, and financial interaction should not proceed on the basis of the website alone.

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, behaviour in a sandbox.

01 Governance Risk

- The public registration record for this domain is incomplete.
Registration and ownership rule:KF_WHOIS_INCOMPLETE

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 exchanged network traffic with destinations TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_TRAFFIC
- The page sent data to a destination TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_POSTS
- The page made background requests to destinations TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_XHR

Identity verification

Status	UNVERIFIED
Identity score	30/100
Identity verification confidence	50%

- 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 plasmatech.ir.

- The request stayed on plasmatech.ir. It was not redirected to another domain. CLEAR
- Registration is published under IRNIC. CLEAR
- DNS for this domain is served by irandns.com, across 2 name servers. NOTED
- The earliest public archive of this site is from 2005-10-30. CLEAR
- It is hosted on OVH, from a server in FR. NOTED

Domain intelligence

Registrar	IRNIC
Hosting	OVH - OVH SAS, FR
Country	FR
Server IP	5.39.23.50
Name servers	cp11.irandns.com, cp12.irandns.com
SSL issuer	YR2
SSL expiry	2026-10-07
Domain age	20.80 years (continuous registration)
Domain expiry	Not available
Archive first seen	2005-10-30
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 3 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about plasmatech.ir 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.