

Is gemini-project.eu a scam? TrustSniffer's high-risk assessment: 5/100

gemini-project.eu

Verdict

5

OUT OF 100

CRITICAL RISK

gemini-project.eu 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 2026-08-20 by automated analysis. Classification confidence 50%.

What this site appears to be

The Gemini Project site describes an Erasmus+ co-funded initiative to support young women in social entrepreneurship and digital innovation, listing aims, activities, events, partners and resources. No payment flows, investment products, or login/credential collection are present.

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.

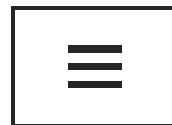
At a glance

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	2.5 years old Registered history	CLEAR
Web archive	Archived since 2021 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YR1	NOTED

The page as captured

<https://gemini-project.eu/>



Home

What gemini-project.eu served when TrustSniffer captured it on 2026-08-20. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: 1 to 3 years (registration continuity).
- Public web-archive history exists since 2021.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Overview

The Gemini Project website presents an informational Erasmus+ initiative focused on supporting young women in social entrepreneurship and digital innovation, with pages describing its aims, activities, deliverables, partners, events, gallery, and contact arrangements rather than selling products or soliciting investment.

Scam/Impersonation Risk

The site's visible content is educational and non-commercial: the homepage describes an online business accelerator simulator, project activities, partners, and resources, with no visible payment flow, investment offering, login form, or credential request. However, this benign presentation is outweighed by confirmed blacklist detections, including a Google Safe Browsing malicious match associated with social-engineering activity and a separate external blacklist detection. Runtime analysis also observed hidden forms during both test runs, despite no visible sensitive form on the captured pages. These signals create a material risk that the current presentation may not fully represent the site's operational risk or that content could change. No identity inconsistency or brand impersonation was established, but the blacklist status is a direct contradiction to the site's apparently legitimate educational presentation.

EVIDENCE

- Google Safe Browsing marked the domain as malicious, with the recorded threat type being social engineering.
- A separate external blacklist also identified the domain; the associated protective response was activated.
- Behavioral testing observed hidden forms in 2 of 2 runs, while the homepage displayed no visible login or payment form.
- The registration-continuity record gives a domain age of 2.46 years; historical records run from 2021-12-05 to 2026-02-16 across 6 years tracked.

Regulatory Verification Notes

The site describes an Erasmus+ educational project and presents partner, activity, deliverable, news, gallery, and contact pages. Those materials provide substantive project information, but the available pages do not establish an independently verified legal operator or a verified regulatory affiliation; no license or registration number is claimed. For this type of educational initiative, the absence of a financial-services license is not itself evidence of fraud, but the unclear governance and ownership disclosures materially limit confidence in who is responsible for the site. The available broker-reputation dataset produced no match, which is only a neutral contextual signal and does not resolve the identity question.

EVIDENCE

- The homepage states that the project has “10 PARTNERS across EUROPE” and describes its objectives for women’s social entrepreneurship and digital innovation.
- The aims, activities, deliverables, partners, news, and gallery pages are presented as project information rather than regulated financial-service disclosures.
- The domain is registered through Papaki.com.
- The site uses a valid DV TLS certificate issued by YR1, valid to 2026-10-28.

What to Verify Next

Before any sensitive interaction, an institution should independently confirm the project’s Erasmus+ status and the listed partner relationships through official institutional or programme records, rather than relying solely on the site’s own claims. The responsible organisation should also be confirmed through an independently obtained contact route, and any request to provide credentials, upload documents, install software, or make a payment should be treated as requiring separate validation.

EVIDENCE

- The homepage provides the project name, stated Erasmus+ context, and partner-count claim for comparison against independent programme or institutional records.
- The partners and deliverables pages provide the project-specific references that should be matched to independently sourced partner information.
- The contact page supplies the site’s stated communication route, which should be cross-checked through an offline or independently published channel.

Summary Verdict

The website has a **critical trust posture** for sensitive interaction. Its coherent informational content does not overcome the confirmed blacklist detections and runtime indicators, while the real-world operator remains unverified. Passive viewing is materially less exposed than credential, account, document, or financial interaction.

Infrastructure Integrity

The site is served through a CDN/WAF layer, which limits direct origin exposure and provides a mitigating layer against some infrastructure-level abuse; that protection does not establish legitimacy and cannot offset the external reputation findings. The observed infrastructure is associated with OVH - OVH SAS in France.

EVIDENCE

- Served from AS16276 (OVH - OVH SAS, FR), with observed edge IP 5.39.70.116.
- CDN/WAF protection was detected; no likely origin candidate was observed.
- TLS validation is DV; certificate issuer is YR1 and validity ends 2026-10-28.

Closing Assessment

Interaction should remain limited to passive review unless the project identity, partner relationships, and any requested action are independently confirmed through trusted channels. Credentials, sensitive documents, software installation, and financial activity should not be undertaken on the basis of the site 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, external reputation.

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 contained a form a visitor cannot see.
Behaviour in a sandbox rule:BEHAV_HIDDEN_FORMS
- 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	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 gemini-project.eu.

- The request stayed on gemini-project.eu. It was not redirected to another domain. CLEAR
- Registration is published under Papaki.com. CLEAR
- DNS for this domain is served by eu for more info.. NOTED
- The earliest public archive of this site is from 2021-12-05. CLEAR
- It is hosted on OVH, from a server in FR. NOTED

Domain intelligence

Registrar	Papaki.com
Hosting	OVH - OVH SAS, FR
Country	FR
Server IP	5.39.70.116
Name servers	ns2.oneup.host ns1.oneup.host Please visit www.eurid.eu for more info.
SSL issuer	YR1
SSL expiry	2026-10-28
Domain age	2.46 years (continuous registration)
Domain expiry	Not available
Archive first seen	2021-12-05
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 gemini-project.eu 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/gemini-project.eu> · assessed 2026-08-20