

Is eurobank.gr legit? TrustSniffer's high-trust assessment: 100/100

eurobank.gr

Verdict

100

OUT OF 100

HIGH TRUST

eurobank.gr appears legitimate.

Our checks found nothing pointing to fraud. Ordinary care still applies when you pay or sign in.

Not Scam

Low Risk

Assessed 2026-08-10 by automated analysis. Classification confidence 70%.

What this site appears to be

Official-looking Greek-language Eurobank retail banking landing page describing accounts, cards, loans, mobile app, security guidance and contact channels. Content includes marketing offers, product links and consumer guidance.

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	Not listed Google	CLEAR
Abuse reports on the host	0 reports AbuseIPDB; shared hosting inflates this count	NOTED
Domain age	28 years old Registered history	CLEAR
Web archive	Archived since 1999 49 snapshots	CLEAR
Certificate	Encrypted connection Issued by DigiCert Global G3 TLS ECC SHA384 2020 CA1	NOTED

The page as captured

No screenshot is retained for this report.

Key findings

- Automated classification: Not Scam.
- Domain age: more than 10 years (registration continuity).
- Public web-archive history exists since 1999.
- No flags from the reputation services TrustSniffer consulted at assessment time.

Full analysis

Overview

The website is an official-looking Greek-language retail and corporate banking portal for Eurobank, presenting deposit accounts, cards, loans, insurance, digital banking, mobile-app onboarding, customer support, and business-banking services through an established institutional model.

Scam/Impersonation Risk

No contradictions were observed: the supplied evidence identifies no phishing, impersonation, malicious, suspicious, or blacklist findings. The homepage presents coherent banking content, security guidance, contact channels, and links for personal, business, private-banking, and group information; observed behavior also showed no login form, hidden form, external sensitive-form submission, cloaking, wallet activity, or suspicious script activity. The available historical record is consistent with domain continuity rather than suspicious repurposing, although the real-world operator identity remains independently unverified.

EVIDENCE

- The retail banking page contains no reported red flags and is classified as a corporate/retail banking marketing page with a low page-risk assessment.
- External reputation checks recorded 0 malicious and 0 suspicious detections, with no confirmed blacklist or phishing finding.
- Domain registration continuity: 27.564681724845997 years.
- Web-archive coverage: 49 snapshots spanning 1999–2016, with 18 years tracked.

Regulatory Verification Notes

The site presents an institutional banking identity and substantive consumer-facing information, including product categories, security guidance, appointment and support channels, and an “About the Group” area. Those on-site materials are consistent with an established financial-services website but do not independently prove the real-world operator's identity. Licensing and registration disclosure is unclear in the supplied page evidence; this is a verification gap rather than evidence of wrongdoing. No separate third-party broker match was identified, and no third-party reputational warning was supplied.

EVIDENCE

- The homepage identifies Eurobank and provides personal, business, private-banking, group, contact, ATM, appointment, and digital-banking sections.
- The site's transport encryption uses a DigiCert Global G3 TLS ECC SHA384 2020 CA1 certificate with EV validation, issued to Eurobank S.A. and valid through 2026-10-16T23:59:59+00:00.
- The homepage contains consumer security guidance and contact information, but the supplied content does not show a licensing authority or license number.

What to Verify Next

Before credential or payment interactions, an institution should independently confirm the bank's legal identity and applicable authorization through the relevant official financial-services register. Contact channels should be confirmed through an independently obtained route, and account-opening or transaction activity should be conducted only through the institution's verified official application or service channel. Applicable account terms, complaint procedures, and payment-protection arrangements should also be reviewed.

EVIDENCE

- The homepage provides telephone, appointment, ATM, branch, and security-guidance pathways that can be cross-checked through an independent source.
- The captured page showed no sensitive form and no untrusted form destination, so verification remains focused on the destination and service channel used for any later interaction.

Summary Verdict

Available evidence supports a **high-trust, low-risk posture** and is consistent with an established, apparently legitimate website. The classification is strong, while the connection between the website and a verified real-world operator should remain qualified rather than treated as proven.

Infrastructure Integrity

The website is protected by Akamai CDN/WAF infrastructure, with the observed address serving as a CDN edge rather than an identified origin. The hosting telemetry records AS20940, AKAMAI-ASN1—Akamai International B.V., NL; this protective architecture mitigates direct origin exposure but is not, by itself, proof of legitimacy.

Closing Assessment

Ordinary use is proportionate to the available evidence, provided that independent identity, service-term, and payment-protection checks are completed before credentials or payments are submitted.

Written analysis generated 2026-08-10 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

No rule findings contributed to this verdict.

Identity verification

Status

LIKELY

Identity score	76/100
Identity verification confidence	76%

- Trusted social count=2

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 eurobank.gr.

- The request stayed on eurobank.gr. It was not redirected to another domain. [CLEAR](#)
- The earliest public archive of this site is from 1999-01-16. [CLEAR](#)
- It is hosted on AKAMAI-ASN1, from a server in US. [NOTED](#)

Domain intelligence

Registrar	Not available
Hosting	AKAMAI-ASN1 - Akamai International B.V., NL
Country	US
Server IP	23.55.163.147
Name servers	Not available
SSL issuer	DigiCert Global G3 TLS ECC SHA384 2020 CA1
SSL expiry	2026-10-16
Domain age	27.56 years (continuous registration)
Domain expiry	Not available
Archive first seen	1999-01-16
Archive snapshots	49
Reputation	VirusTotal: 0 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about eurobank.gr 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.