

Is alrajhibank.com.sa legit? TrustSniffer's high-trust assessment: 100/100

alrajhibank.com.sa

Verdict

100

OUT OF 100

HIGH TRUST

alrajhibank.com.sa 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 75%.

What this site appears to be

Official Arabic retail site of a major Saudi bank offering accounts, cards, financing, insurance, loyalty programs, investor news, regulatory/licensing details and contact/support information.

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% confidence AbuseIPDB, 1 report; shared hosting inflates reports	CLEAR
Domain age	26 years old Registered history	CLEAR
Web archive	Archived since 2000 1201 snapshots	CLEAR
Certificate	Encrypted connection Issued by DigiCert Global G2 TLS RSA SHA256 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 2000.
- VirusTotal and Google Safe Browsing had no flags for this domain; its hosting IP carries AbuseIPDB reports below the confidence level TrustSniffer treats as a flag.

Full analysis

Overview

The website is the Arabic public-facing retail and commercial banking site of Al Rajhi Bank, presenting deposit accounts, cards, personal, automotive and mortgage financing, insurance, loyalty services, investor information, customer support and digital banking access. Its apparent business model is the provision of regulated banking and related financial services through online customer journeys and branch-supported channels.

Scam/Impersonation Risk

No contradictions were observed: the supplied evidence identifies no phishing, impersonation, malicious-content, blacklist, or conflicting-identity indicators. The site's Arabic branding, banking product structure, customer-support content and investor-related material are internally consistent with an established financial institution. One abuse report is associated with the hosting IP, but it is attributed to shared Oracle Public Cloud infrastructure, carries zero confidence, and is therefore not evidence that the website itself is abusive. The real-world operator identity remains independently unverified, so the legitimacy conclusion is evidence-consistent rather than proven. Evidence:

- The homepage is classified as a corporate banking site and presents accounts, cards, financing, insurance, loyalty services and digital banking.
- The page-level review records no red flags and no detected brand-impersonation or phishing indicators.
- The domain has a registration age of 25.973990417522245 years; archival records show 1,201 snapshots from 2000-08-19 through 2026-08-03, spanning 27 tracked years.

Regulatory Verification Notes

The site's legal and institutional content includes regulatory/licensing information, corporate-registration material, investor information and formal support channels. However, the supplied evidence does not independently verify a specific licence number or connect the online service conclusively to a real-world operator; this is a verification limitation rather than a scam indicator. The available external reputation context is clean overall, with no matched broker warning and no confirmed malicious or blacklist finding. Evidence:

- The homepage and associated institutional content identify regulatory/licensing details, investor information and corporate contact material.
- The site's transport encryption uses an OV certificate issued by DigiCert Global G2 TLS RSA SHA256 2020 CA1, valid through 2027-01-23.

- The page capture completed successfully with no sensitive form, hidden form or untrusted form destination detected.

What to Verify Next

Before credential or payment interactions, an institution should independently confirm that the domain is the official digital channel listed by the relevant bank or financial regulator, and confirm the applicable licence and legal-entity details through the regulator's registry. Account holders should also use independently sourced customer-service or branch contact details and confirm the applicable transaction, privacy, complaints and payment-protection terms before conducting material transactions. Evidence:

- The site provides customer-support, branch and contact information suitable for comparison with independently sourced institutional records.
- The homepage presents account opening and login entry points but no sensitive form was captured during review.
- The reviewed content includes privacy and cookie policy topics, customer support, branch/ATM information and investor relations.

Summary Verdict

Available evidence is consistent with an established, apparently legitimate banking website and supports a high-trust, low-risk posture for normal browsing and ordinary banking interaction. The classification is strong, while independent verification of the real-world operator remains incomplete.

Infrastructure Integrity

The site resolves through Oracle Corporation's US infrastructure, with no CDN or WAF detected in the supplied network assessment and one resolved address assessed as a likely origin rather than an edge address. This provides a conventional, identifiable hosting posture, while the absence of an intermediary protection layer means infrastructure controls should be treated as a mitigating factor only, not as proof of legitimacy. Evidence:

- Hosted on AS31898, ORACLE-BMC-31898 - Oracle Corporation, US.
- The infrastructure assessment recorded 1 unique IP, 0 edge IPs and 1 likely origin IP.
- The TLS certificate is OV-validated, issued by DigiCert Global G2 TLS RSA SHA256 2020 CA1, and expires 2027-01-23.

Closing Assessment

Ordinary use is proportionate to the high-trust assessment, provided credential and payment activity is preceded by the normal independent institutional, legal-entity, return-policy and payment-protection checks expected for financial services.

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.

Signals weighed against the site

- AbuseIPDB: 1 report on hosting IP 158.101.252.178 (Oracle Public Cloud, Data Center/Web Hosting/Transit), 0% confidence. The reports are attributed to shared infrastructure, not specifically to this website.

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 alrajhibank.com.sa.

- The request stayed on alrajhibank.com.sa. It was not redirected to another domain. CLEAR
- The earliest public archive of this site is from 2000-08-19. CLEAR
- It is hosted on ORACLE-BMC-31898, from a server in US. NOTED

Domain intelligence

Registrar	Not available
Hosting	ORACLE-BMC-31898 - Oracle Corporation, US
Country	US
Server IP	158.101.252.178
Name servers	Not available
SSL issuer	DigiCert Global G2 TLS RSA SHA256 2020 CA1
SSL expiry	2027-01-23
Domain age	25.97 years (continuous registration)
Domain expiry	Not available
Archive first seen	2000-08-19
Archive snapshots	1201
Reputation	VirusTotal: 0 flagged AbuseIPDB: 0% confidence, 1 report Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about alrajhibank.com.sa 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/alrajhibank.com.sa> · assessed 2026-08-10