

Is unicredit.it legit? TrustSniffer's high-trust assessment: 100/100

unicredit.it

Verdict

100

OUT OF 100

HIGH TRUST

unicredit.it 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 55%.

What this site appears to be

Official-looking UniCredit informational/marketing page describing retail banking products (accounts, cards, loans, investments), promotions, contact channels, and security advice. Provides customer support numbers and links to branch appointment booking and app download; contains promotional disclaimers and regulatory references.

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	CLEAR
	VirusTotal	
Google Safe Browsing	Not listed	CLEAR
	Google	
Abuse reports on the host	0 reports	NOTED
	AbuseIPDB; shared hosting inflates this count	
Domain age	26 years old	CLEAR
	Registered history	
Web archive	Never archived	WATCH
	No public history of this site	
Certificate	Encrypted connection	NOTED
	Issued by Actalis Organization Validated Server CA G3	

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).
- No flags from the reputation services TrustSniffer consulted at assessment time.

Full analysis

Overview

This is the UniCredit Italian retail-banking website, presenting personal and family banking services, digital banking, customer support, branch access, promotional offers, and financial products through an established corporate banking model.

Scam/Impersonation Risk

No contradictions were observed. The reviewed content is consistent with a corporate retail-bank presentation and contains no detected brand-impersonation, phishing, malicious-script, hidden-form, or suspicious external-submission indicators. The site's public-facing material includes structured banking information, security guidance, and customer-contact pathways rather than pressure tactics or anomalous transaction mechanisms.

EVIDENCE

- The homepage is classified as a corporate retail-banking marketing page and contains no detected impersonation or phishing indicators.
- Browser observation recorded no login form, hidden form, password submission to an external destination, wallet connection, clipboard-hijacking activity, or suspicious inline script.
- External reputation checks recorded zero malicious and zero suspicious detections, with the domain within the top one million of the observed global traffic ranking.

Regulatory Verification Notes

The site presents accounts, cards, loans, mortgages, investments, savings products, insurance, and digital banking services. Its promotional material includes a stated 4% gross annual remuneration offer for qualifying new customers and identifies promotional conditions and regulatory references. The reviewed content does not state a licensing authority or license number; this is a disclosure item for independent confirmation, not evidence of deception. Available registration, page-content, reputation, and transport-security signals are otherwise consistent with an established, apparently legitimate financial-services website, while the real-world operator identity remains likely rather than independently verified.

EVIDENCE

- The domain was registered on 2000-03-27 and is approximately 26.39 years old.
- Registration records identify CSC Corporate Domains, Inc. as registrar and UniCredit S.p.A. as the recorded owner and organization.
- The site is served from AS16625, operated by AKAMAI-AS — Akamai Technologies, Inc.
- TLS uses an OV certificate issued by Actalis Organization Validated Server CA G3 for UniCredit S.p.A., valid through 2026-12-24T14:30:54+00:00.

What to Verify Next

Before credential or payment interactions, independently confirm the applicable legal entity and customer-protection terms through authoritative institutional channels. The published branch-booking and contact routes can be compared with independently sourced institutional information, and any application or account-opening process should be reached through the confirmed official domain rather than an unsolicited message. Payment protections and dispute procedures should also be reviewed before a financially consequential transaction.

EVIDENCE

- The homepage provides links for branch appointment booking and customer contact.
- The site includes a dedicated security area containing fraud and account-security guidance.
- The website links to social-presence channels on Twitter, YouTube, LinkedIn, Instagram, and Facebook.

Summary Verdict

Available evidence supports a **high-trust, low-risk posture** consistent with an established, apparently legitimate website. The classification is strongly supported by convergence across substantive banking content, clean observed behavior, long-running domain registration, recognized infrastructure, and clean external reputation; it does not independently prove the real-world operator identity.

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. This reduces direct origin exposure and is a meaningful defensive control, although protective hosting infrastructure is a mitigating signal rather than proof of legitimacy.

Closing Assessment

Routine browsing is proportionate to the assessed posture; credential or payment use should follow ordinary independent checks of institutional identity, customer terms, and available payment protections.

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	80/100
Identity verification confidence	80%

- Trusted social count=5

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 unicredit.it.

- The request stayed on unicredit.it. It was not redirected to another domain. [CLEAR](#)
- Registration is published under CSC Corporate Domains, Inc.. [CLEAR](#)
- DNS for this domain is served by akam.net. [NOTED](#)
- The registration is paid up to 2026-10-18. [NOTED](#)
- It is hosted on AKAMAI-AS, from a server in US. [NOTED](#)

Domain intelligence

Registrar	CSC Corporate Domains, Inc.
Hosting	AKAMAI-AS - Akamai Technologies, Inc., US
Country	US
Server IP	104.126.124.141
Name servers	a13-67.akam.net a28-65.akam.net a22-64.akam.net a6-66.akam.net a11-66.akam.net a1-65.akam.net
SSL issuer	Actalis Organization Validated Server CA G3
SSL expiry	2026-12-24
Domain age	26.39 years (continuous registration)
Domain expiry	2026-10-18
Archive first seen	Not available
Archive snapshots	0
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 unicredit.it 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/unicredit.it> · assessed 2026-08-10