

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

btcblack.it

Verdict

100

OUT OF 100

HIGH TRUST

btcblack.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 2026-07-31 by automated analysis. Classification confidence 70%.

What this site appears to be

BTC Black presents a public cybersecurity clearinghouse offering DNS-queryable blocklists for illicit Bitcoin wallet addresses, abusive email-service and freemail accounts, and fuzzy hashes of spam content. It supplies a contact email for abuse reports and identifies a sponsor, with no visible forms or financial solicitations.

Evidence status and limitations

Evidence completeness:

UNKNOWN

- 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	7.7 years old Registered history	CLEAR
Web archive	Archived since 2019 81 snapshots	CLEAR
Certificate	Encrypted connection Issued by YR1	NOTED

The page as captured

No screenshot is retained for this report.

Key findings

- Automated classification: Not Scam.
- Domain age: 3 to 10 years (registration continuity).
- Public web-archive history exists since 2019.
- No flags from the reputation services TrustSniffer consulted at assessment time.

Full analysis

Overview

The website operates as a public cybersecurity clearinghouse, providing DNS-queryable blocklists for identifying Bitcoin wallets associated with illicit activity, abusive email accounts, and spam-content patterns for integration into security systems and email filters.

Scam/Impersonation Risk

No identity contradictions, phishing indicators, brand impersonation, or malicious reputation findings were observed. Its narrowly defined technical purpose is consistent across the available content and historical record: the Bitcoin list addresses wallet-abuse intelligence, while separate lists cover abusive email-service accounts, individual freemail accounts, and fuzzy hashes of related spam variants. This coherent service model, established provenance, and clean external reputation support the conclusion that the site is legitimate rather than a deceptive cryptocurrency operation.

- The domain was registered in 2018 and is approximately 7.65 years old; the registration is maintained through OVH.
- The archive record contains 81 snapshots spanning May 2019–May 2026, representing eight years of tracked history without an established suspicious repurposing or semantic shift.
- Reputation checks recorded zero malicious and zero suspicious detections, no external threat-list hit, and no reported abuse against the assessed infrastructure.
- The homepage describes standard DNS lookup integration and contains no login form, hidden form, financial solicitation, wallet connection, or sensitive-data request.

Regulatory Verification Notes

The service presents itself as an informational threat-intelligence utility supported by sponsorship, not as a broker, exchange, custodian, investment product, or transaction platform. Accordingly, the absence of an asserted financial-services licence is consistent with the stated business model and is not evidence of regulatory misconduct. The available homepage identifies SNB as sponsor and provides an abuse-reporting channel, although the supplied page set does not establish a detailed legal-entity statement or formal service terms; this is a limited documentation consideration rather than a legitimacy concern.

- The homepage identifies the service as “BTC Black — Blocklist Threat Clearinghouse” and names SNB as its sponsor.
- The homepage presents no deposit mechanism, consumer sale, trading facility, investment return, or licensing claim.

- The hosting infrastructure is served from AS16276 (OVH - OVH SAS, FR).
- The site's transport encryption uses a YR1-issued domain-validated TLS certificate, valid until 2026-09-20.

What to Verify Next

Enterprise adopters should validate the DNS response formats, list-update behavior, false-positive handling, and operational availability in a controlled environment before incorporating the feeds into production filtering. Procurement or compliance teams may also request the service operator's usage terms, data-sourcing methodology, correction process, retention practices, and service-level commitments, while independently confirming official contact channels for any formal relationship.

- The homepage states that each blocklist can be queried independently through standard DNS and integrated into existing security systems and email filters.
- The Bitcoin list is described as covering wallet addresses associated with fraud, scams, ransomware, and other illicit activity.
- The email-focused lists use hashed account identifiers, while the content-focused list uses ZOrder locality-sensitive hashes.
- The site publishes a channel for enquiries and abuse reports but exposes no interactive submission form.

Summary Verdict

The website is a legitimate, established, and trustworthy cybersecurity utility. Its coherent identity, sustained provenance, benign observed behavior, and clean reputation collectively support a high-confidence trust posture with no contradictory risk signals.

Infrastructure Integrity

The site uses OVH-hosted protective CDN/WAF infrastructure in France; the single observed address was an edge endpoint, and the origin server was not exposed during the assessment. This arrangement reduces direct origin exposure and is a mitigating security control, although infrastructure protection alone is not proof of legitimacy.

Closing Assessment

Normal interaction, including routine access, standard use, and account login if such functionality is introduced through the official service, is appropriate; production reliance should follow ordinary technical validation and supplier due diligence.

Written analysis generated 2026-07-31 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	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 btcblack.it.

- The request stayed on btcblack.it. It was not redirected to another domain. CLEAR
- Registration is published under OVH. CLEAR
- DNS for this domain is served by snb.it. NOTED
- The registration is paid up to 2026-12-08. NOTED
- The earliest public archive of this site is from 2019-05-11. CLEAR
- It is hosted on OVH, from a server in FR. NOTED

Domain intelligence

Registrar	OVH
Hosting	OVH - OVH SAS, FR
Country	FR
Server IP	151.80.178.91
Name servers	ns0.snb.it ns1.snb.it
SSL issuer	YR1
SSL expiry	2026-09-20
Domain age	7.7 years
Domain expiry	2026-12-08
Archive first seen	2019-05-11
Archive snapshots	81
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 btcblack.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.