

Is mailin.fr legit? TrustSniffer's high-trust assessment: 90/100

mailin.fr

Verdict

90

OUT OF 100

HIGH TRUST

mailin.fr appears legitimate.

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

Not Scam

Safe for Login

Low Risk

Assessed 2026-08-17 by automated analysis. Classification confidence 55%.

What this site appears to be

Notification/landing page indicating this domain is used by Sendinblue to host tracking links and images for customers; provides abuse contact info and links to privacy policy.

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	16 years old Registered history	CLEAR
Web archive	Never archived No public history of this site	WATCH
Certificate	Encrypted connection Issued by WE1	NOTED

The page as captured

<https://mailin.fr/>



What mailin.fr served when TrustSniffer captured it on 2026-08-17. The page may look different now.

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.
- The operator behind the site could not be independently connected to a real-world brand or person.

Full analysis

Overview

This website is an informational technical-domain notice for Sendinblue, an all-in-one email marketing and transactional-email platform. It explains that the domain is used by customers to send newsletters and transactional messages, host images, and provide tracking links, indicating a SaaS communications and subscription-based business model rather than a consumer-facing financial or commerce service.

Scam/Impersonation Risk

No contradictions were observed: the available evidence contains no confirmed phishing, impersonation, or malicious-detection finding. The page content is consistent with a professional technical-domain notice, including a stated zero-tolerance spam policy and an abuse-reporting process. A separate automated brand-similarity indicator was not corroborated by the page itself, which consistently identifies the Sendinblue use case; observed script and external-traffic anomalies likewise produced no sensitive form, credential-capture, wallet, cloaking, or related high-risk behavior. The long-established registration, clean external reputation, and substantial traffic footprint further support an apparently legitimate site.

EVIDENCE

- The homepage is titled “Sendinblue technical domain” and describes newsletter, transactional-email, tracking-link, and hosted-image functions.
- The domain was registered through OVH on 2010-12-27 and is approximately 15.65 years old.
- External reputation checks recorded 0 malicious and 0 suspicious detections, with no malicious safe-browsing finding; the domain is ranked 16254 and is within the top 1 million globally.

Regulatory Verification Notes

The site presents an operational brand and service explanation, but the real-world operator identity is not independently verified by the available evidence. Its content describes a SaaS email service rather than a regulated financial product, and it makes no financial-services license or registration claim; this is a disclosure point for ordinary business verification, not evidence of deception. The linked privacy policy and abuse-reporting route are consistent with a functioning commercial communications platform. Available technical legitimacy signals converge positively, including recognized hosting infrastructure and valid transport encryption.

EVIDENCE

- The site is served from AS13335, CLOUDFLARENET — Cloudflare, Inc., US.
- The TLS certificate uses issuer WE1, has DV validation, and is valid to 2026-09-27.
- The homepage provides a privacy-policy link and describes an abuse-reporting process for unsolicited messages.

What to Verify Next

Before credential or payment interactions, an interested party should independently confirm the relevant Sendinblue/Brevo corporate entity, review the applicable subscription terms and privacy documentation, and confirm that any commercial payment flow uses expected payment protections. Official contact channels should be confirmed through an independent route rather than relying solely on links encountered in an email.

EVIDENCE

- The observed page contains one contact/abuse-report form and no sensitive form.
- No password-submission-to-an-external-destination, wallet-provider, wallet-drainer, or clipboard-hijacking behavior was observed.
- The page completed two successful behavioral runs with stable HTTP responses.

Summary Verdict

Available evidence is consistent with an established, apparently legitimate website with a low overall risk posture. The classification is well supported by convergence across the page’s coherent service explanation, long operating history, clean reputation, traffic presence, and valid security controls, while operator identity remains independently unverified.

Infrastructure Integrity

The site is fronted by Cloudflare's CDN/WAF, and the observed addresses were CDN edge servers rather than directly exposed origin infrastructure. This provides a meaningful mitigation against direct origin exposure and routine abuse, but it remains an infrastructure-control signal rather than proof of corporate legitimacy.

Closing Assessment

Normal low-risk browsing is proportionate; credentials or payments should be limited to interactions that pass the ordinary independent identity, terms, and payment-protection checks described above.

Written analysis generated 2026-08-17 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 mailin.fr.

- The request stayed on mailin.fr. It was not redirected to another domain. CLEAR
- Registration is published under OVH. CLEAR
- DNS for this domain is served by cloudflare.com, across 2 name servers. NOTED
- The registration is paid up to 2028-12-27. CLEAR
- It is hosted on CLOUDFLARENET, from a server in US. NOTED

Domain intelligence

Registrar	OVH
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US
Server IP	104.17.158.243
Name servers	jim.ns.cloudflare.com, kate.ns.cloudflare.com
SSL issuer	WE1
SSL expiry	2026-09-27
Domain age	15.65 years (continuous registration)

Domain expiry	2028-12-27
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 mailin.fr 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/mailin.fr> · assessed 2026-08-17