# Campaign Readiness Report

Scan ID: b6f79467-c4a5-41d5-8e4a-7785d827a7c5 · Generated: 2026-01-20T17:28:24.757Z

**Headline**

High risk: fix authentication and stability before sending.

Verdict: **high** · Confidence: **low** · Ready: **No**

## SCORES

| EMAIL | WEBSITE | CAMPAIGN RISK |
|---|---|---|
| **30** | **100** | **50** |
| high_risk | strong | high |

## WHY THIS VERDICT

- DMARC is missing (no policy enforcement possible).
- DKIM signing is missing.
- SPF record is missing.

## BLOCKERS

- **DKIM record not detected via DNS.** hard
- **SPF record is missing.** hard
- **DMARC is missing.** hard

## WARNINGS

- None

## TOP ACTIONS

### Publish a DMARC record

impact: high · effort: low

DMARC is the control plane for email authentication. No DMARC means no policy and weak domain protection.

**Steps**

- Start with policy=none and rua reporting enabled.
- Confirm all legitimate sources are aligned (SPF/DKIM).
- Then move to quarantine/reject.

### Enable DKIM signing for your sending domain

impact: high · effort: medium

DKIM is required for stable inbox placement and for DMARC alignment.

**Steps**

- Enable DKIM in your ESP (generate selector + DNS records).

- Publish the DKIM DNS records and verify they resolve publicly.
- Send a test to multiple mailbox providers and confirm DKIM=pass.

### Publish an SPF record for your sending domain impact: medium effort: low

SPF helps mailbox providers validate your sending sources and supports DMARC alignment.

**Steps**

- List only your legitimate sending sources (ESP, CRM, transactional).
- End with ~all initially if you’re unsure, then move to -all when stable.
- Keep DNS lookups ≤ 10.