AUDITLABHQ · BENCHMARK 2026

Préparation DNS email de 100 enseignes e-commerce actives en France

Un état des lieux reproductible de SPF, DMARC, MX, MTA-STS et TLS-RPT sur les domaines publics des enseignes, réalisé le 2026-08-21.

100/100
domaines analysés

67.0%
avec DMARC appliqué

21.0%
avec un risque SPF public

4.0%
avec MTA-STS détecté

Résultat central. 7.0% des domaines analysés n'ont pas de politique DMARC détectable, et 26.0% restent en surveillance uniquement (p=none).

Distribution de l'indice DNS public

Le score médian est de **76.5/100**. Il mesure uniquement des signaux DNS publics et ne constitue ni un test de placement en boîte de réception, ni une certification de conformité Gmail ou Outlook.

Ce que les données montrent

- 79.0% ont un SPF sans anomalie détectée par le scanner.
- 67.0% appliquent DMARC avec p=quarantine ou p=reject.
- 4.0% publient MTA-STS et 4.0% publient TLS-RPT.

Résultats par catégorie

Catégorie	Domaines	Score médian	DMARC absent	Niveau solide
Beauty	10	78.0	20.0%	30.0%
Culture and pets	8	65.0	0.0%	12.5%
Electronics	10	78.0	0.0%	20.0%
Fashion	25	78	8.0%	44.0%
Grocery	12	76.5	0.0%	33.3%
Home and DIY	15	75	0.0%	40.0%
Marketplace	10	76.5	0.0%	30.0%
Sports	10	60.0	30.0%	10.0%

Méthodologie

Échantillon raisonné de 100 enseignes disposant d'un site marchand accessible au marché français. Les requêtes sont réalisées sur le domaine public de l'enseigne. Le score attribue 30 points à SPF, 45 à DMARC, 10 à MX, 10 à MTA-STS et 5 à TLS-RPT.

DKIM est volontairement exclu du score. Sa vérification fiable nécessite le sélecteur utilisé par l'expéditeur ou l'en-tête d'un message réel. Une absence de clé sur quelques sélecteurs courants ne prouve pas l'absence de DKIM.

Limites : le domaine du site peut différer du domaine d'envoi marketing; les DNS évoluent; SPF valide ne prouve pas l'alignement d'un message; DMARC p=none satisfait certains minima mais n'applique pas de protection. Les résultats doivent être décrits comme un état des lieux DNS public.

Contexte fournisseurs

Google demande notamment SPF, DKIM et DMARC aux expéditeurs de plus de 5 000 messages quotidiens vers Gmail. Microsoft impose également ces mécanismes aux expéditeurs à fort volume vers Outlook.

Sources officielles : https://support.google.com/mail/answer/81126 · https://techcommunity.microsoft.com/blog/microsoftdefenderforoffice365blog/4399730

À propos d'AuditLabHQ

AuditLabHQ analyse les principaux signaux d'authentification et de sécurisation email d'un domaine, puis fournit une synthèse et un plan d'action PDF.