GUIDE DE

BONNE COMMUNICATION ENTRE E-ROUTEURS ET OPÉRATEURS

alliance digitale :
dma France
MMAf
iab. France

Sommaire

Introduction

Dans un écosystème numérique en constante mutation, l'email demeure le pilier central du marketing relationnel. Pourtant, la **délivrabilité** constitue un défi permanent, exigeant une agilité technique et une rigueur opérationnelle de chaque instant.

Ce guide, élaboré par le groupe **Délivrabilité de l'Alliance Digitale**, a été conçu pour instaurer une collaboration plus fluide et transparente entre les **e-routeurs** et les **opérateurs de messagerie (MBP)**, qu'ils opèrent en environnement B2B ou B2C.

OBJECTIF DU DOCUMENT

L'ambition de ce document est double :

- **Sensibiliser et accompagner :** offrir aux acteurs de l'envoi une vision claire des bonnes pratiques en vigueur (authentification, conformité juridique, normes anti-spam).

- **Optimiser la résolution technique :** fournir des recommandations concrètes pour faciliter l'échange d'informations, accélérer l'identification des incidents techniques et minimiser les risques de blocages ou de faux positifs.

En encourageant une approche proactive et une compréhension mutuelle, ce guide vise à renforcer la qualité globale des campagnes, à consolider la confiance entre les parties prenantes et à pérenniser l'efficacité du marketing digital.

PUBLIC CIBLE

Ce document s'adresse prioritairement aux **membres de l'Alliance Digitale.** Il est destiné à des professionnels possédant un socle de compétences techniques solide, leur permettant d'appréhender et d'appliquer efficacement les préconisations détaillées.

ÉVOLUTION ET MISE À JOUR

Le secteur de la délivrabilité étant par nature mouvant, ce guide n'est pas un document figé.
Il a vocation à **être actualisé régulièrement** afin de refléter fidèlement les évolutions du marché, les nouvelles exigences technologiques, le contexte juridique et les mutations des politiques de filtrage des opérateurs.

Partie 1

De la bonne prise des éléments fournis par les opérateurs

LA RÉPUTATION CHEZ LES E-ROUTEURS

Pour simplifier le discours vis-à-vis de leurs clients, quelques e-routeurs (Dolist, Brevo…) ont bâti des scores de réputation basés sur l'ensemble des données qu'ils possèdent et qui sont assez riches (désabonnement, plainte, ouverture, clic, spam trap, etc.).

Ces scores permettent notamment :

- de **souligner de mauvaises pratiques** pour les routeurs
- de **suivre une métrique** qui permet notamment de se comparer aux autres expéditeurs de leur catégorie et de suivre l'adéquation de leur pratique marketing par rapport aux contraintes de délivrabilité, pour les utilisateurs finaux des CRM.

LA RÉPUTATION CHEZ LES FOURNISSEURS DE MESSAGERIE

Principalement deux acteurs ont mis à disposition des principes de réputation ou de score.

Gmail présentait cette notion dans ses dashboards de monitoring (voir section II – A), mais l'a abandonné dans ses outils V2 fin 2025.

Microsoft : la réputation existe sous la forme de deux grandes familles d'indicateurs.

Le SNDS visible sur un site web dédié :

- **Le (SNDS)** (voir section II – B), mais cette donnée semble de moins en moins pertinente.

Les autres scores visibles dans l'entête du message, ils sont au nombre de trois.

- **Le SCL (Spam Confidence Level Score)** : l'indicateur permet de jauger le niveau de spam de votre message. Il est compris entre 1 (non-Spam) et 9 (Spam). Ce score est visible dans l'entête technique X-MS-Exchange-Organization-SCL sur chaque message.
- **Le BCL (Bulk Complaint Level)** particulièrement dédié aux expéditeurs d'email en masse. Il est compris entre 0 (non-Spam) et 9 (Spam- nombre élevé de plaintes). Ce score est visible dans l'entête X-Microsoft-Antispam sur le champ BCL sur chaque message.
- **Le PCL (Phishing Confidence Level)** qui indique votre message (le contenu principalement) est perçu ou non comme du phishing.
  De 1 à 3 : Le contenu du message n'est pas susceptible d'être du phishing.
  4 à 8 : Le contenu du message est susceptible d'être du phishing.

LA RÉPUTATION CHEZ LES PLATEFORMES TIERCES SPÉCIALISÉES

Quelques autres indicateurs sont produits par des plateformes tierces privées et notamment :

- **SenderScore (https://senderscore.org/)**, basé principalement sur les données de Microsoft, il vous indiquera si globalement votre trafic email est bien considéré (d'après beaucoup de paramètres, qui sont plus ou moins pertinents selon votre activité), mais il ne représente pas votre réputation sur Orange ou Gmail ou tout autre opérateur de messagerie.

- **Talosintelligence.com**, qui collecte toutes les données de volume gérées par ses services de sécurité, ses services cloud (Cisco Secure Mail), ses réseaux de pièges et de nombreuses autres sources. Talos utilise un score granulaire sur l'IP d'envoi d'email allant de - 10 à + 10, ensuite simplifié pour l'utilisateur en trois catégories : Good, Neutral, et Poor.
  Source : https://support.talosintelligence.com/docs/email-reputation/

Au fil du temps, les opérateurs ont mis en place un certain nombre de services en ligne permettant d'analyser les blocages et la délivrabilité des domaines et IP d'expédition. Ce chapitre fait le point sur les principaux outils, leur usage, leur utilité et la façon dont peuvent être interprétées les informations qui remontent.

A. GPT ou Google Postmaster Tool

Google Postmaster Tools est un **service d'analyse et de monitoring gratuit** développé par Google qui permet de **surveiller**, **analyser** et **optimiser** leurs performances de délivrabilité spécifiquement sur l'écosystème Gmail et Google Workspace.

Lancé officiellement en juin 2015, il permettait enfin aux annonceurs d'accéder à la réputation de leurs domaines et IPS, levant ainsi une réelle « black box » autour des critères de Gmail.
Au fil des années, Postmaster Tools **a enrichi ses tableaux de bord**, proposant le suivi de la réputation de domaine et IP, l'analyse des échecs d'authentification (SPF, DKIM, DMARC), les erreurs de distribution et des taux de spam. Ce **suivi est journalier**, ce qui est remarquable, quand on connait le volume de données reçues quotidiennement par Gmail.

La version 2, déployée en milieu d'année 2024, intègre plusieurs nouveaux tableaux de bord et modernise l'interface.

ABANDON DE LA NOTION DE RÉPUTATION PRÉSENTE DANS LA VERSION 1

Elle se caractérise par l'abandon des notions de réputation d'IP et domaine. Google **explique** les trois (3) raisons de cette suppression :

- Les **données de réputation** ne sont pas facilement exploitables pour la plupart des expéditeurs.
- Les **changements de comportement de l'expéditeur** mettent du temps à se refléter dans le tableau de bord existant. On peut corriger un problème (pression marketing, hygiène de liste, authentification…), et constater que la "réputation" met du temps à se mettre à jour.
- Le **tableau de bord actuel** peut être trompeur, car la réputation n'est qu'un des nombreux facteurs qui affectent la délivrabilité. En effet, en pratique, on peut avoir une « réputation » correcte, mais toujours avoir des problèmes d'Inbox (contenu, plaintes, spam, ciblage, engagement, anomalies de volume, erreurs de config, etc.).

Malgré cela, la réputation qui est largement utilisée dans le vocabulaire des gestionnaires de délivrabilité avait enfin une concrétisation sous forme de quatre couleurs. Elle permettait de concrétiser une notion abstraite et pédagogique qui manque actuellement.

La nouvelle interface contient des éléments plus concrets en ce qui a trait à la conformité et aux signaux observables (plaintes pour SPAM, erreurs de livraison, authentification, conformité générale de l'émetteur…), au lieu d'un score global.

Elle permet désormais d'identifier plus aisément la raison d'un rejet ou d'un retard, rendant la gestion proactive incontournable. Elle vérifie la conformité aux exigences de Gmail, le taux de mise en spam, les détails sur les erreurs de remise, l'authentification et le chiffrement TLS.

Constamment mise à jour, GPT est donc la référence incontournable pour les responsables de délivrabilité, soucieux de maintenir une réputation optimale pour l'expéditeur et d'identifier finement les problèmes techniques et de réputation de Gmail (plus de 1,8 milliard d'utilisateurs actifs, estimation 2025).

MODALITÉ D'ACCÈS À GPT

L'accès aux données nécessite préalablement la vérification de la propriété du domaine d'envoi via l'ajout d'un enregistrement DNS de type TXT contenant une clé de validation spécifique.

Important à noter : les statistiques ne s'affichent dans l'interface qu'après avoir atteint un volume minimal d'emails envoyés vers Gmail, seuil non communiqué publiquement par Google, mais estimé à plusieurs centaines d'emails par jour. Cette condition garantit la pertinence statistique et la fiabilité des données présentées, évitant les fluctuations liées à de faibles volumes.

L'outil propose un historique détaillé des performances sur plusieurs mois (jusqu'à 120 jours), facilitant l'analyse des tendances temporelles, l'identification des corrélations avec les campagnes spécifiques et l'évaluation quantitative de l'impact des optimisations techniques ou stratégiques mises en place.

Les données peuvent être exportées (par API ou autres) pour intégration dans des rapports personnalisés ou des dashboards tiers.

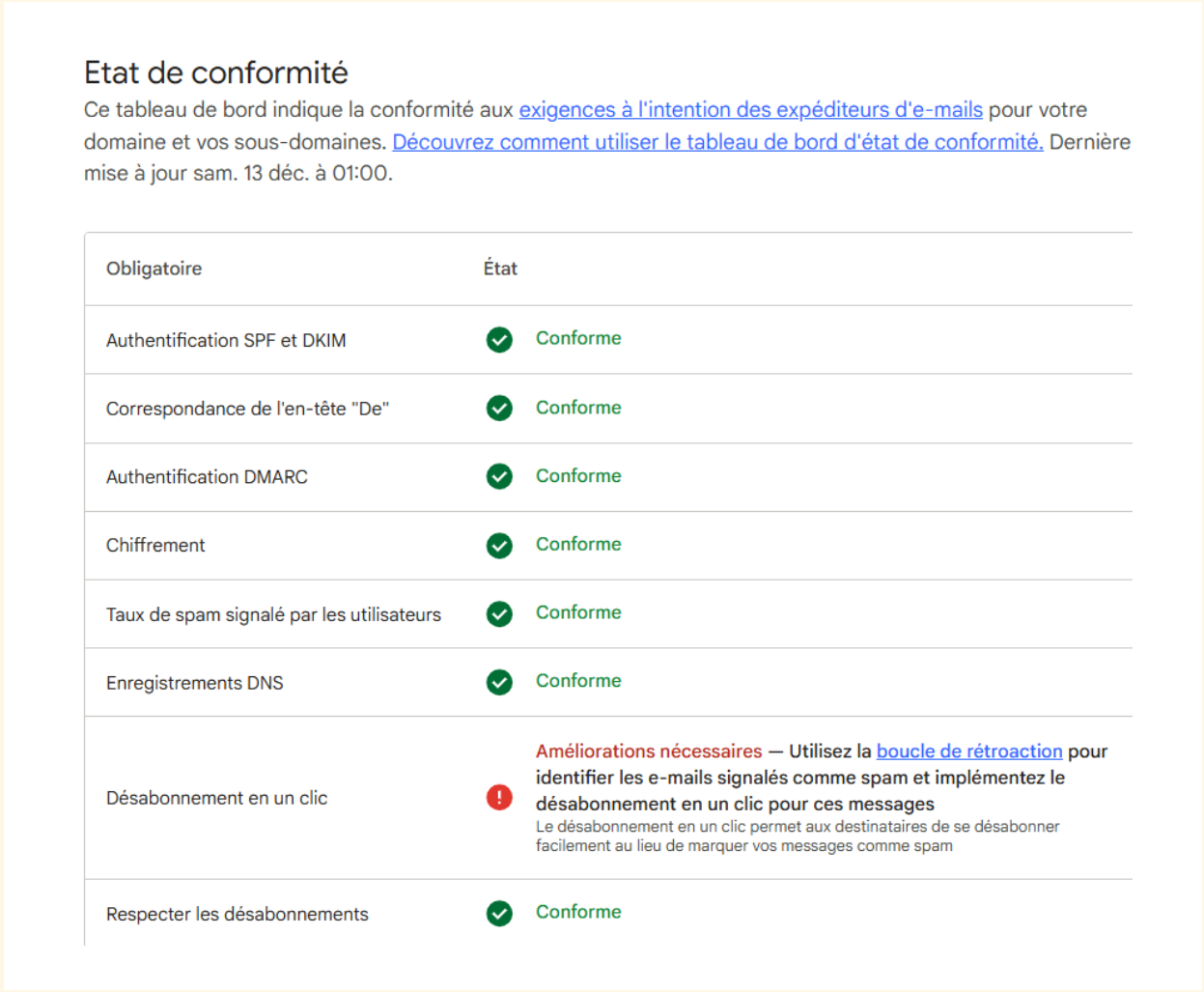
Enfin, l'outil est accessible facilement, quels que soient le e-routeur utilisé et la configuration (IP dédiée ou mutualisée), en déposant un code dans le DNS du domaine d'expédition qui est en général facilement accessible. Cette facilité d'accès tranche avec l'accès du SNDS souvent bloqué par les ESP, notamment dans des contextes d'IP mutualisées.

LES DIFFÉRENTS ÉCRANS DISPONIBLES

L'interface assez intuitive de GPT propose un tableau de bord complet organisé autour de plusieurs indicateurs clés essentiels :

État de conformité

Un écran permet, d'un seul coup d'œil, de faire le point sur votre conformité technique par rapport aux Consignes Google pour les expéditeurs.



Etat de conformité

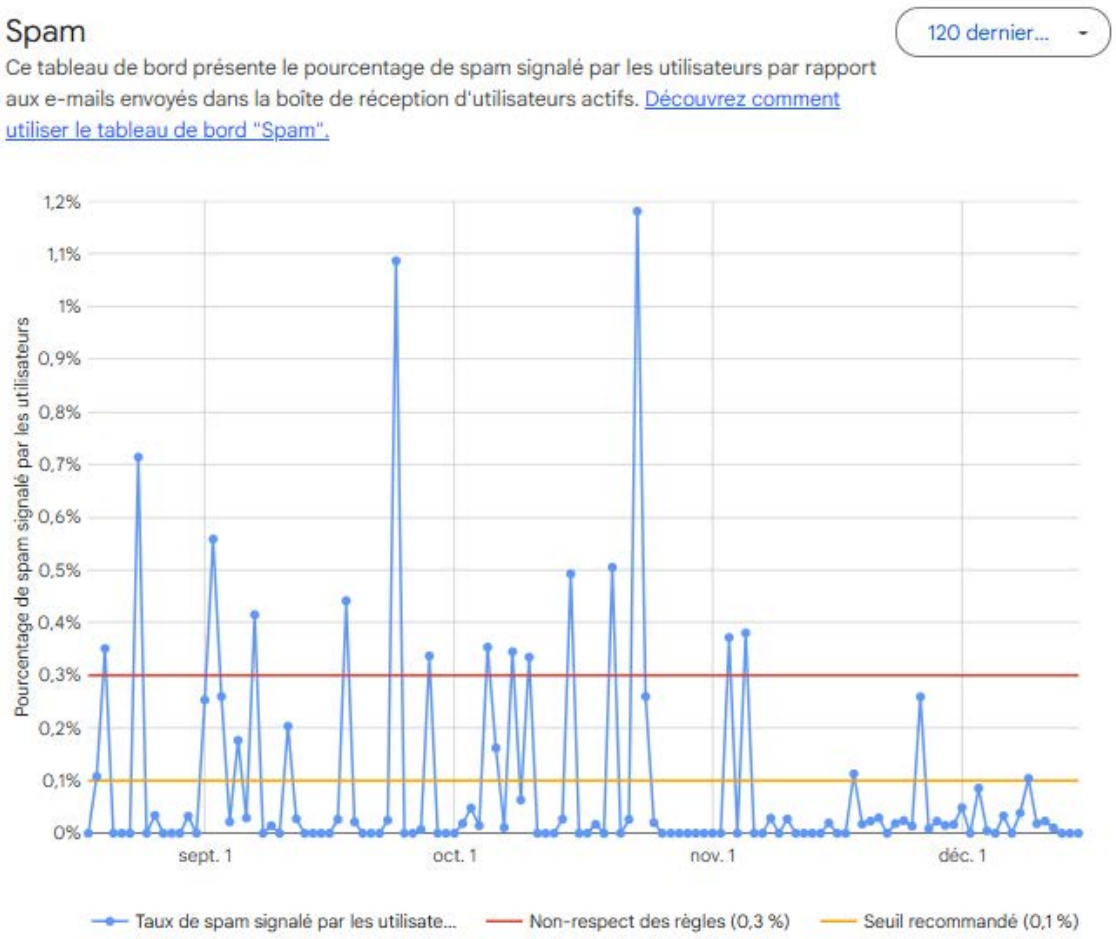
Ce tableau de bord indique la conformité aux exigences à l'intention des expéditeurs d'e-mails pour votre domaine et vos sous-domaines. Découvrez comment utiliser le tableau de bord d'état de conformité. Dernière mise à jour sam. 13 déc. à 01:00.

Obligatoire	État
Authentification SPF et DKIM	Conforme
Correspondance de l'en-tête "De"	Conforme
Authentification DMARC	Conforme
Chiffrement	Conforme
Taux de spam signalé par les utilisateurs	Conforme
Enregistrements DNS	Conforme
Désabonnement en un clic	Améliorations nécessaires — Utilisez la boucle de rétroaction pour identifier les e-mails signalés comme spam et implémentez le désabonnement en un clic pour ces messages Le désabonnement en un clic permet aux destinataires de se désabonner facilement au lieu de marquer vos messages comme spam
Respecter les désabonnements	Conforme

- Les données du tableau de bord concernent **uniquement les messages envoyés vers des comptes Gmail personnels**. Sont donc exclus les messages de Google Workspace
- Les indicateurs de conformité **ne sont pas en temps réel :** les changements apparaissent généralement sous **24 heures ou plus**.
- L'état de conformité est affiché **au niveau du domaine principal uniquement**, même si l'analyse s'appuie sur les sous-domaines.
- Les sous-domaines contribuent au calcul, mais **ne disposent pas d'un état de conformité distinct**.
- En cas de **faible volume d'envoi**, certaines données peuvent être **absentes** afin de préserver la confidentialité des utilisateurs Gmail.
- **Certaines exigences ne concernent que les expéditeurs d'emails en masse**.

Spam

C'est un des rapports les plus importants, car il permet l'accès d'une métrique incontournable pour permettre de délivrer vos emails en boite de réception. C'est le taux de spam.



Date ↓	Taux de spam signalé par les utilisateurs	Moins de 0,3 %
18 août 2025	0,00 %	Oui
19 août 2025	0,11 %	Oui

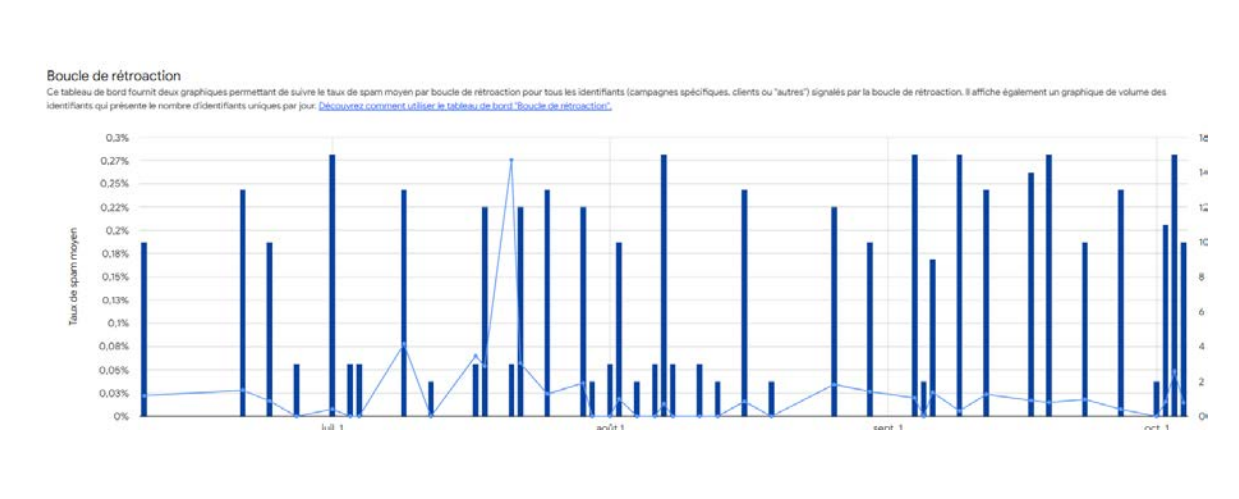
« Le taux de spam correspond au pourcentage de vos messages distribués dans la boite de réception d'un destinataire engagé, puis marqués comme spam par le destinataire. »

L'interface Gmail gérant nativement plusieurs onglets, ce sont uniquement les emails arrivés en boite de réception qui sont pris en compte, et non ceux arrivés dans les autres onglets (type notifications, commercial, etc.).

Le **taux maximum de spam toléré** est de 0,3 % et la bonne pratique est de 0,1%. Au-delà, un nombre de plus en plus grand d'email sera déposé dans l'onglet Spam.

Google précise ensuite : « *Si Gmail envoie automatiquement un nombre important de vos messages dans le dossier "Spam", le taux indiqué dans le tableau de bord peut sembler faible, car les destinataires reçoivent moins de messages de votre part dans leur boite de réception.* »

La Boucle de rétroaction



Google offre la possibilité **d'identifier la campagne** (granularité à définir librement par l'e-routeur), qui a causé un taux de spam en utilisant la donnée passée dans le "Feedback-ID" déclaré dans l'entête de l'email (*cf.* doc).

Exemple de codage :
Feedback-ID: 34935245:34935245.4849825:us9:mc

Par conséquent, une campagne ID 34935245, qui a généré un taux de spam de 0,02 %, produit les résultats suivants :

DATE	IDENTIFIANTS SIGNALÉS	TAUX DE SPAM
10 juin 2025	34935245	0,02 %

Des contraintes techniques sur le DKIM, SPF et enregistrements PTR sont données dans la doc de Google pour éviter notamment le spoofing du Feedback-ID.

Ci-dessous un résumé du fonctionnement du Feedback-ID :

FEEDBACK-ID

Exemple : campaign:segment:esp:SenderId

(**Analyse** de Gmail)
4 champs pris en compte → en partant de la droite

Génération des données FBL
(si Sender Id ≠vide)

Signature DKIM OBLIGATOIRE
- Après ajout Feedback-ID
- Domaine contrôlé par l'expéditeur

Validation Portmaster Tools
- Domaine DKIM ajouté
- Domaine validé

Exigences techniques
- 1 seul Feedback-ID valide
- IP d'envoi publiées en SPF
- PTR + hostname cohérents

Génération des rapports FBL
- Identifiant répété sur un volume suffisant
- Plusieurs signalements spam

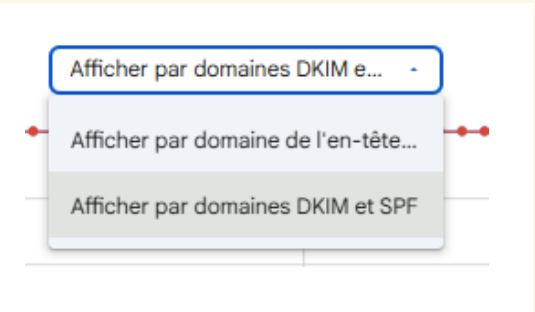
Agrégation des données FBL
- Par identifiant **unique**
- < **3** indentifiants conseillés
- Pas d'ID **unique**/message

La **granularité de la déclaration du codage du Feedback-ID** peut permettre au e-routeur de bien remonter les campagnes ou "parties" de campagne qui ont posé des problèmes de plainte. Finement géré du côté de l'annonceur, ce dispositif permet de **bien identifier**, en complément de la segmentation, **les groupes d'adresse ou segments qui posent des problèmes** de plainte et d'entreprendre **des actions correctrices plus fines.**

L'analyse de l'authentification liée aux protocoles SPF, DKIM et DMARC

Dans le haut du tableau, un menu déroulant permet d'afficher **deux types d'analyse d'authentification.**

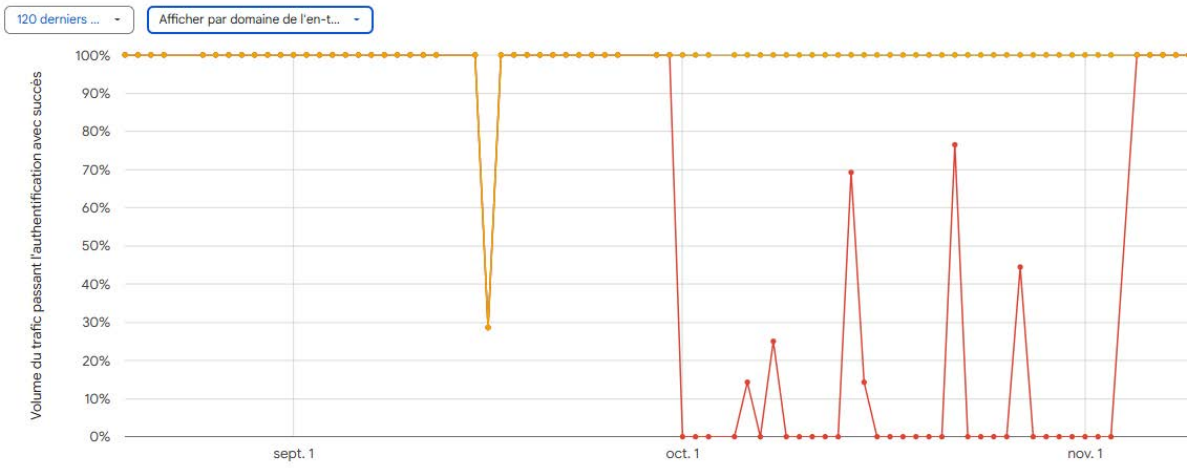
Si on sélectionne l'option « Afficher par domaines DKIM et SPF », le tableau de bord **ne montre pas le taux de réussite DMARC.** Le **tableau de bord d'authentification** affiche le pourcentage de vos emails qui réussissent les tests SPF, DKIM et DMARC.



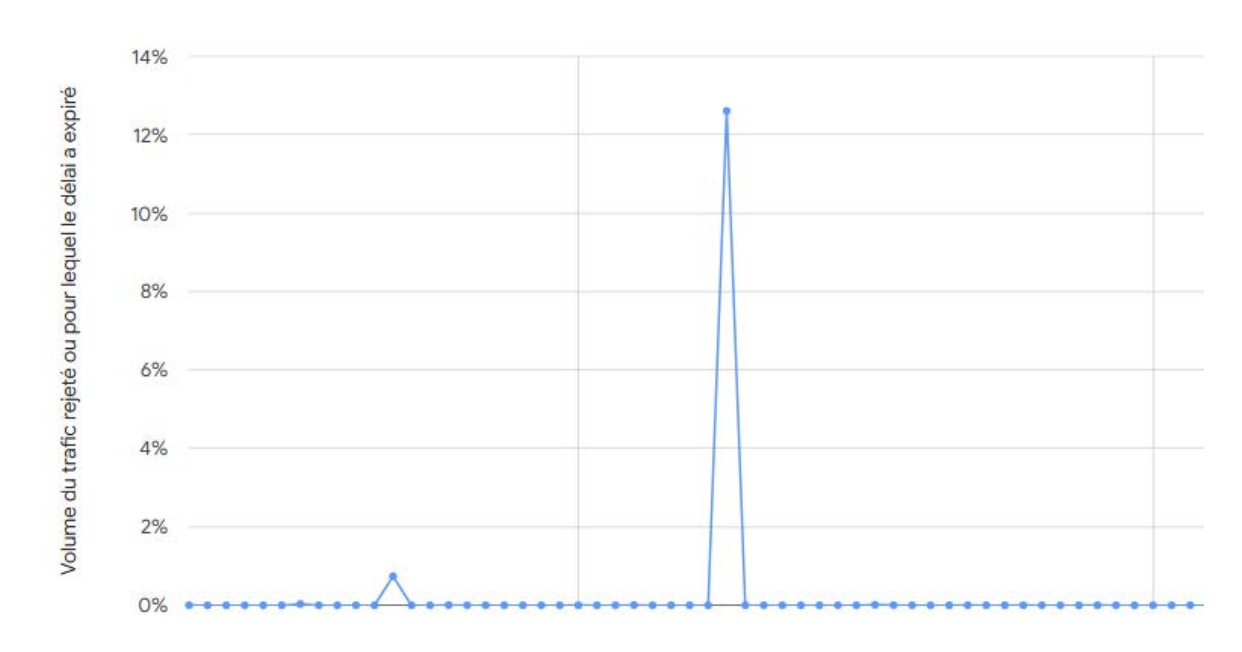
Ce tableau de bord présente les données des messages dont l'entête FROM contient votre domaine d'envoi.

Gmail précise « *Afin de protéger la confidentialité des utilisateurs de Gmail, le tableau de bord peut ne pas afficher toutes les données les jours où le volume d'emails sortants est faible. Cela peut avoir une incidence sur les informations affichées. Le seuil n'est pas précisément connu, mais il avoisine les 300 à 500 @ /jour* ».

Enfin, les transferts ou forward automatique rendent parfois caduques les normes d'authentification DKIM, notamment, et **peuvent avoir un impact de quelques %**, sur le pourcentage d'emails authentifiés par Gmail ou être plus fort si le volume d'envoi est faible (voir copie d'écran ci-dessous).



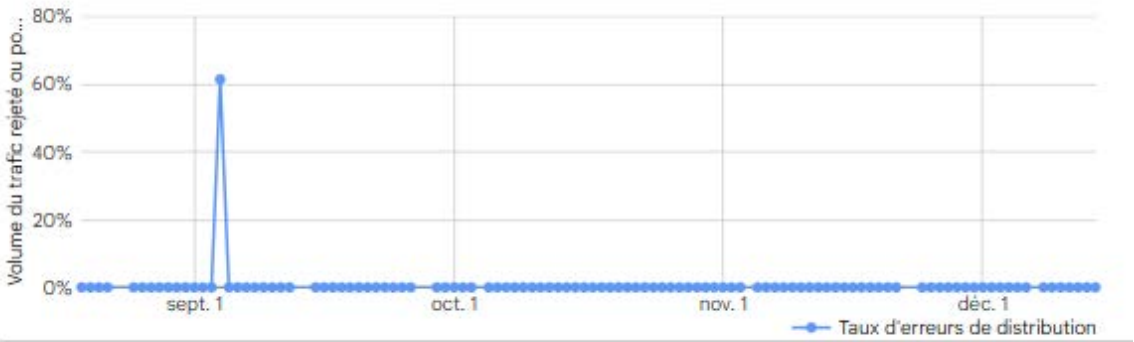
Les erreurs de distribution



Le tableau de bord « Erreurs de distribution » affiche le pourcentage de messages authentifiés (SPF ou DKIM) rejetés ou ayant temporairement échoué, par rapport au nombre total de messages authentifiés. Ce tableau de bord affiche également :

- **Volumes de rejet de messages et d'échec temporaire**
- **Motif du rejet du message ou de la défaillance temporaire**

Exemple de motif de rejet



Date ↓	Type d'erreur	Motif	Pourcentage
4 sept. 2025	Refus	Suspicion de spam	61,40 %

Google fournit les différents types de motifs de rejet et les actions à mettre en œuvre.

1. Fréquence maximale dépassée

Cause du blocage : un volume ou une cadence d'envoi anormalement élevée.
Gmail détecte des pics ou des variations brutales de trafic depuis un domaine ou une adresse IP et applique une limitation temporaire pour protéger ses utilisateurs.

2. Suspicion de spam

Cause du blocage : accumulation de signaux négatifs liés au comportement d'envoi.
Plaintes pour spam, faible engagement des destinataires, envois répétés vers des contacts inactifs ou qualité de base insuffisante dégradent la confiance accordée par Gmail.

3. Emails susceptibles d'être du spam

Cause du blocage : contenu du message jugé à risque.
Certains éléments (liens, structure HTML, vocabulaire promotionnel agressif) augmentent la probabilité que le message soit classé comme spam, indépendamment de l'infrastructure d'envoi.

4. Pièce jointe incorrecte ou non compatible

Cause du blocage : format de pièce jointe non autorisé ou perçu comme dangereux.
Gmail bloque les messages contenant des fichiers incompatibles ou présentant un risque pour la sécurité des destinataires.

5. Règles DMARC du domaine d'envoi

Cause du blocage : échec des contrôles DMARC avec une politique restrictive.
Lorsque la politique DMARC est définie sur le rejet, tout message ne respectant pas l'alignement SPF et DKIM est automatiquement refusé.

6. Adresse IP d'envoi avec mauvaise réputation

Cause du blocage : historique défavorable associé à l'adresse IP.
Une adresse IP ayant suscité des plaintes pour spam ou ayant montré un comportement d'envoi fluctuant est jugée peu fiable par Gmail.

7. Domaine d'envoi avec mauvaise réputation

Cause du blocage : perte de crédibilité du domaine dans la durée.
La répétition de signaux négatifs (engagement faible, pression marketing excessive, plaintes) dégrade durablement la confiance accordée au domaine.

8. Adresse IP listée dans une ou plusieurs RBL

Cause du blocage : présence de l'adresse IP sur des listes de blocage publiques.
Ces inscriptions résultent généralement d'activités assimilées au spam ou à des incidents de sécurité.

9. Domaine listé dans une ou plusieurs listes noires publiques

Cause du blocage : identification du domaine comme source abusive par des organismes tiers.
Cette situation affecte l'ensemble des envois réalisés avec ce domaine, quel que soit le message.

10. Enregistrement PTR incorrect ou manquant

Cause du blocage : configuration DNS incomplète ou incohérente.
L'absence ou l'incohérence de l'enregistrement PTR constitue un signal technique négatif pour Gmail, entrainant des refus de messages.

EN SYNTHÈSE

Google Postmaster permet d'identifier rapidement les dysfonctionnements techniques, les problèmes de configuration ou les dégradations réputationnelles susceptibles d'affecter significativement l'Inbox placement et les performances des campagnes emailing.

Google Postmaster Tools s'intègre parfaitement dans une stratégie globale et multicompte de monitoring de la délivrabilité, complétant les données fournies par d'autres outils de réputation comme :

- **Microsoft SNDS pour Outlook,**
- **Yahoo Sender Hub,**
- **ou encore les plateformes tierces spécialisées (250ok, Validity, MXToolbox et Cisco…), offrant ainsi une vision exhaustive de la performance de délivrabilité cross-provider.**

B. Microsoft SNDS

Le Smart Network Data Services (SNDS) de Microsoft fournit une série de métriques détaillées pour chaque adresse IP enregistrée. Ces métriques sont basées sur l'activité d'envoi d'emails vers les domaines Microsoft publics (comme outlook.com, hotmail.fr, msn.fr, etc.). Ces données sont agrégées quotidiennement à minuit PST (Pacific Standard Time), et leur restitution peut prendre plusieurs heures. Elles sont disponibles sous 90 jours glissants.

Les métriques sont accessibles via l'interface web ou via une API (export CSV). Pour qu'une IP affiche des données, elle doit avoir envoyé au moins 100 messages par jour.

La réputation présente dans le SNDS se base sur le SRD
Le SRD est un échantillon permanent de sondage qui se compose d'utilisateurs réels d'Outlook et de Hotmail. Microsoft sélectionne des utilisateurs (les «Spam Fighters») pour voter sur la nature des messages qu'ils reçoivent.

Le processus de vote

1. Copie miroir

Lorsqu'un email arrive dans la boite de réception d'un membre du panel, Microsoft génère parfois une **seconde copie identique du message**.

2. Le « Sondage »

Cette copie est présentée à l'utilisateur *via* **une bannière spéciale** demandant : *« Ce n'est pas un courrier indésirable (Spam) ou c'est un courrier indésirable (Not Spam) ? »*

3. L'action

L'utilisateur clique sur l'un des deux boutons. Ce vote est déconnecté de l'action de « Supprimer » ou de « Mettre en spam » habituelles ; c'est **un vote purement qualitatif pour entrainer l'IA** de Microsoft (SmartScreen).

Exemple d'email provenant du SRD (les libellés actuellement utilisés pour le vote peuvent avoir été changés).

Ce message a été envoyé par l'équipe chargée de la sécurité.

Classification du courrier indésirable

De : **preventjunk@live.com**
Envoyé :
À :

Merci de nous aider à lutter contre le courrier indésirable ! Veuillez examiner le message électronique ci-dessous et nous dire s'il s'agit ou non d'un courrier indésirable en cliquant sur le bouton de votre choix. Si vous consultez ce message depuis le Web et sélectionnez l'option "C'est un courrier indésirable" ci-dessous, le message sera automatiquement supprimé de votre boîte de réception.

Ce n'est pas un courrier indésirable	Je souhaite recevoir ce message dans ma boîte de réception. Il ne s'agit pas de courrier indésirable.
C'est un courrier indésirable	C'est un courrier indésirable. Je ne souhaite pas recevoir ce message ni les messages similaires dans ma boîte de réception.

Ce message électronique vous a été envoyé car vous vous êtes porté volontaire pour nous aider à lutter contre le courrier indésirable. Si vous avez changé d'avis, vous pouvez mettre fin à votre participation. Cette adresse de messagerie n'est pas contrôlée, merci de ne pas répondre directement à ce message mais d'utiliser le bouton de votre choix ci-dessus.

Si vous utilisez MSN® Hotmail, une page de confirmation s'affichera chaque fois que vous signalerez un courrier indésirable. Si vous le souhaitez, vous pouvez modifier ce paramètre.

De :
Objet : Qu'avez-vous pense de Mon Voisin Totoro?
Reçu :

Pour continuer à recevoir nos offres : ajoutez l'adresse dans vos Contacts
Changer votre adresse email dans votre profil de compte.

DES MILLIONS DE PRODUITS NEUFS ET D'OCCASION

Livres | CD | DVD | Jeux vidéo | Tel. & PDA | Informatique | Image&Son | Maison | Sport | Enfant | Mode

Partagez votre avis et aidez des millions d'acheteurs

Bonjour Emeric,

Vous avez récemment fait un achat sur Nous espérons que vous en avez été satisfait.

Partagez votre opinion sur ce(s) produit(s) avec l'ensemble des , votre avis permettra de les aider lors de leurs prochains achats !

Mon Voisin Totoro
> Donnez votre avis

Samsung S2 Portable HXMU050DA - Disque dur ...
> Donnez votre avis

Vous trouverez également une liste de produits sur lesquels vous pourrez certainement donner votre avis.

voir la liste

Vous pouvez consulter l'ensemble de vos avis sur la page "Tous mes avis", accessible depuis votre compte.
> Voir tous vos avis

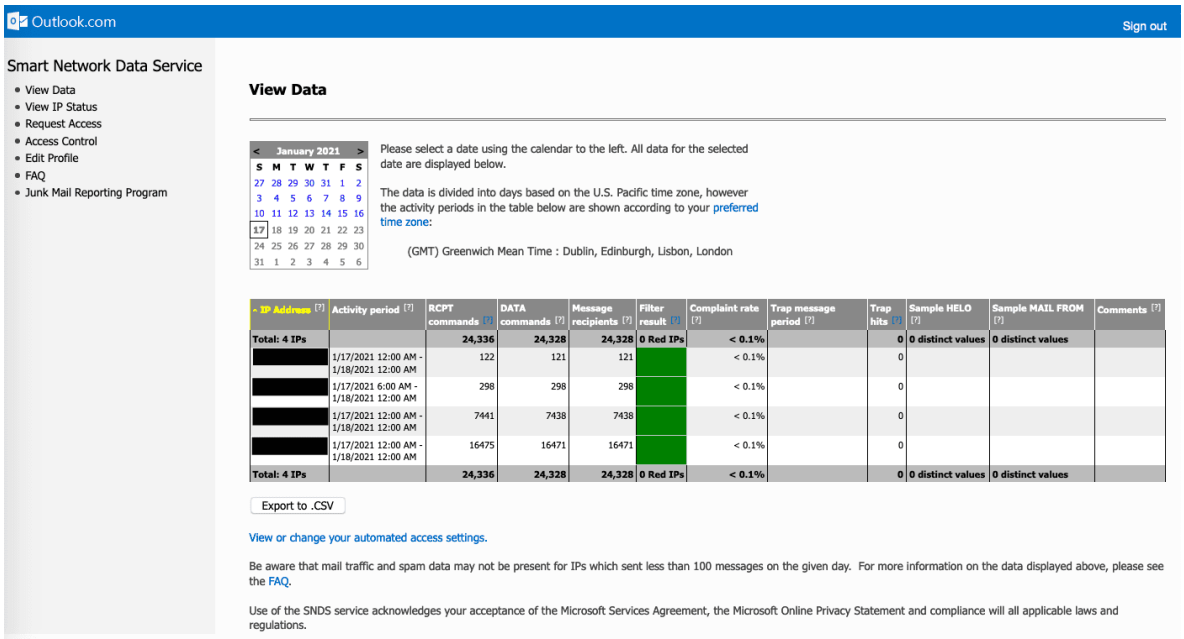
Apportez également votre aide en votant sur les avis déposés par les autres

Retrouvez des millions de produits sur

A tout de suite sur

Si vous ne souhaitez plus recevoir le bilan d'activité sur les avis, vous pouvez vous désinscrire.

Description des informations et métriques exposées



Outlook.com — Sign out

Smart Network Data Service

- View Data
- View IP Status
- Request Access
- Access Control
- Edit Profile
- FAQ
- Junk Mail Reporting Program

View Data

< January 2021 >

S	M	T	W	T	F	S
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

Please select a date using the calendar to the left. All data for the selected date are displayed below.

The data is divided into days based on the U.S. Pacific time zone, however the activity periods in the table below are shown according to your preferred time zone:

(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

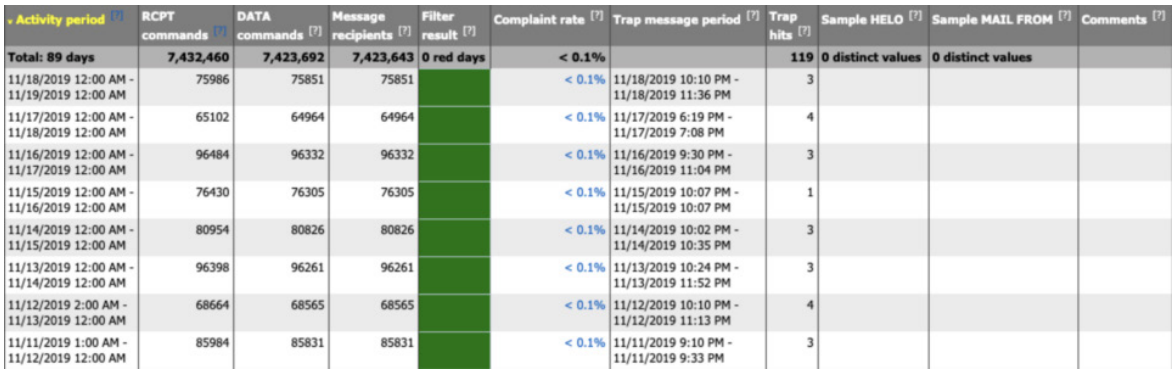
IP Address [?]	Activity period [?]	RCPT commands [?]	DATA commands [?]	Message recipients [?]	Filter result [?]	Complaint rate [?]	Trap message period [?]	Trap hits [?]	Sample HELO [?]	Sample MAIL FROM [?]	Comments [?]
Total: 4 IPs		24,336	24,328	24,328	0 Red IPs	< 0.1%		0	0 distinct values	0 distinct values	
[redacted]	1/17/2021 12:00 AM - 1/18/2021 12:00 AM	122	121	121		< 0.1%		0			
[redacted]	1/17/2021 6:00 AM - 1/18/2021 12:00 AM	298	298	298		< 0.1%		0			
[redacted]	1/17/2021 12:00 AM - 1/18/2021 12:00 AM	7441	7438	7438		< 0.1%		0			
[redacted]	1/17/2021 12:00 AM - 1/18/2021 12:00 AM	16475	16471	16471		< 0.1%		0			
Total: 4 IPs		24,336	24,328	24,328	0 Red IPs	< 0.1%		0	0 distinct values	0 distinct values	

Export to .CSV

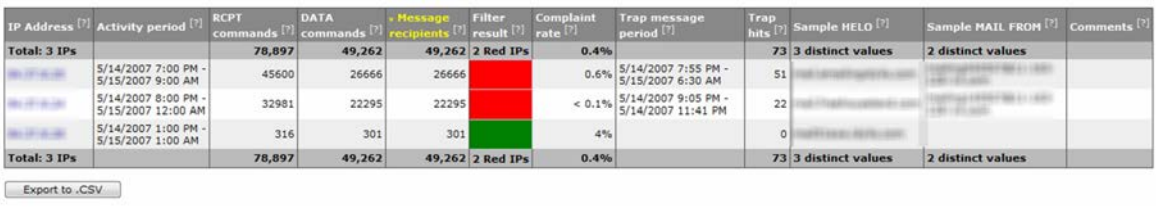
View or change your automated access settings.

Be aware that mail traffic and spam data may not be present for IPs which sent less than 100 messages on the given day. For more information on the data displayed above, please see the FAQ.

Use of the SNDS service acknowledges your acceptance of the Microsoft Services Agreement, the Microsoft Online Privacy Statement and compliance will all applicable laws and regulations.



Activity period [?]	RCPT commands [?]	DATA commands [?]	Message recipients [?]	Filter result [?]	Complaint rate [?]	Trap message period [?]	Trap hits [?]	Sample HELO [?]	Sample MAIL FROM [?]	Comments [?]
Total: 89 days	7,432,460	7,423,692	7,423,643	0 red days	< 0.1%		119	0 distinct values	0 distinct values	
11/18/2019 12:00 AM - 11/19/2019 12:00 AM	75986	75851	75851		< 0.1%	11/18/2019 10:10 PM - 11/18/2019 11:36 PM	3			
11/17/2019 12:00 AM - 11/18/2019 12:00 AM	65102	64964	64964		< 0.1%	11/17/2019 6:19 PM - 11/17/2019 7:08 PM	4			
11/16/2019 12:00 AM - 11/17/2019 12:00 AM	96484	96332	96332		< 0.1%	11/16/2019 9:30 PM - 11/16/2019 11:04 PM	3			
11/15/2019 12:00 AM - 11/16/2019 12:00 AM	76430	76305	76305		< 0.1%	11/15/2019 10:07 PM - 11/15/2019 10:07 PM	1			
11/14/2019 12:00 AM - 11/15/2019 12:00 AM	80954	80826	80826		< 0.1%	11/14/2019 10:02 PM - 11/14/2019 10:35 PM	3			
11/13/2019 12:00 AM - 11/14/2019 12:00 AM	96398	96261	96261		< 0.1%	11/13/2019 10:24 PM - 11/13/2019 11:52 PM	3			
11/12/2019 2:00 AM - 11/13/2019 12:00 AM	68664	68565	68565		< 0.1%	11/12/2019 10:10 PM - 11/12/2019 11:13 PM	4			
11/11/2019 1:00 AM - 11/12/2019 12:00 AM	85984	85831	85831		< 0.1%	11/11/2019 9:10 PM - 11/11/2019 9:33 PM	3			



IP Address [?]	Activity period [?]	RCPT commands [?]	DATA commands [?]	Message recipients [?]	Filter result [?]	Complaint rate [?]	Trap message period [?]	Trap hits [?]	Sample HELO [?]	Sample MAIL FROM [?]	Comments [?]
Total: 3 IPs		78,897	49,262	49,262	2 Red IPs	0.4%		73	3 distinct values	2 distinct values	
[redacted]	5/14/2007 7:00 PM - 5/15/2007 9:00 AM	45600	26666	26666		0.6%	5/14/2007 7:55 PM - 5/15/2007 6:30 AM	51	[redacted]	[redacted]	
[redacted]	5/14/2007 8:00 PM - 5/15/2007 12:00 AM	32981	22295	22295		< 0.1%	5/14/2007 9:05 PM - 5/14/2007 11:41 PM	22	[redacted]	[redacted]	
[redacted]	5/14/2007 1:00 PM - 5/15/2007 1:00 AM	316	301	301		4%		0	[redacted]		
Total: 3 IPs		78,897	49,262	49,262	2 Red IPs	0.4%		73	3 distinct values	2 distinct values	

Export to .CSV

1. Période d'activité (activity period)

Indique la première et la dernière heure pendant laquelle des emails ont été envoyés depuis l'adresse IP. Cette information permet d'identifier **les fenêtres temporelles d'activité** pour établir des corrélations avec d'éventuels problèmes.

2. Commandes RCPT et DATA (RCPT & DATA commands)

RCPT : Nombre de tentatives de contact des destinataires pendant les sessions SMTP
DATA : Nombre de messages effectivement transmis

3. Destinataires de messages (message recipients)

Nombre total de destinataires réels qui ont reçu les messages (quel que soit le nom de domaine Microsoft sollicité). Ce chiffre est généralement proche des commandes RCPT. Un écart important peut mettre en avant une "attaque au dictionnaire" (technique de spam).

4. Verdict Spam (filter result) issu du SRD

Indique une **estimation de pourcentage de messages considérés comme spam** par des panels d'utilisateurs. L'indicateur peut prendre trois couleurs :

- **Vert : Verdict de spam < 10%.** Indique une faible probabilité de spam ; les emails sont généralement considérés comme légitimes et ont une bonne chance d'atteindre la boite de réception.
- **Jaune : 10 % < Verdict de spam < 90%.** Indique des résultats mixtes ; une partie significative des emails est filtrée comme spam, mais pas la majorité. Cela nécessite une investigation pour identifier les causes (contenu, volume, etc.).
- **Rouge : Verdict de spam > 90%.** Indique une forte probabilité de spam ; la plupart des emails sont bloqués ou filtrés comme indésirables.

Même si cet indicateur reste assez subjectif en fonction des panels d'utilisateurs sollicités, il est intéressant à analyser sur la durée.

5. Taux de plaintes (complaint rate)

Fraction des messages signalés comme indésirables par les utilisateurs de messageries Microsoft. Ce taux doit être maintenu sous 0,3%, au-delà, ce taux suggère un contenu non désiré ou la sollicitation d'une liste non consentante.

6. Horodatage et sollicitation d'adresses pièges (trap message period & trap hits)

Première et dernière minute de sollicitation d'une adresse piège suivi du nombre de sollicitations. Met souvent en évidence une liste mal acquise ou obsolète.

7. Message échantillon (sample MAIL FROM)

Un **échantillon par jour et par type** (plaintes ou pièges) pour tenter d'identifier la communication responsable et analyser les problèmes.

8. Exemple de commande HELO (sample HELO)

Identifiant envoyé par le serveur SMTP. Il devrait correspondre au domaine d'envoi, si ce n'est pas le cas, on peut soupçonner un problème d'usurpation d'identité.

9. Commentaires (comments)

Champ textuel avec des détails supplémentaires pouvant fournir du contexte sur le blocage, comme :

- « JMR P1 Sender » : Plainte reçue.
- « JMR Block » : IP bloquée pour abus.
- « Virus Detected» : Malware détecté.
- « Open Proxy Detected » : Proxy ouvert (violation de politique).

C. Yahoo! Sender Hub

Le Yahoo! Sender Hub est **une plateforme développée par Yahoo pour aider les expéditeurs d'emails à optimiser leurs campagnes de marketing par email**, en particulier pour les destinataires utilisant des boites mail Yahoo, AOL ou Verizon. Elle vise à **améliorer la délivrabilité, l'engagement** et **la confiance** des utilisateurs envers les marques. Lancée pour soutenir les professionnels du marketing digital, elle fournit des ressources essentielles pour naviguer dans l'écosystème des emails, en respectant les normes de confidentialité et de sécurité.

Services proposés :

- **Inscription à la Boucle de rétroaction** (Complaint Feedback Loop) :
  L'outil permet de configurer et de gérer la boucle de rétroaction. Lorsqu'un utilisateur clique sur « Spam », l'expéditeur reçoit un rapport lui permettant de retirer le plaignant de sa base. La configuration s'appuie désormais sur les domaines authentifiés par DKIM.
- **Sender Hub Insight** (depuis octobre 2025) :
  Ce tableau de bord offre une visibilité directe sur les performances de vos envois. Il fournit des indicateurs cruciaux :
  - **Volume distribué :** Le nombre d'emails ayant effectivement atteint la boite de réception (Inbox).
  - **Taux de plainte (Spam complaint rate) :** Particularité très importante de Yahoo, ce taux est calculé **uniquement sur la base des emails ayant atteint la boite de réception** (et non sur le volume total envoyé). Un taux situé entre 0,1 % et 0,3 % est considéré comme une zone de danger (« warning »), et un taux supérieur à 0,3 % menace gravement la délivrabilité.
- **Modalité d'accès :**
  L'accès nécessite la création d'un compte sur le Sender Hub et la validation de la propriété du domaine en s'appuyant sur l'authentification DKIM. Les données du tableau de bord Insights s'affichent généralement après 24 à 48h, sous réserve d'avoir atteint un volume d'envoi quotidien minimum requis par Yahoo.

D. Orange Postmaster Page

Orange étant le principal FAI en France, la maitrise de sa politique de filtrage est vitale pour tout acteur du marketing relationnel sur le marché français. Bien qu'Orange ne propose pas un tableau de bord analytique dynamique comme Google ou Yahoo, son site officiel **Postmaster Orange** (*postmaster.orange.fr*) fait autorité pour comprendre les règles et résoudre les incidents vers les domaines orange.fr et wanadoo.fr.

Règles et informations exposées

Le site documente de manière transparente les exigences de l'opérateur pour accepter le trafic entrant :

1. Exigences techniques strictes

Orange impose désormais **l'authentification SPF, DKIM et DMARC** pour les expéditeurs de masse (plus de 1 000 emails/jour). Le chiffrement TLS et un enregistrement PTR (Reverse DNS) valide sont également obligatoires.

2. Limitation de cadence (Throttling)

Les consignes précisent **les limites physiques à respecter,** par exemple, un maximum de 2 connexions simultanées par adresse IP, 100 messages par connexion, et un poids maximum de 45 Mo par email.

3. Référentiel des codes d'erreur (OFR_)

Le site répertorie **tous les codes de rebond** (bounces) **spécifiques à Orange**. Comprendre ces codes internes (ex : erreurs OFR_xxx indiquant un blocage anti-spam, une adresse IP bloquée, ou une limitation de volume temporaire) est indispensable pour configurer les règles de «retry» ou de mise en quarantaine au niveau du e-routeur.

4. Gestion des plaintes

Orange vise **un taux de plainte extrêmement bas** (inférieur à 0,3 %, avec des filtrages de protection déclenchés dès 0,6 %). La boucle de rétroaction (Feedback Loop) est généralement gérée en partenariat avec l'association Signal Spam pour les membres éligibles.

Résolution et mitigation

Le site Postmaster est **la porte d'entrée pour joindre l'« Abuse Desk » d'Orange**. En cas de blocage d'IP (listing) ou de problème de filtrage persistant, il permet d'utiliser un formulaire de contact pour soumettre une demande de déblocage. Lors de ces demandes, il est impératif de fournir des éléments techniques précis (IP source, domaine, date de l'incident, code SMTP renvoyé).

E. Hornet Security (SenderTool)

Vade (racheté par la société allemande HornetSecurity puis récemment acquis par Proofpoint) est un **acteur européen majeur de la cybersécurité et du filtrage des emails**. Sa technologie protège des milliers de boites aux lettres dans le monde, notamment celles de grands FAI (comme SFR, Free, Laposte.net en France) ainsi que de nombreux environnements d'entreprise (Microsoft 365).

Le **Vade Secure Sender Tool** est un outil spécifique conçu pour aider les expéditeurs légitimes à auditer et corriger leur réputation vis-à-vis des algorithmes de filtrage de Vade.

Fonctionnalités

Contrairement aux outils des opérateurs grand public, le Sender Tool de Vade est avant tout un outil de remédiation et de vérification d'infrastructure de routage :

1. Gestion des blocages (Demande de délistage)

C'est la **fonction névralgique pour les équipes délivrabilité des e-routeurs**. Si vos adresses IP se retrouvent sur une blockliste interne de Vade (entrainant des rejets massifs chez les FAI protégés par leur technologie), le Sender Tool permet de soumettre de manière encadrée une demande de délistage («delisting») ou de mitigation.

2. Prévention des faux positifs

L'outil permet **d'identifier plus rapidement** si un blocage est dû à une empreinte de contenu pénalisée par l'IA ou à un comportement d'envoi suspect (hausse anormale des volumes).

3. Précaution importante

Comme dans toute médiation, il est important **d'identifier au préalable et dans la mesure du possible l'origine du blocage opéré**. S'il est de votre fait, corriger l'erreur et contacter Vade pour exposer la situation, décrire les mesures prises et demander une mitigation. Si le blocage vous semble injustifié et que vous avez à faire à un faux positif, n'hésitez pas à les contacter, mais soyez bien sûr de vous. Une réputation est en effet établie en fonction des demandes adressées.

Modalité d'accès

L'outil s'adresse principalement aux **professionnels du routage**, aux **administrateurs système** et aux **experts en délivrabilité**. La gestion des requêtes *via* le Sender Tool nécessite de montrer « patte blanche » : pour obtenir un déblocage, l'expéditeur doit généralement fournir des **preuves de légitimité** (explications sur la collecte des données, correction des configurations techniques, preuve du consentement) afin que les équipes ou les algorithmes de Proofpoint/Vade réévaluent positivement la réputation de l'IP.

F. Signal Spam

Signal Spam n'est pas un opérateur de messagerie à proprement parler, mais une **association française issue d'un partenariat public-privé** (regroupant la CNIL, les autorités publiques, les professionnels de l'emailing et les FAI). Sur le marché français, son rôle est absolument central. Contrairement aux opérateurs américains qui gèrent leurs propres outils d'analyse de réputation, les grands acteurs français (Orange, SFR, La Poste) s'appuient en grande partie sur les données collectées par Signal Spam, générées par les internautes qui signalent les messages abusifs *via* des modules installés sur leurs navigateurs ou clients de messagerie.

Fonctionnalités et métriques exposées

L'interface membre de Signal Spam offre un tableau de bord analytique qui centralise les alertes de plaintes, comblant ainsi le « point aveugle≈» de la délivrabilité sur les messageries françaises :

1. La Boucle de Rétroaction (Feedback Loop – FBL) unifiée

C'est la **fonctionnalité névralgique pour les e-routeurs et les annonceurs**. Lorsqu'un utilisateur clique sur « Signaler comme Spam » *via* le module, l'alerte remonte dans la FBL. L'expéditeur reçoit cette information (format ARF - Abuse Reporting Format) afin de désinscrire immédiatement le plaignant de sa base de données.

2. Suivi volumétrique des plaintes

Le tableau de bord permet de visualiser **les pics de signalements associés à vos adresses IP** ou vos noms de domaine lors de vos envois sur les FAI français partenaires.

3. Lutte contre le Phishing et l'usurpation

L'espace membre permet aux marques d'être alertées si leur identité (nom de domaine) est usurpée dans des campagnes frauduleuses signalées par les utilisateurs, facilitant ainsi les actions de blocage (takedown) des URL malveillantes.

Modalité d'accès et d'engagement

L'accès aux données de Signal Spam est soumis à **des règles beaucoup plus strictes et institutionnelles** que les outils en libre accès comme Google Postmaster :

1. Adhésion et Déontologie

L'accès aux tableaux de bord et à la FBL nécessite d'être **membre de l'association** (adhésion payante pour les entreprises). L'adhésion est conditionnée par la signature d'une **Charte de déontologie stricte**, par laquelle le membre s'engage à respecter les meilleures pratiques de collecte de données et à traiter les plaintes avec diligence.

2. Le rôle pivot de l'e-routeur

Sur le marché, ce sont très majoritairement les **e-routeurs** (ESP) **qui adhèrent à Signal Spam**. Ils se connectent à l'API de l'association pour récupérer les signalements et les intègrent directement dans les statistiques de leurs propres plateformes. Les plaignants sont ainsi placés automatiquement en quarantaine sans action manuelle de l'annonceur.

3. L'accès direct pour l'annonceur

Un annonceur peut tout à fait **adhérer en son nom propre** s'il souhaite avoir une vision directe de sa réputation ou s'il gère sa propre infrastructure d'envoi (On-Premise), ce qui constitue un gage de sérieux fort auprès des FAI français.

Partie 2

Notion de codes par opérateur, rappel des grandes catégories qu'il faut savoir identifier

Les échanges SMTP reposent sur des normes internationales (*cf.* partie précédente). Toutefois, dans la pratique opérationnelle, chaque opérateur de messagerie (B2C ou B2B) applique des politiques de filtrage spécifiques.

Ces politiques peuvent : enrichir les réponses SMTP standards ; ajouter des identifiants internes ; introduire des mécanismes dynamiques de limitation (rate limiting) ; différencier les comportements selon la réputation IP, le domaine ou l'engagement de l'utilisateur ;

Il est donc indispensable pour les e-routeurs :
- de ne pas interpréter les codes de manière isolée
- d'intégrer les spécificités opérateurs dans leurs moteurs de décision
- d'adopter une grille de lecture fonctionnelle commune

A. Notion de codes "par opérateur" (Mailbox providers & B2B gateways)

Les opérateurs respectent les RFC (SMTP, Enhanced Status Codes), mais les implémentent avec leurs propres logiques de filtrage.

Exemples de documentations officielles :
- Gmail :
  https://support.google.com/mail/answer/3726730
  https://postmaster.google.com/
- Yahoo / AOL :
  https://senders.yahooinc.com/smtp-error-codes/
- Microsoft :
  https://learn.microsoft.com/en-us/troubleshoot/exchange/email-delivery/ndr/fix-error-code-550-5-7-1-in-exchange-online
  https://sender.office.com/
- Orange :
  https://postmaster.orange.fr/

Ces pages doivent être consultées en cas d'anomalie persistante.

B. Pourquoi les opérateurs "dépassent" la norme

Les **RFC définissent la structure des réponses**, mais pas :
- les seuils de tolérance,
- les politiques antispam,
- les règles de réputation
- les modèles de machine learning
- les critères d'engagement

Un même code peut donc recouvrir des réalités différentes selon l'opérateur.

Exemple :
- 421 4.7.0 chez Gmail → limitation dynamique
- 421 4.7.0 chez Yahoo → TSS04 (temporary deferral)
- 421 4.7.0 en B2B → politique interne de gateway

Les opérateurs peuvent également ajouter :
- des tags internes (ex : TSS04)
- des identifiants policy (ex : 5.7.511 chez Microsoft)
- des codes propriétaires (ex : OFR_ chez Orange)

Il est donc recommandé :
- d'analyser le code étendu X. Y.Z
- d'examiner le Diagnostic-Code
- de corréler avec les métriques globales

C. Les grandes catégories à identifier (la grille "réflexe")

Afin d'harmoniser les pratiques, les retours SMTP doivent être classés selon **4 grandes catégories fonctionnelles.**

Problème d'adresse / données (souvent définitif)

Codes typiques

5.1.1 – user unknown
5.1.2 – domain invalid

Nature du problème

Adresse inexistante ou incorrecte.

Impact
- Dégradation de la réputation si maintien en base
- Signal négatif envoyé aux opérateurs

Recommandation
- Suppression après confirmation
- Mise en place de mécanismes de validation en amont

Attention

Ne pas confondre avec des blocages policy (5.7.x).

Boite pleine / compte désactivé (mix)

Codes typiques

4.2.2 – mailbox full
5.2.2 – mailbox full

Nature du problème

Problème généralement temporaire.

Recommandation
- Retry progressif
- Mise en quarantaine si répétition
- Éviter suppression immédiate

Technique / transport (temporaire)

Codes typiques

4.4.x – routing
4.5.x – too many connections

Nature du problème

Problème réseau, DNS, surcharge ou configuration.

Recommandation

- Retry avec backoff
- Monitoring renforcé
- Investigation si hausse brutale

Réputation / anti-spam / policy (la zone "délivrabilité")

Codes typiques

4.7.x
5.7.x

Messages associés

- blocked
- rate limited
- policy
- spam detected

Nature du problème

Signal réputationnel ou filtrage anti-spam.

Impact

- Blocage IP ou domaine
- Dégradation de la délivrabilité globale

Recommandation

- Réduction immédiate de la pression
- Ciblage des segments engagés
- Vérification SPF / DKIM / DMARC
- Escalade vers postmaster si nécessaire

D. Exemples "officiels" par mailbox provider

Gmail / Google

Documentation officielle :

- *https://support.google.com/mail/answer/3726730*
- *https://postmaster.google.com/*

Codes fréquents :

421 4.7.0
550 5.7.x

Yahoo / AOL (Yahoo Sender Hub)

Documentation officielle :

- *https://senders.yahooinc.com/smtp-error-codes/*

Exemple :

421 4.7.0 [TSS04]

Orange / Wanadoo

Documentation officielle :
- *https://postmaster.orange.fr/*

Codes spécifiques :
OFR_

Microsoft (Outlook.com / Exchange Online / EOP)

Documentation officielle :
- *https://learn.microsoft.com/en-us/troubleshoot/exchange/email-delivery/ndr/fix-error-code-550-5-7-1-in-exchange-online*
- *https://sender.office.com/*

Codes fréquents :
550 5.7.1
550 5.7.511

Partie 3

Mise en place de règles automatiques (réellement actionnables)

A. Principe : moteur de décision en 3 étages

- Étape 1 : Classe principale (2 / 4 / 5)
- Étape 2 : Famille fonctionnelle (Y)
- Étape 3 : Motif opérateur (texte, tag interne)

Objectif :
Limiter les erreurs d'interprétation et homogénéiser les traitements.

B. Politique de retry recommandée (générique)

- Retry 1 : + 10 min
- Retry 2 : + 30 min
- Retry 3 : + 2 h
- Retry 4 : + 6 h
- Retry 5 : + 12 h

Expiration : 48-72 h

Recommandation : backoff exponentiel.

C. Table "règles types" (modèle)

- 5.1.1 → suppression
- 4.2.2 → retry + hold si répétitif
- 4.4.x → retry + monitoring
- 4.7.x → throttling
- 5.7.x → arrêt + remédiation

D. "Réactivité délivrabilité" : quoi monitorer

- Taux 4.7.x par domaine
- Taux 5.7.x
- Part 5.1.1
- Latence moyenne
- Plaintes

Définir des seuils d'alerte.

Partie 4
Communication de crise

Ce chapitre a pour objectif d'accompagner les e-routeurs dans la détection, la qualification et la résolution des problèmes de délivrabilité. Chaque situation est décrite avec ses signaux d'alerte et les actions correctives associées.

A. Identification et mesure de l'ampleur

L'identification d'un problème de délivrabilité passe avant tout par une baisse de performance dans vos diffusions email, soit au niveau du taux de livraison/succès, soit au niveau du taux d'ouverture. Ces deux cas sont à bien distinguer.

Important : il est fréquent qu'une baisse soit observée sur un opérateur de messagerie en particulier (ex : Microsoft) et non sur les autres. Il est donc essentiel de monitorer la délivrabilité au niveau opérateur de messagerie et pas seulement au global. Dans le cas contraire, des problématiques importantes pourraient rester cachées.

BAISSE DU TAUX DE LIVRAISON / SUCCÈS

Afin d'avoir une valeur fiable, il convient de mesurer ce taux au moins 3 h après le démarrage de la diffusion (voire plus si la vitesse d'envoi de la plateforme est faible ou si la diffusion est vraiment massive).

À NOTER
il peut être intéressant de mesurer ce taux à h+1, h+2, etc., pour détecter les problèmes de throttling. Un opérateur de messagerie peut en effet retarder la livraison d'emails s'il considère qu'il doit les analyser plus finement avant de prendre une décision sur la livraison, le rejet ou la remise en spam de ces emails.

Si une baisse du taux de livraison/succès est observée, il convient d'essayer de comprendre la raison des échecs d'envoi :

- **Si ces échecs sont essentiellement dus à des boites inexistantes, des domaines invalides ou des boites pleines** → ce n'est pas un problème de délivrabilité, c'est un problème de qualité de ciblage.
- **Si ces échecs sont des emails refusés, rejetés, inaccessibles** → c'est beaucoup plus problématique. Il est essentiel d'en comprendre la cause en consultant les logs d'envoi et les messages de **bounce** renvoyés par les opérateurs de messagerie.

BAISSE DU TAUX D'OUVERTURE

Sans entrer dans le détail, le taux d'ouverture est une donnée de moins en moins fiable. Cependant, en 2026, il reste tout de même une donnée essentielle pour monitorer sa délivrabilité.

Ce taux ne se mesure pas le jour même de l'envoi, mais à J+1, et à J+5 pour avoir un taux quasi finalisé.

Un taux d'ouverture considéré comme bon dépend du type d'email :
- **Emails transactionnels :** supérieur à 50 %
- **Emails de masse :** supérieur à 25 %

Une baisse du taux d'ouverture qui soulève un problème, c'est un taux qui baisse brutalement de plus de 10 % et qui devient inférieur à 20 % pour une cible BtoC, ou inférieur à 5 % pour une cible BtoB.

Cela signifie généralement que la majorité de vos emails a été délivrée dans les **courriers indésirables.** Les causes identifiables sont identiques à celles des emails rejetés (voir section B ci-dessous).

Les éléments qui impactent le plus fortement le taux d'ouverture sont :
- **La qualité du ciblage** : si vous ciblez des abonnés inactifs, le taux sera très faible.
- **Le libellé de l'expéditeur :** l'abonné doit comprendre qui vous êtes du premier coup d'œil.
- **L'objet de l'email :** il doit respecter les bonnes pratiques tout en intéressant l'internaute.

B. Problèmes identifiés et résolutions associées

Un problème de délivrabilité a été détecté et son ampleur a été mesurée. Les tableaux ci-dessous associent chaque problème type à ses actions correctives.

Deux cas sont à distinguer avant tout

- **Cas 1 : Le problème est apparu sur une diffusion, puis tout est revenu à la normale.**
  Dans la majorité des cas, le problème vient du contenu de la diffusion : objet non conforme, contenu déjà envoyé par le passé avec de mauvais résultats, ou volume exceptionnellement élevé. Si la fréquence d'envoi est faible, des restrictions temporaires peuvent avoir été appliquées, puis levées automatiquement.

- **Cas 2 : Le problème est récurrent sur toutes les diffusions.**
  Le problème est plus sérieux et ne se résoudra pas sans action de votre part. Les neuf situations décrites ci-dessous correspondent à ce cas de figure.

1. Emails non conformes techniquement

PROBLÈME DÉTECTÉ	RÉSOLUTION RECOMMANDÉE
Les messages de bounce renvoyés par les opérateurs de messagerie signalent un problème de configuration technique. Les outils de monitoring de Gmail permettent également d'identifier ces erreurs. ***Nota :*** *si seulement quelques bounces pointent un problème de configuration sur des domaines peu connus, le problème vient probablement du système du destinataire, pas du vôtre.*	Vérifiez les exigences techniques suivantes : • Le reverse-DNS doit être fonctionnel sur vos IPs d'envoi. Le FQDN doit correspondre à un site web. • Vos IPs d'envoi doivent être référencées dans l'enregistrement SPF (DNS). • Vos emails doivent être signés avec DKIM (clé publique présente dans le DNS). • Un enregistrement DMARC doit être présent dans le DNS du domaine ou sous-domaine d'envoi. • Vos emails doivent contenir une entête SMTP list-unsubscribe au format One-click.

2. Absence de réputation

PROBLÈME DÉTECTÉ	RÉSOLUTION RECOMMANDÉE
Toute nouvelle IP d'envoi ou tout nouveau domaine/sous-domaine expéditeur doit acquérir une bonne réputation avant de pouvoir envoyer des milliers d'emails sans problème. Les opérateurs de messagerie ne vous laisseront pas envoyer de grands volumes sans avoir l'assurance de vos bonnes intentions. ***Attention :*** *si vous n'envoyez pas de trafic pendant plus d'1 mois, votre réputation redeviendra caduque.*	Mettez en place un plan de chauffe : envoyez du bon trafic email en petite quantité, puis augmentez les volumes progressivement pour gagner la confiance des opérateurs. ***Nota :*** *Si vous êtes novice sur le sujet, faites-vous accompagné par un consultant délivrabilité.*

3. Mauvaise réputation

PROBLÈME DÉTECTÉ	RÉSOLUTION RECOMMANDÉE
Si votre réputation est mauvaise, c'est que vous ne suivez pas les bonnes pratiques de l'emailing. Vous ne pouvez envoyer que de petites quantités d'emails ; le reste est rejeté ou délivré en spam. La réputation correspond à l'image qu'a l'opérateur de messagerie de votre trafic email (elle varie d'un opérateur à l'autre). Elle se base sur votre historique d'envoi récent et prend en compte : la configuration technique, les plaintes utilisateurs, l'inactivité, le taux d'échecs d'envoi, les spamtraps touchées, etc.	Vérifiez : • La configuration technique. • Que les plaintes utilisateurs ne sont pas trop nombreuses, • Que vos ciblages ne comprennent pas trop de contacts inactifs, • Que vous ne générez pas trop de hard-bounces • Que vous ne touchez pas trop de spamtraps Vos IPs/domaines d'envoi pourront être blacklistés par l'opérateur si les bonnes pratiques ne sont pas respectées. ***Nota :*** *Au besoin, faites-vous accompagné par un consultant délivrabilité.*

4. Trop de plaintes générées

PROBLÈME DÉTECTÉ	RÉSOLUTION RECOMMANDÉE
Une plainte est un utilisateur qui ouvre un email et clique sur le bouton spam. Les plaintes sont particulièrement nuisibles et souvent à l'origine d'un blocage. Vous pouvez suivre cet indicateur via les outils de monitoring des opérateurs de messagerie (voir section II).	Ne dépassez pas le seuil de 0,3 % de plaintes. Soignez votre ciblage, privilégiez la qualité à la quantité. Quelques pistes d'investigation : • Ciblages trop larges ? Restreignez aux abonnés les plus actifs (= dernière ouverture d'email récente). N'envoyez jamais de campagnes massives sur des abonnés inactifs. • Désabonnement difficile ? Vérifiez que le lien est visible, le process simple (1 clic), et que la désinscription est bien prise en compte dans les ciblages. • Fréquence d'envoi trop élevée ? Réduisez-la. • Contenu déceptif ? Vérifiez l'appétence de vos cibles et évitez la redondance.

5. Trop de hard bounces générés

PROBLÈME DÉTECTÉ	RÉSOLUTION RECOMMANDÉE
Les opérateurs de messagerie autorisent un certain taux d'adresses incorrectes/ inexistantes. Si le taux de hard-bounce est trop important, l'opérateur peut décider de bloquer le reste de la diffusion. Ce taux seuil varie selon l'opérateur ; c'est une mesure de protection automatique.	Si la qualité de votre base est mauvaise, faites appel à un partenaire spécialisé dans le nettoyage de base de contacts. Ne ciblez pas de contacts non sollicités depuis plus de 12 mois. Si ces bounces correspondent à des adresses récemment acquises : • Vérifiez que vos formulaires d'abonnement sont sécurisés (captcha, etc.) — Une faille de sécurité est peut-être en cause. • Si les adresses proviennent d'une source externe (partenaire commercial), exigez des gages de qualité.

6. IPs ou domaines référencés sur des blocklistes

PROBLÈME DÉTECTÉ	RÉSOLUTION RECOMMANDÉE
Vous aurez généralement cette information en consultant les messages de bounce ou les sites internet dédiés aux blocklistes. Il existe de nombreuses blocklistes sur le marché : certaines sont anecdotiques, d'autres très suivies par les opérateurs de messagerie (et impacteront vos envois). Chaque blockliste fonctionne différemment : ciblage d'adresses incorrectes, spamtraps, trop de plaintes, etc. **SpamHaus est l'une des plus importantes ; si vous y êtes listés, votre taux de délivrabilité sera catastrophique.**	C'est avant tout un problème de qualité de la base de contacts. Soignez vos ciblages et vérifiez que l'origine du problème ne correspond pas à l'ajout de nouveaux contacts non vérifiés. Pour certaines blocklistes, une demande de délistage est possible. Pour d'autres, le délistage est automatique après une période sans trafic néfaste. ***Nota :*** *toutes les blocklistes ne sont pas nuisibles, certaines ne sont pas prises en compte par les opérateurs. Si vos statistiques ne baissent pas, ne vous en inquiétez pas outre mesure, mais gardez à l'esprit que cela révèle un problème de qualité de données.* **Attention :** si vos IPs sont mutualisées, vous pourriez subir les conséquences des mauvaises pratiques d'autres entités. Contactez le support de votre plateforme emailing.

7. Emails trop similaires à du spam

PROBLÈME DÉTECTÉ	RÉSOLUTION RECOMMANDÉE
Même si vos emails sont légitimes, s'ils sont trop similaires à des emails de spam, vous risquez d'être pris dans les mailles des solutions antispam. Cela peut venir du code HTML, de liens vers des sites de mauvaise réputation, d'un contenu trop disparate, ou d'un objet qui ne respecte pas les bonnes pratiques. **Attention :** une diffusion peut être considérée comme du spam si elle a déjà été envoyée par le passé avec de mauvais résultats (plaintes, nombreuses adresses incorrectes, faible taux d'ouverture). Les opérateurs n'aiment pas la redondance — chaque diffusion doit apporter de nouvelles informations.	Changez de template email et soignez le code HTML. Pour les cibles BtoC avec bonne réputation, il n'y a pas de précaution particulière à prendre sur le contenu, mais l'objet reste très sensible : certains caractères spéciaux ou mots peuvent amener les opérateurs à bloquer temporairement vos emails. Pour les cibles BtoB, le filtrage sur contenu est toujours très présent. Faites attention au wording, même dans le corps de l'email. ***Nota :*** *Si besoin, faites-vous accompagné par un intégrateur expérimenté et/ou un consultant délivrabilité.*

8. Emails sans valeur ajoutée pour les abonnés

PROBLÈME DÉTECTÉ	RÉSOLUTION RECOMMANDÉE
Plaintes, taux d'ouverture < 10 %, suppressions avant lecture, actions de l'internaute pour bloquer l'expéditeur... tout cela traduit le fait que vos emails encombrent les boites email. L'engagement de vos abonnés est trop faible et la valeur ajoutée n'est pas au rendez-vous.	Faites-vous accompagner par une agence CRM pour repenser toute votre communication digitale.

9. Ciblage d'adresses BtoB (entreprises, universités, associations)

PROBLÈME DÉTECTÉ	RÉSOLUTION RECOMMANDÉE
Toute entité non publique gère son parc d'adresses email comme elle le souhaite et applique ses propres règles de sécurité. Il est très fréquent qu'une entreprise ou une université n'autorise pas les emails commerciaux. Vos emails seront donc systématiquement rejetés, même si l'utilisateur final a donné son consentement.	Si l'organisation cible n'autorise pas les emails commerciaux, la seule option est de la contacter directement pour plaider votre cause. Il peut arriver que le message de bounce vous invite à confirmer l'envoi en vous rendant sur une URL particulière. C'est une mesure de protection pour filtrer les emails de masse. Une validation manuelle peut délivrer cet email spécifique, voire vous faire whitelister pour l'avenir. À vous de juger si le jeu en vaut la chandelle.

Note spécifique : Marchés Asie, Europe de l'Est et Russie
Ces marchés ont des exigences beaucoup plus contraignantes et spécifiques à chaque pays. Faites appel à des spécialistes de la délivrabilité pour les aborder.

C. Médiation avec les opérateurs de messagerie

Une fois que vous avez :
- identifié un problème de délivrabilité, sa nature et son ampleur,
- identifié le ou les opérateurs de messagerie pour lesquels les statistiques sont mauvaises,
- mené une analyse pour comprendre quand le problème a commencé et essayé d'en déterminer la cause,

Si vous ne comprenez pas la cause ou si la résolution nécessite l'intervention de l'opérateur de messagerie, vous pouvez le contacter directement.

Informations à préparer avant de contacter un opérateur

Les éléments généralement demandés sont :
- Le domaine expéditeur des emails
- Les IPs d'envoi (IP publiques)
- La date d'apparition du problème
- La nature du problème (rejets définitifs ou temporaires, filtrage…)
- Le message de bounce reçu

Dans certains cas, l'opérateur de messagerie pourra vous demander de renvoyer l'email qui a posé problème sur une boite technique particulière afin de mener une investigation.

Règles d'or pour la médiation

Soyez honnêtes ! Si vous avez commis une erreur, dites-le. Et surtout, expliquez ce que vous avez mis en place pour que cela ne se reproduise pas.

Soyez respectueux ! Ce sont les opérateurs de messagerie qui font la loi, pas vous. Vous devez vous plier à leurs règles.

Soyez patients ! Certains problèmes se règlent en quelques heures, d'autres en plusieurs jours, voire plusieurs semaines, avec beaucoup d'échanges de courriels.

Partie 5

Autres bonnes pratiques

A. Authentification

L'authentification des emails est un **ensemble de mécanismes techniques conçus pour vérifier l'identité de l'expéditeur d'un email et prévenir les abus**, comme le spoofing (usurpation d'identité), le phishing et le spam. Elle repose principalement sur **trois protocoles complémentaires** : SPF, DKIM et DMARC. Ces protocoles aident les serveurs de réception à déterminer si un email provient bien du domaine prétendu, améliorant ainsi la sécurité et accessoirement la délivrabilité.

En 2025, l'adoption de ces protocoles est devenue **quasi obligatoire** pour les expéditeurs de masse (bulk senders), en raison des exigences renforcées par les grands opérateurs de messagerie comme **Google** (Gmail), **Yahoo**, **Microsoft** (Outlook/Hotmail) et **Apple**. Avec Gmail, par exemple, pour envoyer plus de 5 000 emails par jour, il est requis d'implémenter SPF, DKIM et DMARC avec une politique au moins à « none » pour DMARC, et souvent plus stricte pour éviter certains rejets : *Email sender guidelines - Google Workspace Admin Help*.

SPF (SENDER POLICY FRAMEWORK)

Description

SPF est un **protocole qui permet au propriétaire d'un domaine de spécifier quelles adresses IP sont autorisées à envoyer des emails au nom de ce domaine**. Il fonctionne en vérifiant l'adresse IP de l'expéditeur par rapport à une liste publiée dans les enregistrements DNS du domaine. SPF protège contre le spoofing en empêchant les expéditeurs non autorisés d'utiliser votre domaine dans l'enveloppe SMTP (le « MAIL FROM » ou « Return-Path »).

Aide à l'Implémentation

1. Évaluez vos expéditeurs

Listez tous les serveurs ou services qui envoient des emails pour votre domaine (ex. : votre serveur SMTP, ESP comme Mailchimp, Google Workspace).

2. Créez l'enregistrement DNS TXT

▶ Syntaxe de base : v=spf1 [mécanismes] [qualificateurs] all

▶ Mécanismes courants :
- "ip4:adresse" ou "ip6:adresse" : Autorise une IP spécifique.
- "a" : Autorise les IPs des enregistrements A/AAAA du domaine.
- "mx" : Autorise les adresses IP des serveurs MX du domaine.
- "include:domaine" : Inclut la politique SPF d'un autre domaine (ex. pour un e-routeur donné).

▶ Qualificateurs :
- **- (Fail) :** Si l'adresse IP n'est pas listée, l'email est considéré comme non autorisé. Cela déclenche un échec SPF, et le serveur de réception peut rejeter l'email ou le marquer comme spam. C'est le qualificateur le plus strict, conseillé donc.

- **~ (SoftFail) :** Si l'adresse n'est pas listée, l'email est suspect, mais pas explicitement rejeté. Le serveur de réception peut l'accepter, mais avec une pénalité potentielle. Il est uniquement conseillé pendant une phase de test ou pour des scénarios où des transferts pourraient altérer l'IP sans être malveillants.

▶ **Exemple :** v=spf1 ip4:192.0.2.0/24 include:_spf.google.com -all

3. Publiez dans le DNS

Ajoutez l'enregistrement TXT pour votre domaine en suivant les recommandations de votre registrar (ex. GoDaddy, OVH, ...).

4. Testez

Utilisez des outils comme MX Toolbox pour vérifier. Envoyez un email test et vérifiez les entêtes du message reçu (headers) et recherchez une mention de type « Received-SPF: pass ».

Pour une implémentation avancée, si vous utilisez plusieurs e-routeurs, limitez les includes à 10 (limite SPF pour éviter les lookups excessifs).

Bonnes pratiques

▶ N'autorisez que les IPs nécessaires pour éviter les failles.
▶ Utilisez -all pour rejeter les adresses IP non-autorisées
▶ Surveillez les lookups DNS. SPF permet au maximum 10 lookups, au-delà, le serveur de réception peut retourner un « PermError » et avoir une incidence sur DMARC.
▶ Mettez à jour au moindre changement, notamment dans le cas d'un changement de e-routeur.

DKIM (DOMAINKEYS IDENTIFIED MAIL)

Description

DKIM **ajoute une signature cryptographique à l'email**, vérifiant que le contenu n'a pas été altéré en transit et provient bien du domaine. Il utilise une paire de clés : privée (pour signer sur le serveur expéditeur) et publique (publiée dans les DNS). La signature est placée dans un header « DKIM-Signature ».

DKIM **protège le corps et certains headers de l'email.** Les résultats sont Pass (signature valide), Fail (invalide), ou None (pas de signature). Il est plus robuste que SPF, car il survit au transfert du message.

Aide à l'Implémentation

Générez les clés

Utilisez OpenSSL pour créer une paire RSA (recommandé 2048 bits)

openssl genrsa -out private.key 2048

puis

openssl rsa -in private.key -pubout -out public.key

Configurez le serveur

En général votre e-routeur se charge de **générer et d'intégrer votre clé privée** pour signer les emails sortants. Pour Google Workspace ou Microsoft 365, activez DKIM dans les paramètres administreur.

Publiez l'enregistrement DNS TXT

[Sélecteur]._domainkey.[Domaine] TXT «v=DKIM1; k=rsa; p=[Clé publique].
Le sélecteur est un **nom arbitraire** (ex. «default») pour permettre à plusieurs clés de coexister sur un même domaine.

- **Exemple :** s1._domainkey.example.com TXT «v=DKIM1; k=rsa;p=MIGfMA0GCSqGSI...»

Testez

Envoyez un email et vérifiez les headers avec des outils comme dkimvalidator.com.

Bonnes pratiques

- Préférez un chiffrement en 2048 bits au lieu de 1024 bits.
- Opérez une rotation des clés, à minima sur une fréquence annuelle, surtout si la clé RSA est en 1024 bits.
- Signez les entêtes essentiels (« From », « To », « Subject », ...)
- Utilisez plusieurs sélecteurs, notamment celui du e-routeur si vous en utilisez un.

DMARC (DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING, AND CONFORMANCE)

Description

DMARC est un protocole qui s'appuie sur SPF et DKIM pour définir une politique de traitement des emails non authentifiés. Il publie une politique DNS indiquant quoi faire si SPF/DKIM échoue : **none** (surveiller), **quarantine** (spam), ou **reject** (rejeter). DMARC fournit aussi des rapports (aggregate et forensic) pour monitorer les abus.

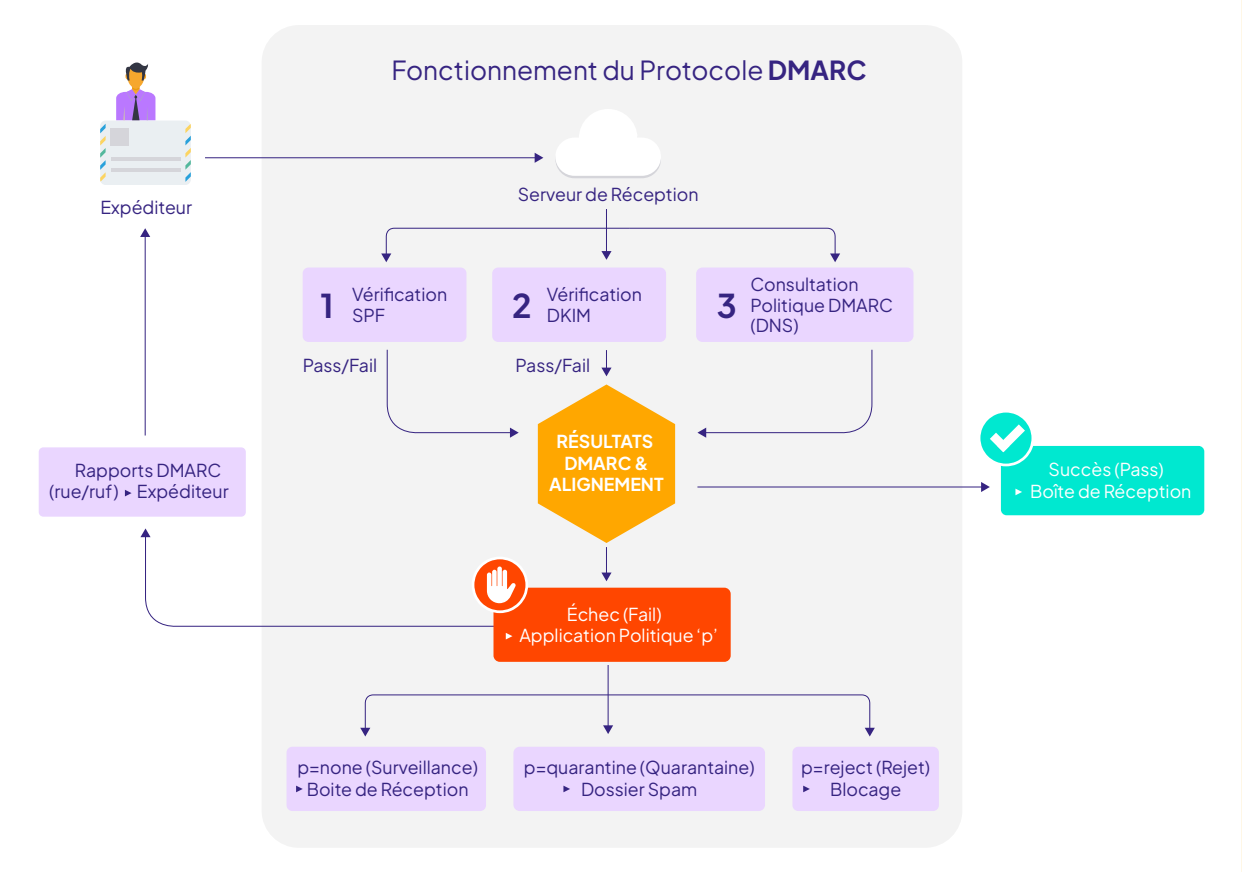
La clé de DMARC est l'**alignement** : Il vérifie si le domaine dans le header « From » (visible par l'utilisateur) correspond au domaine authentifié par SPF ou DKIM.

Alignement SPF

Le domaine du « Return-Path » doit correspondre ou être un sous-domaine du « From » (strict) ou partager l'organisation (relaxed).

Alignement DKIM

Le domaine dans la signature DKIM (d=) doit correspondre avec le « From » de la même manière. DMARC est **validé si au moins un des deux** (SPF ou DKIM) **est aligné et passe**. Sans alignement, même un SPF/DKIM validé peut faire échouer DMARC.



Aide à l'Implémentation

Vérifiez SPF et DKIM

Avant de déployer DMARC, assurez-vous que SPF et DKIM sont correctement configurés et stables. DMARC s'appuie sur leur réussite.

Définissez votre politique

DMARC utilise une balise «p» pour dicter l'action à entreprendre en cas d'échec :

- **p=none :**
  Aucune action (mode surveillance). Le serveur accepte l'email, mais vous envoie un rapport. C'est le point de départ obligatoire.
- **p=quarantine :**
  Les emails non conformes sont envoyés dans le dossier Spam/Indésirables.
- **p=reject :**
  Les emails non conformes sont purement et simplement bloqués. C'est l'objectif final pour une sécurité maximale.

Créez l'enregistrement DNS TXT

- **Hôte/Nom :**
  _dmarc (ou _dmarc.exemple.com)
- **Syntaxe de base :**
  v=DMARC1; p=none; rua=mailto:dmarc@exemple.com

▶ **Balises courantes :**

- **rua :** Adresse email pour recevoir les rapports agrégés (essentiel pour le monitoring).
- **ruf :** Adresse pour les rapports forensiques (détails techniques des échecs, moins supportés par les FAI).
- **adkim / aspf :** Mode d'alignement (r pour relaxé, s pour strict).

Bonnes pratiques

Adoptez une approche graduelle

Ne commencez jamais directement en p=reject. Commencez par p=none pendant 2 à 4 semaines pour auditer vos flux. Passez ensuite à p=quarantine, puis enfin à p=reject une fois certain qu'aucun email légitime n'est bloqué.

Surveillez l'alignement

DMARC exige que le domaine du « From » (visible par l'utilisateur) corresponde au domaine validé par DKIM ou SPF. C'est ce qu'on appelle l'alignement des identifiants.

Utilisez une adresse dédiée pour les rapports

Ne mettez pas votre adresse personnelle dans la balise rua, vous serez inondé d'emails automatiques. Créez une adresse spécifique (exemple : admin-dmarc@...) ou utilisez celle fournie par votre outil d'analyse DMARC.

BIMI (BRAND INDICATORS FOR MESSAGE IDENTIFICATION)

Description

BIMI est **la « récompense » visuelle d'une authentification rigoureuse**. C'est un standard émergent qui permet d'afficher le logo officiel de votre marque directement dans la boite de réception du destinataire, à côté de l'objet du message (au lieu de l'icône générique ou des initiales). Au-delà de l'aspect esthétique, **BIMI renforce la confiance** : pour l'afficher, les messageries (comme Gmail ou Apple Mail) exigent que le domaine soit parfaitement sécurisé *via* DMARC. C'est un puissant levier de taux d'ouverture et de notoriété de marque.

Aide à l'implémentation

L'implémentation de BIMI est plus stricte que les autres protocoles :

Exigence DMARC stricte

Vous devez impérativement avoir une politique DMARC configurée à p=quarantine (avec un pourcentage pct=100) ou p=reject. Le mode p=none ne suffit pas.

Préparez votre Logo (SVG Tiny PS)

Le logo ne peut pas être un simple fichier JPG ou PNG. Il doit être au format vectoriel spécifique SVG Tiny Portable/Secure. Il doit être carré, centré et sur fond uni.

Obtenez un certificat VMC (Verified Mark Certificate)

C'est l'étape souvent payante et complexe. Pour que Gmail ou Apple affichent le logo, vous devez prouver que vous possédez la marque (dépôt INPI/EUIPO) *via* un certificat VMC délivré par une autorité de certification (comme DigiCert ou Entrust).

Publiez l'enregistrement DNS TXT

- **Hôte/Nom :** default._bimi
- **Syntaxe :**
  v=BIMI1; l=https://exemple.com/logo.svg ;
  a=https://exemple.com/certificat.pem ;
- **L'attribut l=** pointe vers votre fichier SVG hébergé.
- **L'attribut a=** pointe vers votre certificat VMC (obligatoire pour la plupart des grands opérateurs).

Bonnes pratiques

Validez votre SVG

Utilisez des outils de validation BIMI officiels pour vous assurer que votre fichier SVG respecte le profil « Tiny PS », sinon il ne s'affichera pas.

Pensez au « Dark Mode »

Testez le rendu de votre logo sur des fonds sombres et clairs. Les messageries peuvent adapter l'interface, et votre logo doit rester lisible.

C'est un investissement marketing

Considérez le coût du certificat VMC non pas comme une dépense technique, mais comme un budget marketing pour augmenter la visibilité de votre marque dans des boites de réception saturées.

B. Gestion de la donnée personnelle email

LA COLLECTE

La collecte est la **fondation de votre délivrabilité**. C'est à cette étape que vous définissez la qualité future de votre base et votre niveau de protection juridique. En e-marketing, le consentement doit être « **libre, spécifique, éclairé et univoque** ».

Il existe trois niveaux de collecte, offrant des degrés de sécurité très différents :

Opt-in Simple

L'utilisateur entre son email et valide. C'est la méthode la plus fluide (meilleur taux de conversion), mais la plus dangereuse (fautes de frappe, adresses inexistantes, «spam traps»).

Opt-in Certifié (Preuve de Saisie)

Il s'agit d'un opt-in simple enrichi. On enregistre techniquement les traces de l'inscription (Timestamp, adresse IP, URL source).

Nuance importante : Cela prouve uniquement qu'une inscription a eu lieu depuis une machine donnée à un instant T (prouvant votre bonne foi contre le « scraping » d'adresses). Cela ne garantit pas que c'est le propriétaire de l'adresse qui a fait la démarche.

Double Opt-in (DOI)

L'utilisateur s'inscrit, reçoit un email de confirmation, et doit cliquer sur un lien pour valider son inscription.

C'est le seul mécanisme qui apporte **la preuve du consentement du titulaire**. Si le lien est cliqué, cela prouve que la personne qui a rempli le formulaire a bien accès à la boite de réception.

Aide à l'Implémentation

Transparence du « Pacte »

Ne cherchez pas à piéger l'utilisateur. Au moment de l'inscription, soyez clair sur ce qu'implique le consentement :

- **Fréquence :** Indiquez le rythme (ex : « Une newsletter hebdomadaire »).
- **Contenu :** Précisez la nature des envois (ex : « Conseils marketing », « Offres partenaires », ...).
- **Exemple de mention** : « En cliquant sur "M'inscrire", vous acceptez de recevoir nos actualités chaque mardi. Vous pourrez vous désinscrire à tout moment via le lien intégré.»

Configuration du Double Opt-in

- **L'email de confirmation** ne doit contenir aucune promotion. Son seul but est la validation.
- **Objet conseillé :** « Action requise : [NOM], confirmez votre inscription à la Newsletter ».

Bonnes pratiques

Privilégiez le Double Opt-in (DOI) pour le B2C

Il vous protège contre les **inscriptions malveillantes** (mail bombing) où un tiers inscrit une victime à des centaines de newsletters. Avec le DOI, l'inscription n'est jamais finalisée sans le clic de validation.

Bannissez l'achat de bases

Les adresses achetées ou louées n'ont jamais donné leur consentement explicite pour votre marque. Elles génèrent **des taux de plainte élevés** et **ruinent votre réputation d'expéditeur**.

Documentez vos preuves

Stockez précieusement les logs (IP, Date, Source) et, si possible, le statut « Validé par DOI ». En cas de contrôle CNIL ou de plainte spam, ces éléments sont votre assurance vie.

L'EXPLOITATION ET L'HYGIÈNE DE BASE

Une base de données est une **matière vivante** qui se dégrade naturellement avec le temps. Maintenir une bonne hygiène consiste à **identifier les contacts inactifs**, mais surtout à **écouter et interpréter les signaux techniques** renvoyés par les serveurs de réception (les retours SMTP ou «bounces»). Ne pas traiter ces erreurs signale aux opérateurs de messagerie (Gmail, Yahoo, Microsoft) que vous ne gérez pas vos listes avec rigueur, ce qui dégrade directement votre réputation.

Aide à l'Implémentation

Mettez en place une politique de gestion des inactifs :

Définir l'inactivité

Par exemple, un abonné qui n'a ouvert aucun email depuis 6 mois (la durée varie selon votre fréquence d'envoi).

Scénario de réengagement

Avant de les exclure, tentez une dernière approche automatisée.
Email 1 : « Vous nous manquez » (Offre spéciale ou contenu exclusif).
Email 2 : « Dernière chance » (demandez explicitement s'ils veulent rester inscrits).

Mise en quarantaine / Exclusion

Si aucune réaction suite à la campagne de réengagement, l'adresse doit être exclue des envois marketing (supprimée de la liste active).

Adoptez une gestion granulaire des retours SMTP : Il est crucial de catégoriser les erreurs SMTP pour appliquer le bon traitement automatisé.

Les Erreurs Définitives (Hard Bounces)

- **Cause :**
  L'adresse email n'existe pas, n'existe plus, ou le nom de domaine est invalide (ex: erreur 5.1.1). La non-validité ne fait aucun doute.
- **Action :**
  L'adresse doit être **supprimée ou mise en quarantaine immédiatement** et automatiquement dès le premier retour. Continuer d'écrire à une adresse inexistante est un critère majeur de pénalisation.

Les Erreurs temporaires (Soft Bounces) & Boites Saturées

- **Cause :**
  Le serveur distant est indisponible, le message est trop lourd, ou la **boite de réception est pleine (Over Quota)**. Ce dernier point est devenu critique : les messageries comme Gmail (qui partage ses 15 Go gratuits avec Drive et Photos) et prochainement Yahoo réduisent ou limitent la capacité de stockage de leurs utilisateurs. Les erreurs pour «boite saturée» se multiplient.

▶ **Action :**
Une erreur temporaire ne doit pas entrainer une suppression immédiate. Cependant, vous devez configurer une règle de conversion : **si une adresse renvoie un statut «boite saturée» de manière consécutive sur une période donnée (ex: 3 campagnes successives sur 30 jours), elle doit être reclassée en «Hard Bounce» et exclue des envois**. Une boite qui reste pleine est très souvent une boite abandonnée qui finira par se transformer en «Spam Trap» (adresse piège).

Les Blocages de Réputation (Block Bounces)

▶ **Cause :**
L'email est rejeté non pas à cause du destinataire, mais à cause de vous. Le serveur de réception bloque le message, car votre adresse IP est sur une liste noire (blacklist), le contenu est identifié comme du spam, ou un filtre anti-spam a été déclenché (erreurs de type 5.7.1).

▶ **Action :**
Ces retours nécessitent une **lecture humaine et une investigation immédiate**. Mettez en pause vos envois vers le domaine concerné, vérifiez la configuration de vos protocoles (SPF, DKIM, DMARC), contrôlez vos IP sur des outils comme MXToolbox, et révisez le contenu de votre message.

Bonnes pratiques

Automatisez les règles de traitement

Votre outil de routage (ESP) doit être capable d'appliquer ces règles (suppression immédiate pour les hard bounces, compteur pour les soft bounces) sans intervention manuelle.

LA SUPPRESSION

Conformément au principe de « limitation de la conservation » imposé par le RGPD, vous ne pouvez pas conserver indéfiniment des données personnelles sans justification. Au-delà de l'obligation légale, s'accrocher à des données obsolètes est une erreur stratégique. Une adresse email inutilisée depuis des années n'a plus aucune valeur commerciale ; elle constitue au contraire un risque de sécurité (fuite de données) et un véritable danger pour votre délivrabilité (transformation potentielle en « Spam Trap » par les FAI).

Aide à l'Implémentation

Il est vital de faire la distinction entre ce que la loi vous autorise à faire et ce qu'il est judicieux de faire pour votre réputation d'expéditeur.

Le cadre légal (Le plafond)

La CNIL recommande de conserver les données de prospection pendant une durée maximale **de trois (3) ans** à compter du dernier contact émanant de la personne (ex : un clic dans un email, un achat, une connexion au compte). Passé ce délai, la suppression ou l'anonymisation est obligatoire.

Le bon sens marketing (La réalité du terrain)

N'exploitez pas ce cadre légal jusqu'au bout ! Le fait d'avoir le droit de conserver un contact inactif pendant trois (3) ans ne signifie pas que vous devez continuer à lui envoyer des campagnes pendant tout ce temps.

- **Si un abonné n'a pas ouvert un seul de vos emails depuis 12 ou 18 mois,** continuer de le solliciter jusqu'à la limite des 3 ans va inexorablement dégrader votre réputation auprès de Gmail, Outlook ou Yahoo.
- **La règle d'or :** Le plafond légal dicte quand la donnée doit disparaitre de vos serveurs, mais vos règles d'engagement (Sunset Policy) doivent dicter bien plus tôt quand vous cessez de router des emails vers cette adresse.

Bonnes pratiques

Automatisez la purge

Configurez votre CRM ou votre outil d'emailing pour qu'il identifie et traite automatiquement les contacts ayant dépassé la date limite légale de conservation, sans action manuelle de votre part.

Choisissez entre suppression et anonymisation

- **Suppression physique :** L'email et les données associées sont totalement effacés.
- **Anonymisation :** Les données identifiantes (nom, email) sont remplacées par des identifiants aléatoires. Cela vous permet de conserver l'historique de vos statistiques (ex : « un utilisateur a généré X euros de CA en 2024 ») sans pouvoir identifier la personne physiquement.

Facilitez la sortie volontaire (List-Unsubscribe)

La meilleure suppression reste celle initiée par l'utilisateur avant qu'il ne se fâche. Assurez-vous que votre lien de désinscription est visible, fonctionne en un clic (sans mot de passe requis) et implémentez l'entête technique List-Unsubscribe. Ce dernier permet aux messageries d'afficher un bouton « Se désabonner » natif en haut de l'email, évitant ainsi que l'utilisateur ne clique sur le bouton « Signaler comme Spam » pour s'en débarrasser.

Annexes

A. Glossaire

Block

Refus lié à la politique ou la réputation.

Blockliste / Blackliste

Une blockliste (ou liste de blocage) est une base de données qui regroupe des adresses IP, des noms de domaine ou des adresses email identifiés comme sources de spam, de contenu malveillant ou d'envois non sollicités.

Les fournisseurs de messagerie et les services anti-spam utilisent ces listes pour filtrer ou bloquer les emails provenant de ces sources avant qu'ils n'atteignent la boite de réception.

Quelques exemples de blocklistes majeures : Spamhaus, Spamcop, Barracuda Reputation Blocklist (BRBL), SORBS...

Bounce (rebond)

Un message de bounce (ou rebond) est une notification générée automatiquement par le serveur de messagerie pour informer l'expéditeur qu'un email n'a pas pu être délivré à son destinataire.

Ce message contient généralement :

- La raison de l'échec (ex. adresse inexistante, boite pleine, blocage par le serveur).
- Un code d'erreur SMTP (ex. 550, 554, 421, ...).
- Des informations techniques sur le serveur qui a refusé le message.

Il existe trois types de bounces :

- Hard bounce (le code d'erreur commence en général par 5) :
- Échec permanent (ex. adresse email invalide ou domaine inexistant).
- Soft bounce (le code erreur commence en général par 4) : Échec temporaire (ex. boite pleine, problème de serveur, limite de quota).
- Block bounce (le code erreur peut commencer par 4 ou 5) : Refus d'acceptation du flux SMTP, souvent en raison d'un problème de réputation de l'entité émettrice.

Deferral

Refus temporaire nécessitant une nouvelle tentative d'envoi.

E-routeur (routeur d'emails)

Plateforme ou service spécialisé dans l'acheminement, l'envoi et la gestion d'emails en masse, particulièrement pour des campagnes marketing, transactionnelles ou newsletters, en optimisant la délivrabilité *via* des infrastructures dédiées (serveurs, IPs, authentification SPF/DKIM/DMARC, ...), des outils de segmentation et de conformité anti-spam. L'e-routeur peut agir comme intermédiaire entre l'expéditeur et les ISP/MSP pour améliorer les taux de livraison et éviter les filtres spam.

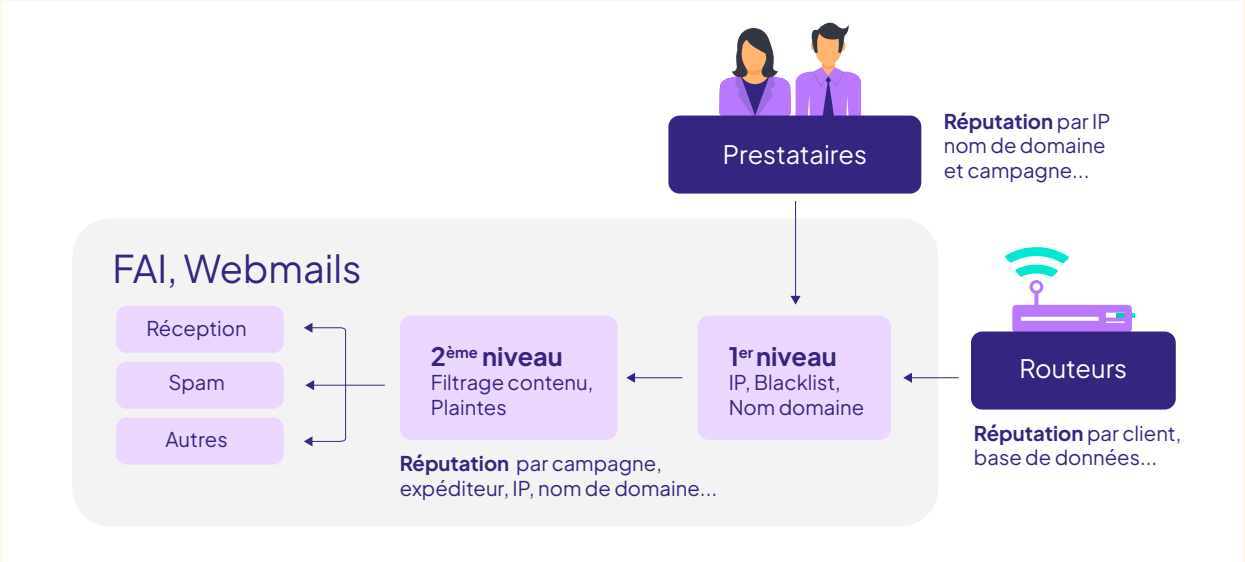
FAI (Fournisseur d'Accès à Internet)

Voir ISP

Hard bounce

Échec définitif lié à l'adresse.

Honey Pot (“Pot de miel”)	Adresses email fictives délibérément placées sur des sites web de manière cachée (par exemple, via du CSS invisible aux humains, mais accessible aux bots), afin de piéger les outils de scraping et d’identifier les expéditeurs qui collectent illégalement des adresses, indiquant une mauvaise qualité de liste.
ISP (Internet Service Provider ou Fournisseur d’Accès à Internet)	Entité qui fournit principalement un accès à Internet à des clients payants (comme Orange, SFR ou Bouygues), et qui inclut des services de messagerie électronique intégrés. Dans le contexte de l’email marketing, les ISP gèrent la délivrabilité des emails vers leurs abonnés, en veillant à un niveau de service élevé du fait des relations contractuelles et payantes avec les utilisateurs. Cela implique souvent une approche spécifique afin d’éviter de frustrer les clients.
MSP (Mailbox Service Provider, ou Fournisseur de Services de Messagerie)	Entité spécialisée dans la fourniture de boites de réception email, souvent gratuite (comme Gmail, Outlook.com ou Yahoo), sans nécessairement inclure un accès Internet. Dans l’email marketing, les MSP se concentrent sur la gestion massive d’emails pour des utilisateurs non payants, ce qui les rend plus vulnérables aux abus et les incite à adopter des filtres plus stricts pour maintenir la qualité du service.
Policy	Règle interne opérateur.
Rate limiting	Limitation dynamique du débit d’envoi.
Réputation	La notion de réputation permet de concrétiser un ensemble de données techniques (taux de plaintes, taux de bounces, taux de Spam Trap...) en un vocabulaire qui peut être compris facilement par notamment les utilisateurs de CRM et les marketeurs. On trouve des scores de réputation produits par : ▶ Les e-routeurs à partir de leurs données propres ; ▶ Les gestionnaires de boites aux lettres (webmail et FAI) ; ▶ Enfin, quelques plateformes tierces spécialisées existent, principalement senderscore de validity et talosintelligence de Cisco.



Soft bounce

Échec temporaire.

Spamtrap (adresse email piège)

Un spamtrap est une adresse email spécialement créée ou utilisée par les fournisseurs de messagerie, les organisations anti-spam ou les blocklistes pour identifier les expéditeurs qui envoient des emails non sollicités.

Ces adresses ne sont jamais utilisées par de véritables personnes et ne s'inscrivent à aucune liste volontairement. Si un expéditeur envoie un email à un spamtrap, cela indique généralement une mauvaise hygiène de base (adresses obsolètes ou achetées) ou une pratique non conforme (envoi à des bases non-opt-in).

Il existe trois types de spamtrap (par ordre de dangerosité décroissant) :

- Pristine : Créées par les organisations anti-spam et jamais utilisées par des humains. Elles se retrouvent dans des listes collectées illégalement ou par scraping. 1 seul email suffit pour que l'IP d'envoi soit blacklistée.
- Recycled : Anciennes adresses valides, abandonnées puis transformées en spamtrap par un fournisseur.
- Typo traps : Adresses avec fautes courantes (ex. gmial.com) pour détecter les erreurs ou les pratiques douteuses.

Throttling

Le throttling côté FAI désigne la pratique par laquelle le fournisseur de messagerie ralentit volontairement la réception des emails provenant d'un expéditeur, en imposant des limites de volume ou de cadence.

Vous recevrez des messages de bounce indiquant un rejet temporaire d'emails. Le message précise parfois quand vous pourrez retenter l'envoi.

À noter que la plupart des solutions d'envoi d'emails de masse réalisent de nouvelles tentatives automatiquement.

Le FAI applique généralement du throttling pour :

- Évaluer la réputation de l'expéditeur avant d'autoriser un flux plus important.
- Limiter les risques de spam ou d'attaques massives.
- Prévenir la surcharge de ses serveurs.

Webmail

Service de messagerie électronique intégré à un navigateur web, ne nécessitant pas l'installation d'un client de messagerie dédié. Il permet de lire, d'envoyer, de recevoir et de gérer des courriels depuis n'importe quel appareil connecté à Internet. Les webmails (comme Gmail, Outlook.com ou Yahoo Mail) sont couramment utilisés par les destinataires, influençant la délivrabilité des campagnes, le rendu des emails (compatibilité HTML/CSS) et les pratiques anti-spam, car ils intègrent souvent des filtres avancés et une analyse comportementale pour protéger les utilisateurs.

B. Liens de référence (officiels / normatifs)

- **RFC 5321 – SMTP**
  https://datatracker.ietf.org/doc/html/rfc5321

- **RFC 3463 – Enhanced Status Codes**
  https://datatracker.ietf.org/doc/html/rfc3463

- **IANA registry**
  https://www.iana.org/assignments/smtp-enhanced-status-codes

- **Google Postmaster**
  https://postmaster.google.com/

- **Yahoo Sender Hub**
  https://senders.yahooinc.com/

- **Microsoft Delist**
  https://sender.office.com/

- **Orange Postmaster**
  https://postmaster.orange.fr/

MERCI AUX PARTICIPANTS

Alliance Digitale
112ter rue Cardinet
75017 Paris
contact@alliancedigitale.org