ChatGPT

Guide anti-spam pour la prospection par email avec Google Workspace

Utiliser Google Workspace pour faire de la prospection à froid par email peut être très efficace, à condition de suivre des bonnes pratiques strictes pour éviter que vos messages ne finissent en spam. Ce guide couvre tous les aspects essentiels – de l'authentification de votre domaine jusqu'au monitoring – afin que vos emails arrivent bien en boîte de réception. Chaque section détaille des recommandations techniques et comportementales, avec des seuils précis et des distinctions lorsque vous opérez avec un seul compte ou plusieurs comptes sur un même domaine.

Authentification du domaine (SPF, DKIM, DMARC)

Pourquoi ? L'authentification de votre domaine d'envoi est la base d'une bonne délivrabilité. Gmail et les autres fournisseurs vérifient que vos emails sont légitimes via SPF, DKIM et DMARC. Google exige d'ailleurs que **tout expéditeur massif configure SPF et DKIM, et que les expéditeurs en volume configurent DMARC** [1] [2]. Sans ces enregistrements, vos emails auront bien plus de chances d'être marqués comme spam ou rejetés.

SPF (Sender Policy Framework) – Certifiez les serveurs autorisés à envoyer des emails pour votre domaine. Pour Google Workspace, cela consiste à créer un enregistrement DNS TXT du type :

```
v=spf1 include:_spf.google.com ~all
```

Ce `include:_spf.google.com` indique que les serveurs Gmail peuvent envoyer en votre nom [3] [4]. Si un enregistrement SPF existe déjà, ajoutez-y l'instruction `_spf.google.com` (et les autres services autorisés le cas échéant). Une fois le TXT SPF publié, attendez la propagation (quelques minutes à 24h) puis vérifiez que les emails de votre domaine affichent « **pass SPF** » dans les en-têtes Gmail.

DKIM (DomainKeys Identified Mail) – Associez une signature numérique à vos emails pour prouver qu'ils n'ont pas été altérés et qu'ils proviennent bien de votre domaine. Avec Google Workspace, activez DKIM en suivant ces étapes :

1. Accédez à la console d'administration Google Workspace (Admin Console) et ouvrez la section **Gmail > Authentifier les emails (Authentification DKIM)** [5].
2. Sélectionnez votre domaine et cliquez sur **Générer un enregistrement DKIM**. Google fournira une clé publique sous forme d'enregistrement TXT (par défaut sur un sélecteur `google._domainkey`).
3. Publiez cet enregistrement TXT DKIM dans la zone DNS de votre domaine (nom d'hôte correspondant et valeur fournie). Attendez ~1 heure que le DNS se propage [6].
4. Retournez dans l'Admin Console et cliquez sur **Commencer l'authentification**. Gmail signera alors automatiquement vos emails sortants. Une fois activé, vos emails afficheront une entrée « **signed-by: votredomaine.com** » dans les en-têtes, gage de confiance.

DMARC (Domain-based Message Authentication, Reporting and Conformance) – C'est le dernier pilier qui permet aux destinataires de décider du sort des emails non authentifiés et de vous envoyer des rapports. Configurez DMARC seulement **après** SPF et DKIM (laissez-les tourner 1–2 jours). Créez un enregistrement DNS TXT nommé `_dmarc.votredomaine.com` avec une valeur comme :

```
v=DMARC1; p=none; rua=mailto:postmaster@votredomaine.com; pct=100;
```

Ici `p=none` signifie qu'aucune mesure de rejet n'est prise (mode observation) – idéal pour débuter. Le tag `rua` envoie les rapports agrégés quotidiens à votre adresse (adaptez l'email). Vous pourrez plus tard passer en `p=quarantine` (spam) voire `p=reject` une fois sûr que SPF/DKIM sont bien configurés [7]. DMARC assure qu'un email de votre domaine **échoue** si ni SPF ni DKIM ne valident, ce qui protège contre l'usurpation. À terme, utiliser une politique stricte (p=quarantine/reject) renforcera votre réputation d'expéditeur en bloquant les abus, et les messages légitimes bien authentifiés auront plus de facilité à atteindre la boîte de réception [8] [9].

Compte unique vs. plusieurs comptes : L'authentification se gère au niveau du domaine – vous n'avez pas besoin de réglages distincts par compte utilisateur. Ainsi, un seul jeu d'enregistrements SPF/DKIM/DMARC couvre tous les comptes sur le domaine. **Assurez-vous simplement que chaque compte utilise l'adresse du domaine authentifié** (évitez par exemple d'envoyer depuis un alias non configuré). Si vous ajoutez un sous-domaine ou un domaine alias pour vos envois, pensez à configurer également SPF/DKIM/DMARC pour celui-ci. En résumé, la configuration est à faire une fois, mais **elle est indispensable** quel que soit le nombre de comptes : *les messages authentifiés ont bien moins de risque d'être marqués indésirables par Gmail* [10] [11].

Warm-up : montée en charge progressive

Pourquoi ? Un domaine ou un compte email sans historique d'envoi doit **faire ses preuves graduellement**. Envoyer brusquement de gros volumes depuis une nouvelle adresse est un signal d'alerte pour Gmail et les autres FAI. Le « warm-up » consiste à *chauffer* le domaine et la boîte mail en augmentant petit à petit le nombre d'envois, afin de bâtir une réputation positive.

Démarrage d'un nouveau domaine : Si votre domaine est tout neuf (enregistré il y a quelques jours), faites preuve de patience. Il est conseillé **d'attendre 24 à 48 heures avant d'envoyer le tout premier email**. En effet, certains systèmes anti-spam (ex: Spamhaus) peuvent bloquer automatiquement un domaine qui commence à émettre des mails massifs dès son enregistrement [12]. Profitez de ce laps de temps initial pour configurer correctement SPF/DKIM.

Les premiers envois – commencer très bas : Pour un domaine ou un compte « froid » sans historique, débutez avec un volume infime. Par exemple, **les 2–3 premiers jours, envoyez seulement 5 à 10 emails par jour** [13]. L'idée est d'**établir une activité d'envoi normal** (un individu qui envoie quelques emails personnels, non pas des dizaines de messages commerciaux d'un coup). Si possible, envoyez ces premiers emails à des contacts connus ou collaborateurs susceptibles d'ouvrir et répondre – ces interactions initiales aideront à crédibiliser votre adresse.

Augmentation graduelle : Après cette phase ultra-limitée, vous pouvez **doubler le volume tous les quelques jours environ** tant que tout se passe bien (aucun blocage ni taux d'ouverture anormalement bas). Une progression type pourrait être : 10 emails/jour la première semaine, ~20/jour la deuxième, ~40 la troisième, et ainsi de suite jusqu'au rythme cible [14] [15]. **Évitez absolument les sauts brusques** – par exemple ne passez pas de 20 à 100 d'un coup. Un étalement sur **2 à 4 semaines** est recommandé

pour atteindre des volumes modérés (~50–100/jour) sans alerter Gmail [13]. Rappelez-vous qu'**une augmentation progressive et régulière a l'air "naturelle"** aux yeux des filtres.

Simuler de l'engagement : Pendant la montée en charge, il est utile d'obtenir des signes positifs pour votre adresse. Si des collègues peuvent répondre à vos emails de test, faites-le – un échange aller-retour montre à Google que vos courriels intéressent le destinataire. Il existe aussi des outils de *warm-up automatisé* : ils envoient depuis votre compte des emails factices vers d'autres boîtes participants au programme, qui à leur tour ouvrent, répondent et marquent vos messages comme « non spam ». Ces interactions artificielles peuvent améliorer votre réputation initiale. C'est optionnel mais potentiellement bénéfique si vous partez de zéro absolu.

Ne pas brûler les étapes : Soyez attentif aux retours durant le warm-up. Surveillez votre taux de rebond (bounces) – un pic de mails invalides est mauvais signe, nettoyez vos listes avant d'augmenter l'envoi. Vérifiez si certains messages atterrissent en spam (par des tests vers vos propres adresses). Tant que tout est vert, continuez l'augmentation graduelle. En cas de problème (ex. Gmail qui bloque temporairement l'envoi), **stoppez la montée** et réduisez le volume le temps de rétablir la situation.

Compte unique vs. plusieurs comptes : Avec **plusieurs comptes sur un même domaine**, il faut *réchauffer chaque adresse email individuellement*. Ne créez pas 5 nouvelles boîtes et n'envoyez pas 50 mails par jour avec chacune dès la première semaine – ce serait équivalent à envoyer 250 mails/jour sur le domaine, ce qui est beaucoup trop sans historique. Si vous avez, par exemple, deux nouvelles adresses sur le domaine, vous pouvez répartir le warm-up en alternant ou en les faisant monter en parallèle **mais en divisant les volumes** : par ex. 5 emails/jour sur chaque adresse la première semaine (total domaine ~10/jour), puis 10 chacune la deuxième (total ~20/jour), etc. L'important est que le **volume cumulé du domaine** reste cohérent avec une progression naturelle. De plus, assurez-vous que *chaque compte obtienne aussi de l'engagement* (ouverture, réponses) durant son warm-up – l'effort de chauffe doit être fait pour chaque boîte. En pratique, il peut être judicieux de **décaler les ramp-ups** (ex: commencer à envoyer avec la 2e adresse une fois que la 1e est déjà un peu établie) afin de ne pas cumuler une charge trop forte sur le domaine d'un coup.

Contenu des emails (bonnes pratiques)

La qualité et la présentation de vos emails de prospection influencent fortement leur sort. Voici comment **rédiger et structurer vos messages** pour minimiser les risques de spam :

- **Personnalisation et pertinence :** Écrivez vos emails comme si vous contactiez une personne en direct. Utilisez le prénom du prospect, mentionnez éventuellement un contexte qui le concerne (par exemple une référence à son entreprise ou à une problématique spécifique). Un message générique copié-collé à des centaines d'exemplaires aura de faibles réponses et peut être signalé. Au contraire, un email qui semble **personnel et utile** a plus de chances d'être bien accueilli.

- **Objet et ton du message :** Choisissez un objet court, explicite et professionnel, sans mots racoleurs. Évitez les majuscules intégrales ou les points d'exclamation multiples dans le sujet (exemple à proscrire : **"OPPORTUNITÉ INCROYABLE!!!"**). Des termes typiquement utilisés par les spammeurs comme *« gratuit », « promotion », « gagnant », « argent »* sont à bannir autant que possible [16]. Préférez un **ton courtois et direct**, évitez les hyperboles commerciales. Le corps du mail doit rester **court et aéré** (quelques phrases ou un court paragraphe) : en prospection à froid, un long pavé décourage la lecture et peut sembler suspect.

- **Format texte/HTML :** Un email purement *image* ou avec un design HTML lourd a plus de risques de finir en spam. Préférez un format **texte brut ou HTML léger**, avec éventuellement votre signature visuelle mais pas plus. Si vous incluez une image (logo, visuel explicatif), assurez-vous qu'elle n'est pas trop lourde et accompagne un texte substantiel – le ratio texte/ image doit pencher largement en faveur du texte. De même, ne joignez pas de pièce jointe volumineuse à un email de prospection initial (si vous devez partager un PDF de présentation, faites-le plutôt après une réponse du prospect, ou via un lien). **Évitez les URL raccourcies** de type bit.ly : Gmail peut les considérer comme suspectes. Insérez des liens explicites, idéalement vers un site de domaine reconnu (votre site officiel). Évitez aussi d'avoir trop de liens dans un même message (un seul lien principal est un bon maximum). Enfin, soignez la version texte simple (*plain-text*) de votre email (si vous envoyez en HTML multipart) : beaucoup de clients mail et filtres anti-spam l'examinent.

- **Signature et crédibilité :** Incluez une **signature professionnelle** en bas de vos emails : nom, poste, entreprise, site web, voire numéro de téléphone. Cela montre que vous êtes une vraie personne avec une identité vérifiable. Dans un contexte B2B, indiquer les coordonnées de l'entreprise (adresse postale, SIRET…) n'est pas obligatoire pour de la prospection ponctuelle, mais c'est un plus pour la transparence. En tout cas, une signature complète inspire confiance et peut aussi passer les filtres (qui vérifient la présence d'éléments comme une adresse physique dans les newsletters marketing, par analogie).

- **Lien de désinscription (opt-out) : Proposez systématiquement une option de désinscription facile** dans vos emails de cold outreach. Par exemple, une courte phrase en bas du message du style : *« Si vous ne souhaitez plus recevoir de courriels de ma part, faites-le moi savoir ici »* avec un lien cliquable de désabonnement, ou à minima *« …répondez simplement "STOP" à ce mail. »*. Cette pratique est vivement conseillée pour éviter les signalements spam. En effet, si le destinataire a un moyen propre de se retirer, il utilisera moins le bouton *« Signaler comme indésirable »*. Google indique d'ailleurs que les campagnes doivent supporter le **unsubscribe en un clic** et afficher un lien clair de désinscription dans le message [17] [18]. Même pour des volumes modestes, c'est une *bonne pratique professionnelle*. *Astuce avancée :* utilisez l'en-tête **List-Unsubscribe** dans vos emails (votre outil d'envoi le fait peut-être déjà) pour que Gmail affiche un bouton de désabonnement natif au destinataire. En tout cas, ne négligez pas cet aspect – **un seul signalement spam pour 1000 envois peut déjà nuire à votre domaine** [19], alors qu'un désabonnement ne pénalisera pas votre réputation.

- **Nombre de relances :** En prospection à froid, suivez la règle *« pas plus de 1 ou 2 relances »*. Si le prospect n'a pas répondu à votre email initial, il est accepté de renvoyer un **deuxième email 3 à 5 jours plus tard** en guise de rappel [20]. Maximum, une troisième et dernière tentative une semaine après. Au-delà, vous risquez d'irriter le destinataire et de provoquer un spam report. Gardez vos relances **courtes et courtoises** : rappelez en une ligne que vous faites suite à votre précédent message, et éventuellement apportez une information nouvelle ou valeur ajoutée (une ressource, une réponse à un problème potentiel du prospect). Si après deux relances espacées vous n'avez aucun signe d'intérêt, n'insistez pas davantage – mieux vaut retirer cette personne de vos envois futurs (ou la recontacter bien plus tard) pour préserver votre réputation.

Compte unique vs. plusieurs comptes : Si vous utilisez plusieurs adresses pour prospecter, veillez à **coordonner le contenu et les cibles** :
- Ne contactez pas la *même* personne depuis deux comptes différents, cela ferait un effet "spam" démultiplié et pourrait la pousser à se plaindre. Répartissez plutôt les prospects en listes distinctes par expéditeur.
- Assurez une **cohérence de ton** entre vos comptes (pour ne pas donner des messages contradictoires

venant de la même entreprise), tout en pouvant personnaliser chaque signature (par exemple chaque commercial a son style).
- Si vous envoyez des séquences d'emails depuis plusieurs comptes, évitez de copier mot pour mot le même texte sur les 2–3 comptes. Introduisez de légères variations dans le style ou la tournure des phrases entre les expéditeurs – cela réduit la probabilité que Gmail identifie vos messages comme des doublons automatisés.
En somme, sur le fond du message, les mêmes règles anti-spam s'appliquent quel que soit le nombre de comptes. La différence, c'est qu'avec plusieurs comptes vous devez redoubler d'organisation pour ne pas saturer les destinataires ni générer d'incidents involontaires (par exemple deux personnes de votre équipe qui écrivent au même client la même semaine – à éviter).

Volume et rythme d'envoi

Même si votre contenu est de qualité, **la quantité et la cadence d'envoi** peuvent vous faire basculer en spam si elles sont inappropriées. Voici les seuils et limites à connaître et nos recommandations pour un envoi *safe* :

- **Limites officielles de Gmail/Workspace :** Un compte **Google Workspace** (abonnement payant) peut envoyer jusqu'à **2 000 emails par jour** [21] . En pratique, il y a aussi des sous-limites : pas plus de **2 000 destinataires par message** (dont 500 *externe* max par mail) [22] , et un total de **10 000 destinataires distincts par jour** par compte [23] . Pour comparaison, un compte Gmail gratuit est limité à **500 envois/jour** [21] . **Cependant, ces chiffres sont des plafonds théoriques**. Approcher ces maximums en cold email vous assurerait quasiment d'être filtré en spam avant même d'y arriver. Google lui-même ne fournit pas de limite horaire précise, mais **il est conseillé de ne pas dépasser ~20 envois par heure** pour Gmail [24] . De plus, Gmail peut temporairement vous bloquer si vous atteignez ces caps (blocage 24h) ou même **abaisser automatiquement vos limites** si des comportements spammeurs sont détectés [25] [26] .

- **Bonnes pratiques de volume pour la prospection :** Dans le cadre du cold outreach, de nombreux experts suggèrent de se fixer une limite **bien inférieure aux maxima**. Une référence courante est **≈100 emails par jour par adresse** afin de garder une délivrabilité optimale [27] . Ce niveau reste suffisamment élevé pour générer des leads sans alerter les filtres, si le reste des pratiques est bon. Bien sûr, ce chiffre de 100/jour n'est pas à atteindre dès le début : suivez la démarche de warm-up progressive décrite plus haut (par ex. ~20/jour la première semaine [14] , ~50 la deuxième, puis 100…). Au-delà de 100–150/jour, on constate généralement une dégradation des taux d'ouverture/réponse et un risque accru de passer en spam. **Envoi horaire :** plutôt que d'envoyer 100 emails en une rafale, étalez-les tout au long de la journée. Par exemple, *10 emails par heure pendant 10 heures* donne 100/jour de manière fluide. Vous pouvez même intégrer des **pauses aléatoires** entre les envois pour imiter un rythme humain (certains outils le font automatiquement). Nous recommandons de ne pas dépasser **20–30 mails par heure** sur un même compte [24] [28] . Cela évite des pics de trafic suspects sur votre boîte.

- **Éviter les envois groupés massifs :** N'utilisez pas votre compte Gmail comme une plateforme d'emailing de masse classique (même si la limite quotidienne semble élevée). Par exemple, envoyer le *même message* à 300 destinataires en CCI est une très mauvaise idée – Gmail détectera immédiatement un comportement de spammeur. En prospection B2B, on envoie typiquement **un email à la fois, à une personne à la fois**, éventuellement en utilisant un outil qui personnalise et envoie individuellement chaque mail. Respectez toujours cette logique d'envoi individualisé. De plus, **évitez d'envoyer trop d'emails vers un même domaine destinataire dans un court laps de temps**. Si vous prospectez 50 personnes d'une même

entreprise (donc même domaine de réception), ne leur écrivez pas tout à la suite. Espacez sur plusieurs jours ou heures. Les serveurs des entreprises peuvent vous bloquer s'ils reçoivent une rafale soudaine d'emails similaires.

- **Taux de spam et seuils de tolérance :** Gmail attache une grande importance au **taux de plaintes pour spam** (*User-Reported Spam Rate*). Il s'agit du pourcentage de vos emails vers Gmail qui sont signalés comme indésirables par les utilisateurs. Il faut **garder ce taux en dessous de 0,1–0,3 %** absolument. En pratique, cela signifie **pas plus d'environ 1 signalement pour 1000 emails envoyés** [29] [30]. Google a récemment confirmé qu'au-dessus de **0,3 % de spam reports, votre délivrabilité va sévèrement en pâtir** (emails envoyés en spam automatiquement, voire rejetés) [31] [32]. Ces chiffres serrés soulignent qu'en cold email *chaque plainte compte*. Votre objectif doit être de n'en avoir **aucune**. Pour cela, soignez le ciblage (contactez des prospects pertinents qui seront intéressés, pas des listes massives non qualifiées) et respectez les bonnes pratiques de contenu et d'opt-out vues plus haut.

- **Autres indicateurs à surveiller :** Le taux de rebond (*bounce rate*) est le pourcentage d'emails non délivrés (adresses invalides, boîtes pleines, etc.). Un bounce élevé affecte également votre réputation. Maintenez-le le plus bas possible (idéalement <3–5%). Utilisez des outils de vérification d'emails pour nettoyer vos listes et éviter d'envoyer à des adresses inexistantes. De même, le taux d'ouverture peut donner une indication indirecte : si vos ouvertures s'effondrent alors que vous augmentez le volume, c'est possiblement que vos mails finissent en spam. Réagissez en réduisant le volume ou en améliorant le contenu si besoin.

Compte unique vs. plusieurs comptes : L'avantage d'avoir plusieurs comptes d'envoi sur un domaine, c'est de **pouvoir répartir le volume**. Par exemple, au lieu d'un seul compte qui envoie 200 emails/jour (ce qui commence à être risqué), deux comptes peuvent en envoyer 100 chacun, ce qui allège la charge par adresse [33]. Gmail verra deux expéditeurs distincts modérés plutôt qu'un seul très actif. **Mais attention :** du point de vue du domaine, cela fait toujours 200/jour au total. Si votre domaine est nouveau ou peu utilisé, 200/jour peut être trop élevé d'emblée. Donc, ajouter des comptes ne double pas magiquement ce que vous pouvez faire sans précaution – il faut *là aussi monter progressivement*. En revanche, sur un domaine bien établi, 2 comptes à 100/j peuvent être acceptables là où 1 compte à 200 d'un coup aurait pu déclencher un blocage. Avec plusieurs comptes, **respectez les limites par compte ET globalement**. Évitez, par exemple, d'utiliser 5 comptes pour envoyer 5×100 = 500 mails/jour si votre domaine n'a jamais dépassé 100 auparavant – Gmail remarquera la soudaine explosion d'activité sur le domaine. Une stratégie multi-comptes sert surtout à **diversifier les risques et toucher plus de prospects sans sur-solliciter une seule adresse**. Elle doit s'accompagner d'une coordination rigoureuse : chaque compte doit garder un volume raisonnable et sa propre cadence. Idéalement, utilisez des outils de campagne qui ont des fonctionnalités de **rotation d'expéditeurs** [34] [35] : ainsi, vos prospects sont automatiquement répartis entre vos comptes sans dépasser les quotas de chacun. Dernier point crucial : **si un de vos comptes venait malgré tout à être temporairement bloqué ou pénalisé par Gmail**, stoppez ses envois immédiatement et réduisez le rythme des autres comptes le temps d'analyser la cause. Ne compensez pas en "pressant" plus les comptes restants – ce serait empirer le problème au niveau du domaine.

Engagement utilisateur et interaction

L'« engagement utilisateur » désigne la manière dont vos destinataires réagissent à vos emails. Gmail surveille de près ces interactions, car elles reflètent la pertinence de vos messages. Un bon engagement

améliore votre réputation, tandis que l'indifférence ou les réactions négatives l'affectent négativement. Voici comment maximiser les signaux positifs :

- **Obtenir des réponses :** La réponse d'un destinataire à votre email est sans doute le **signal le plus positif** qui soit. Cela indique à Gmail que votre message était désiré et utile (puisque l'utilisateur a pris la peine de répondre). Pour favoriser cela, posez une question dans votre email, ou incitez à un échange (demande d'avis, proposition concrète d'appel, etc.). Un email de prospection efficace est souvent celui qui engage le dialogue. Même une courte réponse du type « intéressé, envoyez-moi plus d'infos » est très bénéfique. De plus, lorsque quelqu'un répond, Gmail a tendance à automatiquement considérer la conversation comme importante et à la garder en boîte de réception principale.

- **Encourager des actions sur le mail :** Si obtenir une réponse n'est pas évident à chaque fois, d'autres interactions comptent aussi : par exemple, si le destinataire clique sur un lien de votre email, ou le transfère à un collègue, ou le déplace de la Promotion vers la Principale (pour les utilisateurs Gmail particuliers). Vous ne contrôlez pas directement cela, mais vous pouvez *favoriser* ces comportements. Comment ? En envoyant du contenu pertinent qui donne envie de cliquer (par ex. un lien vers une ressource de qualité), ou en demandant au prospect de prendre une petite action (par ex. « pouvez-vous regarder ce court document attaché ? » – s'il le fait, c'est un engagement). Bien sûr, restez subtil et ne forcez pas artificiellement la main. L'idée est que plus vos emails seront utiles, plus les destinataires auront naturellement envie d'interagir, ce qui envoie à Gmail des signaux de légitimité.

- **Réduire les signaux négatifs :** Le pire signal, on l'a dit, est le *« Signaler comme spam »*. Pour l'éviter, utilisez les bonnes pratiques précédentes : ciblage précis, désinscription claire, ton respectueux. Un autre signal négatif plus subtil est le **manque total d'engagement** : si vos emails sont systématiquement ignorés (ni ouverts, ni cliqués, ni répondus) sur de longues périodes, Gmail pourra estimer qu'ils n'intéressent pas les utilisateurs et les filtrer plus volontiers en spam à l'avenir. C'est pourquoi il est important de *rafraîchir vos listes* : éliminez ou mettez en pause les contacts qui n'ont jamais ouvert/cliqué/répondu après plusieurs tentatives. Inutile de continuer à marteler des destinataires inactifs – non seulement ça ne donnera rien, mais ça peut ternir votre réputation (par un effet statistique de faible engagement global).

- **Créer de la confiance :** Si un prospect est vraiment intéressé par vos emails, il peut faire quelque chose de très bénéfique : vous ajouter à ses contacts ou marquer explicitement votre message comme « important » ou « non spam ». Cela, Gmail le retient et il est probable que tous vos envois futurs vers cette personne arriveront en boîte de réception. Vous pouvez subtilement encourager cela en fin d'email, par exemple en disant *« N'hésitez pas à m'ajouter à vos contacts pour faciliter nos échanges »* – certains destinataires le feront. De même, si vous téléphonez ou contactez autrement un prospect et qu'il vous dit *« j'ai vu votre mail dans mes spams »*, invitez-le à cliquer sur « Pas spam » – cette action améliore votre délivrabilité auprès de ce domaine. Bien sûr, ce sont des cas ponctuels, mais chaque petit geste compte pour bâtir votre réputation.

- **Taux d'ouverture et indicateurs d'intérêt :** Comme mentionné, un taux d'ouverture élevé (surtout sur Gmail) signifie que vos sujets et préheaders attirent l'attention et que vos mails n'ont probablement pas été filtrés. Continuez d'optimiser ces éléments. Le taux de clic, s'il est applicable (liens dans vos mails), est aussi un signe d'intérêt. Bien que Gmail ne voit pas directement le taux de clic, un bon taux de clic va souvent de pair avec moins de plaintes spam. **Astuce :** vous pouvez utiliser Gmail Postmaster Tools pour suivre l'engagement négatif (spam reports), mais pour l'engagement positif, utilisez votre outil d'envoi (pour opens/clicks) et éventuellement les réponses manuellement comptabilisées. L'important est de **tenir un suivi** :

par exemple, si vous constatez que sur 100 emails envoyés depuis un compte, seuls 5% sont ouverts, c'est un signal d'alarme (peut-être vos mails tombent en promo/spam). Ajustez votre approche en conséquence.

Compte unique vs. plusieurs comptes : Sur plusieurs comptes, les principes d'engagement restent identiques, mais il faut veiller à **uniformiser la qualité** : si un de vos comptes a un contenu ou un ciblage moins pertinent, il recevra moins d'engagement et plus de plaintes, ce qui pourrait affaiblir toute la réputation du domaine. Par exemple, disons que vous avez deux commerciaux envoyant chacun 50 emails/jour : si l'un d'eux insiste pour relancer 5 fois les prospects et force un peu trop la main, il y a plus de chances qu'il génère des « spam reports » – et *une seule des adresses qui dérape peut mettre le domaine sur liste grise*. Il est donc crucial en équipe de **partager les bonnes pratiques** et de suivre les stats de chaque compte séparément. Vous pouvez instaurer des mini-bilans : taux d'ouverture/réponse par expéditeur, nombre de désabonnements, etc., pour repérer si un compte a des métriques anormales. Si oui, formez la personne à améliorer ses emails avant que cela n'affecte tout le monde. En positif, plusieurs comptes peuvent aussi se soutenir : si globalement vos 2–3 comptes reçoivent tous des réponses et peu de plaintes, cela renforce le signal global que *"les emails de @votredomaine.com sont bien reçus et légitimes"*. Pour finir, sachez que Gmail calcule la réputation autant au niveau domaine qu'au niveau de chaque adresse expéditrice. Donc, prendre soin de **chaque identité d'envoi individuellement** est payant.

Réputation du domaine et de l'expéditeur

Votre **réputation d'expéditeur** est un score invisible qui conditionne la délivrabilité de vos emails. Gmail évalue en permanence la réputation de votre **domaine** (et dans une certaine mesure de chaque adresse). Cette réputation est influencée par tout ce que nous avons évoqué : authentifications en place, historique de spam/bonnes interactions, volumes d'envoi, taux de retour négatifs, etc. [36] [37].

Voici comment bien gérer et préserver votre réputation sur le long terme :

- **Construire une réputation positive dès le départ :** Après le warm-up, si tout s'est bien passé, vous aurez envoyé quelques centaines d'emails sans encombre, avec peut-être quelques réponses et zéro plainte spam. Vous commencez à avoir une *bonne réputation naissante*. Continuez sur cette lancée en maintenant des pratiques stables. Le facteur temps joue : plus vous envoyez régulièrement de *bons* emails sur plusieurs semaines/mois, plus Gmail vous fera confiance. À l'inverse, un nouveau domaine est toujours sous surveillance : considérez que les 4 à 8 premières semaines d'envoi régulier sont critiques pour "faire vos preuves".

- **Conséquences d'une mauvaise réputation :** Si, malheureusement, vos emails génèrent des plaintes ou des taux de bounce élevés, Gmail pourra **dégrader votre réputation**. Concrètement, vos futurs mails iront de plus en plus en spam, même auprès de prospects qui n'ont jamais entendu parler de vous. Gmail peut même *ralentir ou bloquer* vos envois si la réputation atteint un point critique (par ex, rejet des messages avec une erreur du style « messagerie non disponible – message bloqué pour cause d'abus »). Il est donc très difficile de « travailler sous le radar » avec une mauvaise réputation : cela vous suit comme une casserole tant que vous n'avez pas rectifié le tir et patienté suffisamment. Notez que la réputation est partagée au niveau du domaine : **si un compte fait des bêtises, tous les comptes du domaine trinquent**. Par exemple, Gmail a déjà affiché des alertes du genre *« Beaucoup de messages de votredomaine.com sont du spam »* lorsque l'un des expéditeurs abusait [38]. Donc en équipe, la discipline commune est essentielle.

- **Redresser la barre si nécessaire :** Si vous constatez une détérioration (voir section monitoring juste après pour savoir comment le détecter), il faut **agir vite**. Réduisez immédiatement vos volumes d'envoi (de moitié ou plus) pour donner du répit au domaine. Analysez ce qui a pu causer le problème : liste d'envoi de mauvaise qualité ? Contenu trop commercial ? Spam trap touché ? Une fois le problème identifié, corrigez-le (purgez les contacts douteux, modifiez vos modèles d'emails, etc.). Ensuite, passez éventuellement par une phase de « réchauffe » de réputation : n'envoyez pendant quelque temps qu'aux contacts les plus engagés ou à de toutes petites listes triées sur le volet (ceux qui ouvrent/répondent) pour générer un maximum d'interactions positives. Avec du temps et des signaux positifs, la réputation peut remonter progressivement et vos emails reviendront en boîte de réception.

- **Changement de domaine ?** Certains, face à une réputation ruinée, envisagent de changer de domaine d'envoi (par ex. passer de `votredomaine.com` à `votre-domaine.io`). Cela peut être un *dernier recours* si réellement Gmail vous a mis en liste noire informelle. Mais attention : **changer de domaine sans changer les pratiques ne sert à rien**. Gmail repérera vite les mêmes schémas et le nouveau domaine sera à son tour pénalisé [39]. De plus, vous perdez le bénéfice de l'ancienneté du domaine précédent. Ne voyez donc pas cela comme une solution magique. Mieux vaut investir dans les bonnes pratiques dès le début et ne pas brûler son nom de domaine principal. D'ailleurs, certaines organisations choisissent dès le départ un *domaine alternatif* pour leurs campagnes de cold email (pour protéger le domaine principal de la société). C'est envisageable – par ex. `prospection-votredomaine.com` – mais gardez en tête que ce domaine alternatif devra lui aussi être correctement authentifié et chauffé. Qu'il soit principal ou secondaire, **tout domaine d'envoi doit gagner sa réputation par l'usage responsable**.

- **Réputation des adresses IP :** Dans le cas de Gmail, vos emails sortent des serveurs Google – vous n'avez pas d'IP dédiée. Gmail s'appuie donc surtout sur la réputation de votre domaine et de l'adresse expéditeur. L'IP Google qui achemine votre mail est partagée avec d'autres envois clients Workspace : elle est globalement bien vue tant que vous, et les autres, ne faites pas de spam. Cette mutualisation vous aide (infrastructure de confiance) mais peut aussi vous pénaliser si Google détecte un abus grave, il peut limiter votre compte individuellement. À l'inverse, si vous utilisiez un SMTP tiers (serveur Exchange, etc.), vérifiez la réputation des IP utilisées (certaines blocklists publient des *IP sending reputation*). **Mais pour Google Workspace, concentrez-vous sur le domaine.**

Compte unique vs. plusieurs comptes : Comme déjà souligné, la réputation est principalement **attachée au domaine**. Donc que vous ayez un ou dix comptes, c'est la **qualité globale de tous les envois** depuis ce domaine qui comptera. Un seul compte facilite le contrôle (une seule personne envoyant, moins de risque d'écart de conduite) mais limite le volume. Plusieurs comptes augmentent le volume possible, mais demandent un **pilotage centralisé de la réputation** : par exemple, surveillez si l'un des comptes obtient plus de refus ou de réponses négatives – il pourrait être le maillon faible. En interne, partagez les retours d'expérience entre utilisateurs du même domaine, et pourquoi pas **instaurez des règles communes** (par ex, pas plus de 2 relances, toujours inclure l'opt-out, etc. – tout ce que ce guide couvre). Ainsi, chaque compte contribuera positivement à la réputation commune plutôt que de la ternir. En bref, *la réputation, c'est l'affaire de tous sur le domaine*. Si tout le monde respecte les bonnes pratiques, la réputation de `votredomaine.com` deviendra un atout solide qui vous permettra d'atteindre les boîtes de réception Gmail plus facilement au fil du temps.

Suivi et monitoring de la délivrabilité

Enfin, un pilier souvent négligé : **mesurer et surveiller** la performance de vos envois. Pour ne pas découvrir trop tard qu'on atterrit en spam, il faut mettre en place du monitoring dès le début :

- **Google Postmaster Tools :** C'est un service gratuit de Google qui fournit des données sur vos envois vers Gmail. Enregistrez votre domaine sur **Postmaster Tools** (postmaster.google.com) en le validant via un enregistrement DNS. Une fois configuré, vous aurez accès à plusieurs indicateurs clés :
- *Reputation du domaine* (une note de Google de **Bad** à **High**). C'est un critère synthétique de votre réputation d'envoi auprès de Gmail. Vous visez *High* ou *Medium* au minimum. Si vous descendez à *Low* ou *Bad*, il y a un sérieux problème à résoudre.
- *Taux de spam (user-reported spam rate)* : le pourcentage d'emails de votre domaine que les utilisateurs Gmail ont marqués indésirables. Vous verrez ce chiffre sur une période donnée. Gardez-le le plus bas possible – idéalement proche de 0%. Comme dit, tout pic approchant ou dépassant **0,3% est critique** [32] . Google Postmaster met clairement en avant ce seuil dans sa nouvelle interface de conformité.
- *Taux de livraison, erreurs, etc.* : vous saurez si Gmail a rejeté certains messages (par ex. pour cause de blocage de volume ou autre). Vous verrez aussi le taux d'emails acceptés, mis en spam (ce dernier n'est pas explicitement donné, mais on peut le déduire en partie des autres stats).
- *Authentification SPF/DKIM* : Postmaster indique le pourcentage de mails de votre domaine qui passent SPF et DKIM. Ça devrait être 100%. Si ce n'est pas le cas, vous avez un problème technique à corriger (par exemple un envoi via un outil non déclaré dans le SPF).

En surveillant Postmaster Tools régulièrement (par ex. une fois par semaine au début), vous pourrez **détecter une dégradation** de réputation ou une hausse du spam rate avant qu'il ne soit trop tard. C'est vraiment l'outil de référence pour Gmail [40] [32] .

- **Rapports DMARC :** Si vous avez activé DMARC avec `p=none` et une adresse `rua`, vous commencerez à recevoir des rapports XML quotidiennement de la part de Gmail, Microsoft, Yahoo, etc. Ces rapports listent les sources d'envoi utilisant votre domaine et indiquent si SPF/DKIM ont passé ou échoué. Utilisez un outil en ligne (il en existe des gratuits) pour les lire confortablement. Les rapports DMARC vous aident à *identifier d'éventuelles utilisations abusives* de votre domaine (quelqu'un qui essaierait de spammer en se faisant passer pour vous). Ils montrent aussi si une partie de vos mails légitimes échouent aux tests (ce qui serait à corriger rapidement). Ce n'est pas directement sur la « livraison en inbox », mais c'est crucial pour s'assurer que l'authentification fonctionne en permanence.

- **Suivi interne des métriques campagne :** Parallèlement, suivez vos **taux d'ouverture, de clic, de réponse** via l'outil d'envoi que vous utilisez (ou même manuellement si vous n'avez pas d'automatisation). Une chute soudaine du taux d'ouverture sur Gmail peut indiquer un passage en spam. Un taux de réponse très faible pourrait signifier que le message n'est pas reçu ou pas convaincant – dans tous les cas, c'est un signal d'alerte. Comparez les performances entre vos différents comptes si vous en avez plusieurs. Si l'un d'eux voit ses stats chuter par rapport aux autres, enquêtez : a-t-il été trop ambitieux sur le volume ? A-t-il envoyé à une liste de moindre qualité ? Plus globalement, conservez l'historique de ces indicateurs pour voir l'évolution au fil du temps et l'impact de vos ajustements.

- **Adresses de test et seed list :** Il est utile d'avoir quelques adresses email de test pour vérifier la délivrabilité de vos campagnes. Par exemple, créez un compte Gmail test et ajoutez-le (discrètement) dans chacune de vos campagnes. Regardez si les mails arrivent en *Inbox*, en

Promotions ou en *Spam*. Attention, ce n'est qu'un indicateur (Gmail peut traiter différemment un mail de test et un mail envoyé en masse), mais cela peut quand même alerter en cas de gros problème (si même votre test arrive en spam, il y a fort à parier que les vrais destinataires aussi). Vous pouvez également utiliser des services de seed list plus élaborés, qui testent l'inbox placement sur plusieurs FAI, bien que pour commencer ce n'est pas indispensable.

- **Logs de rebonds et blocages :** Si vous recevez des notifications de non-délivrance (messages "bounced" ou rejetés), lisez-les attentivement. Gmail renvoie parfois des indications dans les erreurs SMTP. Par exemple un code d'erreur `5.7.26` indique un refus pour cause d'authentification manquante ou de politique (c'est lié à DMARC manquant ou mal aligné souvent) [11]. Un code `4.7.0` pourrait signaler que vous avez atteint une limite de taux et que l'envoi est temporairement différé. Bref, ne les ignorez pas : corrigez ce qui peut l'être (fausse adresse, domaine mal orthographié, etc.), et si c'est un blocage général, suspendez la campagne et revoyez vos paramètres d'envoi.

- **Surveillance des listes noires :** Vérifiez de temps en temps si votre domaine ou vos adresses IP figurent sur des **blacklists publiques** (Spamhaus, Barracuda, etc.). Pour l'IP Gmail ce n'est pas vraiment sous votre contrôle individuel, mais pour le domaine il existe des listes de domaines spammeurs (URIBL, Spamhaus DBL). Être listé dessus peut expliquer des problèmes de délivrabilité. Si cela arrive et que c'est dû à vos envois, suivez la procédure de demande de retrait après avoir corrigé le problème.

- **Feedback loop autres FAI :** Ce guide est centré sur Gmail, mais si vous prospectez d'autres domaines, sachez que certains (Yahoo, AOL…) proposent des mécanismes de *Feedback Loop* où vous pouvez recevoir un rapport quand un utilisateur marque un de vos mails en spam. Avec Google, on l'a vu, il faut passer par Postmaster Tools pour voir ça (agrégé). Pour Outlook/Office365, il n'y a pas d'outil équivalent accessible facilement, mais vous pouvez au moins surveiller les taux de bounce et vos réponses. L'idée générale : multipliez les sources d'information pour ne pas voler à l'aveugle.

En somme, **instaurez une vraie routine de monitoring**. La délivrabilité n'est pas un acquis, c'est un équilibre à maintenir. En suivant régulièrement vos indicateurs (réputation, plaintes, ouvertures, etc.), vous pourrez ajuster proactivement vos pratiques de prospection. L'objectif final est d'atteindre un niveau où vos emails arrivent en inbox de manière fiable – ce qui est réalisable en combinant : *domaine bien authentifié, warm-up patient, contenu propre, volumes mesurés, engagement maximisé, réputation surveillée*. Avec ce guide et une exécution disciplinée, vos campagnes de cold email via Google Workspace devraient éviter le terrible dossier Spam et toucher efficacement vos prospects .

Sources : Les recommandations chiffrées et techniques de ce guide s'appuient sur les meilleures pratiques publiées par Google et des experts de la délivrabilité. Pour aller plus loin, vous pouvez consulter les guidelines officielles de Google Workspace [41] [42], ainsi que des ressources spécialisées comme les blogs de Lemlist, Sparkle ou Allegrow cités tout au long du texte. En appliquant consciencieusement ces conseils, vous mettez toutes les chances de votre côté pour que vos emails de prospection à froid ne soient pas filtrés comme indésirables par Gmail. Bonne prospection !

---

1 4 Set up SPF - Google Workspace Admin Help
https://support.google.com/a/answer/33786?hl=en

2 9 10 11 17 18 30 31 41 42 Email sender guidelines - Google Workspace Admin Help
https://support.google.com/a/answer/81126?hl=en

3 5 6 8 SPF/DKIM/DMARC Setup Guide for Google Workspace (formerly known as G Suite) (Gmail for Business) - DMARCLY
https://dmarcly.com/blog/spf-dkim-dmarc-set-up-guide-for-g-suite-gmail-for-business

7 Set up DMARC - Google Workspace Admin Help
https://support.google.com/a/answer/2466580?hl=en

12 36 Comment chauffer un nouveau domaine d'envoi – Assistance client ActiveCampaign
https://help.activecampaign.com/hc/fr-fr/articles/11874237112988-Comment-chauffer-un-nouveau-domaine-d-envoi

13 20 Combien d'e-mails froids envoyer par jour : 4 conseils d'experts pour de meilleurs résultats
https://sparkle.io/fr/blog/how-many-cold-emails-to-send-per-day/

14 19 28 29 Eviter SpamFlag guide.pdf
file://file-NRc7sHEwNBPPorNmGc8noR

15 24 25 26 How Many Emails Before Spam? Avoiding Over-Send Penalties
https://www.allegrow.co/knowledge-base/email-before-spam

16 37 38 39 Pourquoi vos e-mails sont-ils considérés comme spam par Gmail ? - Dolist
https://www.dolist.com/blog/delivrabilite-email/pourquoi-vos-emails-sont-consideres-comme-spam-par-gmail/

21 27 33 34 35 Comment dépasser les limites quotidiennes d’envoi de mails (et contacter plus de prospects !)
https://www.lemlist.com/fr/blog/depasser-limite-envoi-mail

22 23 Gmail sending limits in Google Workspace - Google Workspace Admin Help
https://support.google.com/a/answer/166852

32 40 Google Postmaster Tools V2: Ultimate Deliverability Guide
https://www.allegrow.co/knowledge-base/google-postmaster-tools