

**OPTIMISER LA
DÉLIVRABILITÉ
DE SES
CAMPAGNES**

SOMMAIRE

1. Définitions	01
2. Types de filtres FAI	02
3. Construire une bonne réputation d'expéditeur	04
3.1. Construire une base de données saine	04
3.2. Soigner son code HTML	07
3.3. Spam words à éviter	09
3.4. IP mutualisée vs. IP dédiée	10
3.5. Uniformisation des noms de domaines	11
4. Tester, analyser les résultats et entretenir une bonne réputation	12

01 DÉFINITIONS

TAUX DE DÉLIVRABILITÉ

Le taux de délivrabilité est le pourcentage d'e-mails qui est réellement reçu par le destinataire, c'est-à-dire qui est parvenu dans sa boîte de réception.



**Taux de délivrabilité =
la totalité des e-mails envoyés
(100%) - le taux de bounce**

TAUX DE REBOND OU BOUNCE

Il fait référence à la proportion d'emails pour lesquels vous avez reçu un message d'erreur vous prévenant que votre mail n'a pas atteint son destinataire. Nous différencions deux types de taux de rebond : ceux qui sont définitifs (appelés aussi hard bounce) et ceux qui sont temporaires (soft bounce).

Les raisons pour l'apparition de hard bounces peuvent être différentes : domaine invalide, serveur inexistant, etc. En ce qui concerne les soft bounces, ils se produisent souvent quand une boîte de réception est saturée ou quand nous recevons un message d'absence du bureau par exemple.

02 TYPES DE FILTRES FAI

Le nombre croissant de pratiques malveillantes (spam, piratage, phishing, etc.) a rendu obligatoire le filtrage des messages par les FAI et les différentes messageries.

Aujourd'hui, avant d'atteindre son destinataire, votre campagne passe par une série de vérifications. Voyons lesquelles !

ANALYSE DE VOTRE RÉPUTATION

- Est-ce que votre adresse IP a été blacklistée par les FAI ou les filtres anti-spam ?
- Quelle information a été collectée sur vous par des fournisseurs de données de réputation comme Return Path par exemple.



Ces filtres analysent aussi la réaction de vos abonnés lors de vos anciennes campagnes :

- Est-ce qu'ils ont signalé un spam ?
- Est-ce qu'ils vous ont rajouté à leur liste de contacts (liste verte) ?

VÉRIFICATION DU CONTENU DE VOTRE MESSAGE



- Est-ce que votre texte contient des spam words ?
- Est-ce que l'orthographe de vos textes est correcte ?
- Quel est le ratio images / texte dans l'e-mail ?
- Les balises <alt> sont-elles présentes ?
- Vos CTA renvoient-ils vers des sites web avec une bonne réputation ?

VÉRIFICATIONS TECHNIQUES DE VOTRE IDENTITÉ



- SPF (Sender Policy Framework)

Grâce à ce protocole les FAI peuvent vérifier si l'envoi du message a été autorisé par l'expéditeur en question.

- DKIM (DomainKeys Identified Mail)

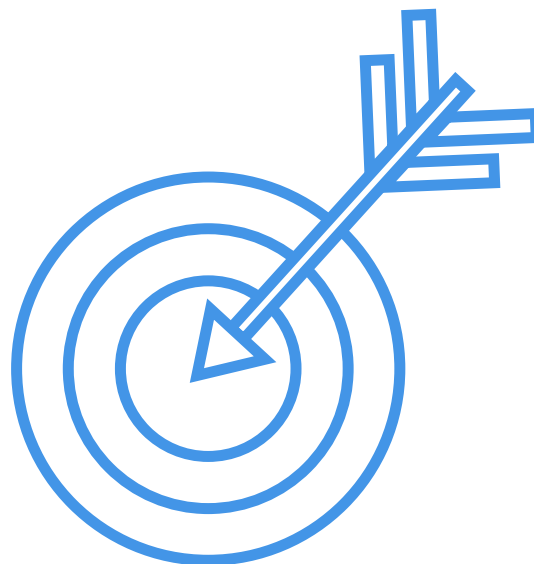
Grâce à une signature cryptographique, ce filtre vérifie l'authenticité du domaine expéditeur et garantit l'intégrité du message.

03 ÉVITER LES FILTRES SPAM ET CONSTRUIRE SA RÉPUTATION

3.1. CONSTRUISEZ UNE BASE DE DONNÉES DE QUALITÉ

CONTACTEZ UNIQUEMENT DES CONTACTS OPT-IN

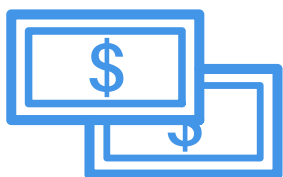
Les contacts opt-in sont ceux qui ont donné leur accord préalable pour recevoir vos newsletters. Il est obligatoire de demander leur permission et si vous ne respectez pas cette règle, vous risquez de lourdes amendes.



- Double Opt-In -

Le double opt-in ajoute l'internaute à votre liste de contacts uniquement après qu'il a cliqué sur un lien qui lui a été fourni dans l'e-mail de confirmation de son inscription.

En adoptant le double opt-in vous serez sûr d'obtenir une personne intéressée par vos produits ou services et vous allez donc créer une base de données de qualité.



OUBLIEZ L'ACHAT DE BASES DE DONNÉES

Cette pratique est non seulement illégale mais elle ne vous apportera pas non plus des contacts de qualité. De plus, vous risquez d'augmenter considérablement votre taux de plainte et de désabonnement et de nuire ainsi à votre réputation d'expéditeur.

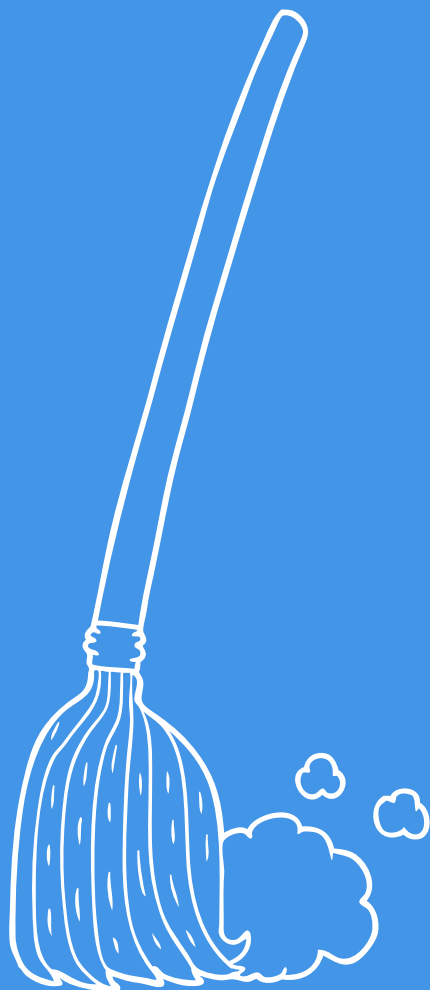


SPAM TRAPS

Un spam trap (littéralement de l'anglais « piège à spam »), est une adresse ou un réseau d'adresses créé spécialement pour détecter les actions et les serveurs utilisés par les spammeurs. Ces e-mails n'ont jamais été utilisés par une vraie personne, ils ne souscrivent pas à des newsletters et n'envoient jamais rien.

Si un email arrive sur une telle adresse, c'est parce qu'elle a été collectée par un spambot : il s'agit donc d'un spam. Le message peut alors être répertorié et par conséquent, les serveurs utilisés pour son envoi se retrouveront en blacklist.

NETTOYEZ PÉRIODIQUEMENT VOTRE BASE DE DONNÉES



Le nettoyage d'une base de données consiste à supprimer les adresses invalides qu'elle contient. Ces dernières ont un impact très négatif sur votre délivrabilité et sur votre réputation d'expéditeur.

Supprimez aussi immédiatement les contacts qui ont utilisé le bouton "*ceci est un spam*" après la réception d'un de vos messages.

Si vous avez votre base de données depuis plusieurs années mais que vous ne l'avez pas vraiment utilisée, nous vous conseillons de lancer une campagne de confirmation d'opt-in. Cela vous permettra d'analyser l'activité de votre base de données pour y laisser uniquement les prospects intéressés par votre entreprise.

N'OUBLIEZ PAS LE LIEN DE DÉSINSCRIPTION

Dans chaque e-mail que vous envoyez, l'utilisateur doit être capable de trouver un moyen simple et facile de se désabonner.

Si votre lien n'est pas présent ou ne fonctionne pas, le client souhaitant se désinscrire appuiera tout simplement sur « *signaler comme spam* ». Il vaut mieux perdre un abonné désintéressé que faire souffrir votre réputation d'expéditeur.

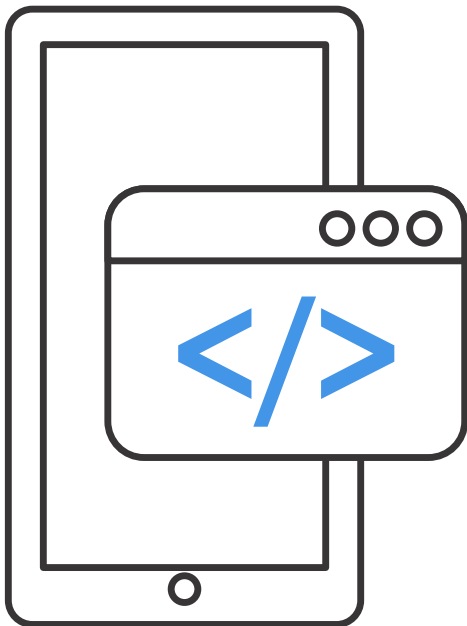


3.2. SOIGNEZ VOTRE CODE HTML

Si vous utilisez l'éditeur de création de newsletters de MailStronger, vous n'avez pas besoin de vous soucier du code HTML. Nos développeurs connaissent et respectent les bonnes pratiques de l'emailing.

Néanmoins, il y a quelques détails qui peuvent vous aider à améliorer votre délivrabilité.

RENSEIGNEZ LES ALT TAGS



L'alt tag est un texte alternatif qui décrit les images que vous avez utilisées dans votre newsletter. Vu que la plupart des boîtes mails bloquent l'affichage des photos par définition, cette description aidera les utilisateurs (mais aussi et avant tout : les robots) à mieux comprendre votre message. L'absence d'alt tags dans vos campagnes peut déclencher un filtre anti-spam.

OPTIMISEZ VOS IMAGES

Si vous soignez le poids de votre message, il s'ouvrira beaucoup plus rapidement. Voilà pourquoi nous vous conseillons d'optimiser les images que vous y intégrez. Il y a plusieurs outils qui vous permettent de réduire le poids de vos fichiers sans altérer leur qualité. En voici quelques-uns :



RATIO IMAGES/TEXTE

On estime qu'un ratio idéal dans un email est de 60% de texte et 40% d'images. Le respect de cette proportion est important pour votre délivrabilité car les filtres anti-spam considèrent le surplus d'images comme indicateur de contenu indésirable et peuvent donc bloquer votre newsletter.

3.3. EVITEZ LES SPAM WORDS ET FAITES ATTENTION AU BON ORTHOGRAPHE

QU'EST-CE QUE LES SPAM WORDS ?

Le Spam Word est un mot qui est surveillé par les fournisseurs de messagerie pour déterminer si un e-mail est un spam ou pas. Chaque fois que vous envoyez un courriel, son contenu est scanné et analysé par un robot afin d'être classé dans le bon dossier de la boîte e-mail du récepteur.



MOTS ET EXPRESSIONS À ÉVITER :

- gratuit, cadeau, remboursé, remise, rabais, promotion, pas cher, offre spéciale, -50 %, bonne affaire, vous avez gagné, félicitations, vous avez été choisi
- les signes spéciaux comme \$, %, €
- les mots en majuscules

3.4. CHOISIR UNE ADRESSE IP : DÉDIÉE VS MUTUALISÉE

Lorsque vous choisissez une adresse IP mutualisée, vous partagez avec d'autres clients non seulement le serveur mais aussi sa réputation. De ce fait, si un expéditeur présente une activité douteuse, la réputation de tous les autres comptes sera impactée également (taux de délivrabilité, blacklistage des opérateurs/messageries, etc...).

Afin d'être le seul qui contrôle la réputation de votre adresse IP, vous devez opter pour une IP dédiée. Or, MailStronger propose uniquement des offres avec des IP dédiées. De cette façon nous nous assurons que nos clients obtiennent la meilleure réputation possible.



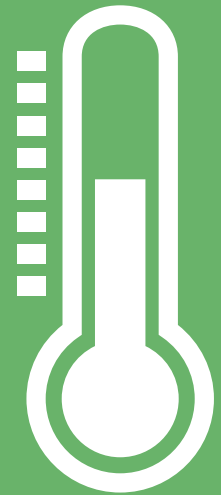
Attention !

Si vous décidez de mettre en place une nouvelle IP dédiée, vous devrez effectuer un préchauffage (ou un warm-up) de cette dernière.

QU'EST-CE QU'UN WARM-UP IP ?

Vu que les fournisseurs d'accès internet ne connaissent pas encore votre nouvelle adresse IP, elle ne bénéficie pas d'une bonne réputation déjà établie. La procédure de warm up consiste à découper l'envoi de vos premières campagnes en plusieurs parties afin de minimiser les risques de non-délivrabilité de vos e-mails.

Afin d'en apprendre plus, veuillez consulter notre livre blanc «*Comment préchauffer (warm up) une adresse IP ?*».



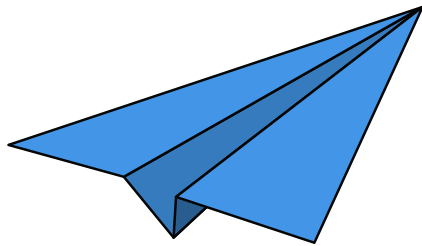
3.5. UNIFORMISATION DU NOM DE DOMAINE UTILISÉ DANS TOUTES LES PARTIES DU MESSAGE

Pour éviter le blocage de la part des FAI vous devez aussi uniformiser votre nom de domaine dans toutes les parties de votre message: le nom de l'expéditeur doit être le même que le site web vers lequel renvoient vos liens.

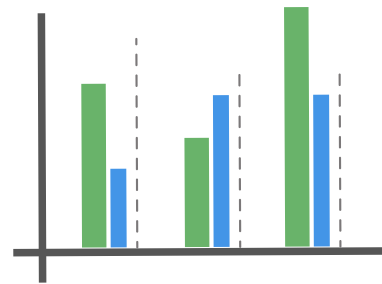
Évitez donc d'inclure des CTA qui redirigent vos destinataires vers les sites web de vos partenaires.

04

ENTREtenir UNE BONNE RÉPUTATION



Avant chaque envoi d'une campagne, faites des tests et analysez de la délivrabilité dans les différentes messageries. Pour ainsi faire, déterminez au préalable les services de messageries les plus utilisés dans votre base.



Ensuite envoyez des BAT TEST pour détecter si votre newsletter a été bien reçue chez les différents fournisseurs. Analysez vos résultats et essayez d'identifier les raisons pour lesquelles votre message a pu se retrouver dans le spam afin de rectifier les erreurs avant l'envoi réel de votre campagne.

BAT

Acronyme utilisé dans l'industrie de l'édition et de la publicité qui signifie "bon à tirer".

ENVOYEZ VOS CAMPAGNES EN ILLIMITÉ AVEC MAILSTRONGER !



- Envois illimités
- Contacts illimités
- Aucune limite journalière
- Aucune Publicité
- Marketing Automation
- API/SMTP

[INSCRIPTION GRATUITE](#)