



**Message Business**<sup>®</sup>  
*communiquiez, prospérez*

# **Sur le Front**

*Webinaire n°1*

*du Marketing électronique*

***L'Emailing, un voyageur international en temps de guerre...***

***Comment votre Emailing arrive, ou n'arrive pas, à vos destinataires ?  
Comment améliorer la délivrabilité de vos messages ?***

## Sommaire

<b>COMPRENDRE POUR REUSSIR.....</b>	<b>3</b>
<b>UN VOYAGEUR INTERNATIONAL EN TEMPS DE GUERRE ! .....</b>	<b>4</b>
Rien à déclarer ? Tout est dans le message ! .....	4
Avant de partir : la check List de l'emailing voyageur .....	6
<b>DES DESTINATAIRES QUI ACCUEILLENENT A BRAS OUVERTS LE VOYAGEUR.....</b>	<b>7</b>
Des adresses exactes ! .....	7
Des adresses consentantes .....	7
Des adresses bien routées ! .....	8
<b>VOS PAPIERS ! L'EMAILING, UN VOYAGEUR À L'IDENTITÉ AUTHENTIFIÉE .....</b>	<b>8</b>
Visa n° 1 sur le passeport électronique de l'emailing : Reverse DNS .....	9
Visa n° 2 sur le passeport électronique de l'emailing : Sender Policy Frame Work.....	9
Visa n° 3 sur le passeport électronique de l'emailing : Domain Key.....	10
Autre vérification de l'identité : l'IP Black Listée .....	10
<b>LES ANTI-SPAM : OUVREZ VOS BAGAGES .....</b>	<b>11</b>
Ce qu'il faut mettre et ce qu'il ne faut pas mettre dans vos bagages .....	12
L'objet : votre déclaration d'entrée sur le territoire.....	11
Retentez votre chance en cas d'échec.....	12
Les Webmail : des millions de douaniers .....	12
<b>POUR RÉSUMER : LES 8 COMMANDEMENTS DE LA DÉLIVRABILITÉ .....</b>	<b>13</b>
<b>A PROPOS DE MESSAGE BUSINESS .....</b>	<b>13</b>
<b>DANS LES PROCHAINES EDITIONS DE « SUR LE FRONT ».....</b>	<b>15</b>

## COMPRENDRE POUR REUSSIR

Lors d'une campagne [emailing](#), le premier objectif est de s'assurer que les messages envoyés arriveront bien dans la messagerie électronique de vos destinataires. S'il est à la portée de chacun d'envoyer un email, effectuer un [emailing](#) de masse est une toute autre affaire. En effet, même une newsletter envoyée à une base d'adresses loyalement collectées peut ne pas passer les mailles du filet de la lutte anti-spam. Cet enjeu a été résumé dans un terme un peu barbare : « la délivrabilité ». Cet anglicisme évoque le taux de livraison effectif du message et son caractère potentiellement améliorable.

Cependant, derrière le mot, une grande opacité persiste. Le chemin parsemé d'embûches que parcourt un [emailing](#) avant d'arriver sur la boîte mail de ses destinataires et le travail effectué conjointement par l'émetteur et le routeur pour fournir une délivrabilité optimale restent souvent extrêmement flous pour le plus grand nombre.

Quelles sont les différentes étapes qui séparent l'émetteur et le destinataire ? Comment expliquer pourquoi certains [emailings](#) arrivent à bon port et d'autres terminent lamentablement dans une boîte à courrier indésirable ? Voire nulle part... Quels sont les impacts du contenu, du design graphique, du code HTML, du système d'envoi, des serveurs de réception, de la liste des destinataires ?

### Et surtout, comment s'améliorer ?

Pour essayer de répondre à toutes ces questions il fallait beaucoup surfer sur Internet, interroger des experts, décrypter la langue de bois des prestataires et analyser des jargons ambigus. Beaucoup de promesses mais aucune explication sur ce qui se passe « sous le capot », aucune vision à 360° et encore moins de vulgarisation des questions techniques.

Nous ne gloserons pas sur les raisons de cette absence d'information. Fidèles à notre mission de facilitateur du marketing électronique, nous avons décidé de combler ce manque en consacrant le numéro 1 de notre webinaire à cette thématique brûlante et peu traitée.

Parfaitement impartial il vise à être compris par le plus grand nombre. Notre objectif : que tous les protagonistes d'une campagne réussie - au premier rang desquels les entreprises elles-mêmes - comprennent les leviers d'amélioration.

Ce webinaire est constitué :

- 👉 D'une présentation visuelle et synthétique au format Power Point
- 👉 Du document rédigé ci-après (qui constitue en quelque sorte le commentaire de la présentation pour ceux qui n'auraient pas pu assister à une présentation orale)

Les commentaires sont les bienvenus sur le Message Business Center, la communauté des utilisateurs : [www.message-business-center.com](http://www.message-business-center.com).

## **UN VOYAGEUR INTERNATIONAL EN TEMPS DE GUERRE !**

Entre le moment où quelqu'un envoie un [emailing](#) et le moment où son destinataire reçoit le message, le courrier électronique traverse plusieurs systèmes informatiques. Ces systèmes ont notamment pour mission de limiter le volume de Spam, c'est-à-dire de messages non sollicités. Cette lutte contre le Spam est une véritable guerre mondiale avec plusieurs milliards de messages de ce type qui circulent quotidiennement sur Internet : médicaments illicites, sites pornographiques, placements douteux, détournements de fond, virus informatiques... Au-delà de veiller à diminuer l'agacement des destinataires, c'est une lutte légitime pour un Internet plus sécurisé et plus fiable que livrent ses systèmes informatiques.

On peut faire une analogie entre le voyage de ce message et celui d'un voyageur qui voudrait traverser plusieurs pays. Au cours de ce périple, ces systèmes informatiques fonctionnent un peu comme une force de protection à mi chemin entre la Douane, la Police des Aéroports et des Frontières et l'Armée. Cette force de protection peut décider soit de laisser passer l'email et de l'envoyer vers un autre serveur, soit de le bloquer. Dans quel cas l'email n'arrivera peut-être jamais dans la messagerie du destinataire. L'émetteur sera éventuellement averti de cette situation mais - comme nous sommes en temps de guerre - il arrive parfois que le message soit supprimé et que son émetteur ne soit jamais averti de cette disparition.

Quand un voyageur passe la Douane, le douanier vérifie son identité et s'assure qu'il ne transporte rien de suspect sur lui ou dans ses bagages. Il l'interrogera aussi sur l'objet de son déplacement ainsi que les personnes qui vont l'accueillir. Pour résumer, les systèmes informatiques que va traverser le message fonctionnent exactement de la même façon. Ils vérifient la bonne identité des expéditeurs, s'assurent que le contenu de l'email ne soit en rien suspect d'être un Spam, et vérifie que l'email est bien envoyé à une vraie adresse.

### **Rien à déclarer ? Tout est dans le message !**

Avant de suivre notre [emailing](#) dans son périple, nous allons présenter son équipement de voyageur qui sera régulièrement inspecté et surveillé tout au long du voyage.

- ✦ Son passeport : d'où vient-il ? Qui est-il ? Quelle est son origine ?
- ✦ Le contenu de sa valise : c'est-à-dire le fond et la forme du message.
- ✦ Les adresses des personnes qui vont le recevoir : c'est-à-dire la liste des destinataires.
- ✦ La compagnie de transport : c'est-à-dire l'infrastructure du routeur, celle de votre entreprise ou de votre fournisseur d'accès Internet.

Techniquement, un [emailing](#) est donc constitué :

- ✦ D'une liste de destinataires.
- ✦ D'un courrier électronique envoyé à chacun des destinataires. Chaque courrier électronique constitutif de l'[emailing](#) est un fichier dont la structure se découpe en 3 principales parties :
  - L'entête technique du message dont le contenu n'est pas immédiatement visible et qui peut être considéré comme le passeport de l'email. Il contient notamment :
    - L'adresse email du destinataire.
    - L'adresse IP du serveur d'expédition et celui des serveurs relais.
    - Son nom de domaine d'expédition ([@message-business.com](#) par exemple).
    - Dans certains cas, des éléments d'authentification du domaine d'expédition tel sender, return path, Domain Keys ou de gestion des désabonnements (List Subscribe)
  - Le contenu même de l'email
    - Le message lu par les destinataires
      - Le nom de l'expéditeur.
      - L'objet du message.
      - Le rédactionnel.
      - Les images.
      - Le code HTML (qui assemble entre eux le rédactionnel et les images et permet des mises en page attrayantes).
      - Une version sans image dite « version Texte » qui sera affichée si le logiciel de messagerie ne supporte pas la version HTML.
    - Les pièces attachées.

C'est de la qualité de l'ensemble de ces éléments et le respect des bonnes pratiques que nous détaillons ci-dessous que va dépendre la bonne livraison de votre [emailing](#).

## Avant de partir : la check List de l'émailing voyageur

L'équipement de l'émailing voyageur	Où se trouvent ces informations dans l'émailing ?	Qui inspectent l'information et bloquent éventuellement votre message ?
<b>PASSEPORT</b>	Entête technique du message envoyé (« header »)	Serveurs de Mail <ul style="list-style-type: none"> <li>✦ Les serveurs d'envois (de votre entreprise ou de votre fournisseur d'accès)</li> <li>✦ Les serveurs relais sur lesquels vont transiter les messages</li> <li>✦ Les serveurs de réception</li> </ul>
<b>LE CONTENU DE LA VALISE</b>	<ul style="list-style-type: none"> <li>✦ Le message lu par les destinataires</li> <li> <ul style="list-style-type: none"> <li>■ Le nom de l'expéditeur</li> <li>■ L'objet</li> <li>■ Le texte</li> <li>■ Les images</li> <li>■ Le code HTML (qui assemblent entre eux le texte et les images)</li> <li>■ Une version sans image dite « version Texte »</li> </ul> </li> <li>✦ Les pièces attachées éventuelles ou autres fichiers directement joints à votre emailing</li> </ul>	Antispam installés sur <ul style="list-style-type: none"> <li>✦ Les serveurs de réception</li> <li>✦ Les ordinateurs des destinataires</li> </ul>
<b>LES ADRESSES DES PERSONNES QUI ACCUEILLENENT L'émailing (vos destinataires)</b>	Entête technique du message	<ul style="list-style-type: none"> <li>✦ Serveurs d'envois (en fonction du volume envoyé)</li> <li>✦ Serveurs de réception (en fonction du volume reçu et du taux d'adresses défectueuses / NPAI)</li> </ul>

## **DES DESTINATAIRES QUI ACCUEILLENENT LE VOYAGEUR... A BRAS OUVERTS**

Le premier impératif pour s'assurer d'une bonne délivrabilité est d'envoyer ses [emailings](#) à une base de contact « propre ».

Une base est considérée comme « propre » si elle répond à trois critères.

### **Des adresses exactes !**

Tout d'abord, il faut que la base ait été actualisée récemment pour veiller à un minimum de d'adresses NPAI (N'habite Plus à l'Adresse Indiquée). En effet, si le ratio NPAI/emails envoyés est supérieur de 15% (ratio variant selon les serveurs de réception), l'[emailing](#) peut être tout simplement bloqué.

### **Des adresses consentantes !**

Vos destinataires doivent vous accueillir avec le sourire.

Assurez vous de leur consentement ! Ce consentement sera d'une nature différente en fonction du pays d'accueil, du type de communication (fidélisation, prospection) et de la nature de la communication (grand public VS professionnelle). A ce propos nous vous invitons à lire la synthèse « [Prospectez en toute légalité](#) ». Pour l'international, le SNCD a édité un petit guide très synthétique qui résume bien les [enjeux au niveau européen](#).

Inutile de préciser qu'il ne faut pas collecter des adresses email aveuglement sur Internet. Au delà d'un consentement aléatoire, le risque est grand de récupérer des adresses leurres (Spam Trap), c'est-à-dire des adresses dont la seule vocation est de vous identifier comme spammeur. Sur ce sujet vous pouvez consulter le texte de la Loi sur la Confiance en L'Economie Numérique et la position de la CNIL.

De même, il est primordial que le message que vous envoyez suscite l'intérêt des destinataires. En effet, les gens ont tendance à signaler comme Spam tous les messages qui ne les intéressent pas. Si vous avez été signalé trop souvent comme spammeur par vos contacts, les FAI et boîtes de messagerie peuvent décider de refuser tous les envois provenant de votre adresse IP (ou de celles de votre routeur). Il faut savoir qu'une fois blacklisté par les FAI ou les webmails, il est très difficile pour un non-initié de retrouver leurs bonnes grâces.

Stimulez vos contacts régulièrement avec des offres intéressantes en les incitant à inscrire votre adresse d'expéditeur dans leur carnet d'adresses de messagerie électronique.

## Des adresses bien routées !

Il est aujourd'hui vivement recommandé de passer par une infrastructure fiable et professionnelle pour envoyer vos [emailings](#) offrant une bonne qualité de service et de suivi de l'envoi, notamment :

- 🔹 Serveur d'envois (SMTP) haute capacité
- 🔹 Gestion des adresses défectueuses et des retours à l'expéditeur
- 🔹 Authentification de l'émetteur
- 🔹 Déclaration auprès des Webmails et des principaux Fournisseurs d'Accès Internet

En effet, si vous envoyez des emails en masse depuis une simple connexion internet, il y a de forts risques que votre fournisseur d'accès refuse de vous laisser envoyer autant d'emails dans un laps de temps aussi court. Ce refus s'explique autant par des raisons de sécurité que par des motivations commerciales.

Dans ce genre de cas, il est fréquent que l'expéditeur ne soit même pas averti que ses emails n'ont pas été reçus et l'efficacité de votre opération sera nulle. Par ailleurs, vous risquez aussi que vos courriers électroniques personnels soient eux-mêmes bloqués.

## VOS PAPIERS ! L'EMAILING, UN VOYAGEUR À L'IDENTITÉ AUTHENTIFIÉE

Les serveurs relais ou le serveur de réception peuvent identifier l'ordinateur d'expédition grâce à l'adresse IP et le nom de domaine présent dans l'email. Cette adresse IP est l'identité physique de l'émetteur. Chaque machine sur Internet dispose d'une adresse IP unique. Plus l'adresse IP sera authentifiée, reconnue et acceptée, plus votre [emailing](#) aura des chances d'arriver à bon port.

L'intérêt de passer par un routeur professionnel digne de ce nom réside notamment dans le fait que les adresses IP de ses serveurs remplissent le maximum de garantie et ont une identité connue et reconnue par les serveurs destinataires.

Les Spammeurs ayant ainsi intérêt à cacher la réelle provenance des emails qu'ils envoient, la quasi-intégralité des serveurs de réception ont mis en place des dispositifs pour s'assurer de la bonne origine des courriers électroniques. Selon les serveurs, ces procédures sont plus ou moins sophistiquées et prennent plus ou moins de temps. Vous avez beau ne pas être un terroriste, ou un trafiquant de drogue, si vos visas ne sont pas à jour, les douaniers vous empêcheront de traverser la frontière.

C'est la même chose pour un [emailing](#). Même si vous n'avez jamais spammé, si votre [emailing](#) n'est pas doté de ce que l'on pourrait comparer à un passeport électronique avec les visas nécessaires, une partie significative de vos envois risquent de ne pas arriver à destination. Il existe trois principaux types de vérification. Nous allons les examiner de la moins à la plus sophistiquée.

## **Visa n° 1 sur le passeport électronique de l'emailing : Reverse DNS**

Cette première vérification concerne 95 à 99% des serveurs relais.

L'entête du message contient une adresse IP (217.174.192.18 par exemple).

Quand un message arrive, la plupart des serveurs effectuent ce qu'on appelle une requête inverse sur les déclarations DNS. Il existe sur Internet des tables qui mettent en relation des adresses IP à des noms de domaine, les tables DNS. Le référencement sur ces tables peut se faire via son fournisseur d'accès Internet ou par des tiers spécialisés dans ce genre d'enregistrement. Certains fournisseurs d'accès enregistrent de façon dynamique votre adresse IP dans une table DNS lorsque vous effectuez un envoi d'email.

Cependant, la plupart ne le font pas. Il existe des milliers de tables DNS. Les serveurs lancent des requêtes pour vérifier que l'adresse IP correspond à un domaine valide, c'est à dire qu'elle est associée à un nom de domaine, mais pas forcément celui indiqué lors de l'envoi. Si le serveur ne trouve aucune table DNS où apparaît le nom de domaine, l'email sera systématiquement bloqué et les serveurs n'envoient pas nécessairement de message d'erreur à l'expéditeur.

## **Visa n° 2 sur le passeport électronique de l'emailing : Sender Policy Framework**

Cette deuxième vérification concerne 40 % des serveurs relais dans le monde (décembre 2006) et devrait concerner l'ensemble des serveurs prochainement.

Elle est communément appelée SPF (Sender Policy Framework).

Cette vérification fonctionne de la même façon que la première. Le header d'un email contient un nom de domaine et une adresse IP.

Lorsque l'on inscrit son nom de domaine dans une table DNS, on le fait correspondre à une adresse IP. Le SPF consiste donc à vérifier que le nom de domaine correspond bien à l'adresse IP d'expédition sur au moins une table DNS. Cela permet de détecter les expéditeurs qui indiquent un faux email d'expédition (mail from) pour ne pas être traçable.

La conséquence pratique de cette vérification est simple : si vous envoyez un message avec un nom de domaine qui ne correspond pas à l'adresse IP de votre serveur SMTP sur une table

DNS, vos messages seront tout simplement refusés par la majorité des serveurs mondiaux sans que vous en soyez forcément informés.

### **Visa n° 3 sur le passeport électronique de l'emailing : Domain Key**

Ce troisième niveau de sophistication est le plus récent. C'est un peu le passeport biométrique de l'[emailing](#). Il concerne environ 15% des serveurs avec un taux de progression rapide de cet équipement.

Avec Domain Keys, il est désormais possible d'inclure une clé (Domain Key) dans chaque message permettant de garantir message par message, la provenance d'un domaine d'expédition authentique et connu.

### **Autre vérification de l'identité : l'IP Black Listée**

La plupart des serveurs de réception vérifient que l'expéditeur n'a pas été référencé dans une ou plusieurs listes noires de référence où sont inscrites des adresses IP suspectes ou reconnues comme source de spam.

Ces "listes noires" (black lists) sont gérées par des communautés mondiales d'informaticiens qui référencent tous ceux qu'ils ont identifiés comme étant des Spammeurs. Il existe des dizaines de listes noires à travers le monde. La plupart des serveurs interrogent systématiquement ces listes avant de relayer un message.

Si l'expéditeur est identifié comme Spammeur, l'email est refusé. Si le référencement de l'adresse IP d'expédition se trouve être présente par accident sur une de ces listes (dénonciation abusive ou sauvage), un travail de « déréférencement » doit alors être mené, liste par liste pour prouver que l'adresse IP correspond à des serveurs ayant légitimement le droit d'envoyer des [emailings](#).

## LES ANTI-SPAM : OUVREZ VOS BAGAGES

La quasi-totalité des serveurs relais et un nombre croissant de serveurs de réception sont équipés avec des systèmes anti-spam. Le logiciel le plus répandu est Spam Assassin qui est installé sur la plupart de ces machines. Une fois que l'expéditeur a été identifié, le logiciel interroge à nouveau la réputation de l'expéditeur et étudie le contenu du message.

Les serveurs se renseignent sur certaines bases de données pour savoir quelle est la réputation de l'adresse IP d'expédition et celle du nom de domaine. La réputation est elle-même basée sur les anciens comportements de l'expéditeur (mauvaises pratiques, réputation chez les FAI, nombre de plaintes, taux de NPAI...). Il est possible de connaître la réputation de son adresse IP sur de nombreux sites listés en fin de document. Si la réputation est mauvaise, le serveur sera alors bien plus difficile et méticuleux dans la vérification du contenu que si la réputation est excellente.

Le logiciel est également paramétré par défaut pour reconnaître certaines pratiques souvent utilisées par les Spammeurs (certains mots..., certains types de montage HTML, des objets écrits seulement en majuscule...). Pour chaque mauvaise pratique, un nombre de mauvais points est alloué à l'email. Selon le paramétrage de Spam Assassin, si l'email dépasse un certain seuil de points, il sera alors rejeté par le serveur. Un email peut ainsi être relayé par un serveur mais considéré comme un Spam par un autre serveur.

Spam Assassin fonctionne aussi sur le principe de la solidarité entre utilisateurs. Tous les logiciels communiquent entre eux, partagent des informations et effectuent des mises à jour communes pour être plus efficace dans la lutte anti-spam. Il y a donc une évolution permanente de ce qui est considéré ou non comme un Spam par les différents serveurs. Cependant, globalement, il existe quelques dizaines de règles de base à respecter lors de l'élaboration de l'emailing, notamment lors de sa conception graphique et de son montage HTML, pour avoir de grandes chances de ne pas être considéré comme spammeur par Spam Assassin.

### L'objet : votre déclaration d'entrée sur le territoire

Dans l'objet de votre message proscrivez :

- ✦ Les objets vides
- ✦ Un objet uniquement en majuscule (Ex : OFFRE PROMOTIONNELLE)
- ✦ Les signes « ! », « % » ou « / » répétés plusieurs fois
- ✦ Les signes € ou \$
- ✦ Les répétitions de mot
- ✦ Les mots coupés par des points ou les mots espacés avec de nombreux espaces.
- ✦ Les mots à caractère sexuel
- ✦ L'adresse email de l'internaute dans le sujet
- ✦ Les chiffres en début ou en fin de sujet
- ✦ Les termes associés à la gratuité, aux régimes aminçissants, ...

## Ce qu'il faut mettre et ce qu'il ne faut pas mettre dans vos bagages

### A évitez !

- ✦ L'image unique
- ✦ Trop d'images pour pas assez de textes
- ✦ Trop de textes dans le code alternatif aux images (qui s'affiche quand les images ne sont pas chargées)
- ✦ Un grand pourcentage de lignes vides
- ✦ La vidéo dans le corps du message
- ✦ Les formulaires et le JavaScript
- ✦ Les tableaux imbriqués
- ✦ Les commentaires dans le code
- ✦ Le flash et les iframe
- ✦ Le tag <TBODY>
- ✦ Les balises <DIV>
- ✦ Les appels à des styles hébergés ailleurs ou déclarés en début de mail
- ✦ Les contenus HTML trop courts
- ✦ Une taille de police soit trop petite, soit trop grande
- ✦ Le flag de priorité mis à « importance haute »
- ✦ Les pièces attachées
- ✦ Une couleur de police proche de celle du fond
- ✦ Les tailles négatives dans les attributs de la balise « <FONT> »

### A conseiller

- ✦ Un équilibre à 50 / 50 entre le texte et l'image
- ✦ Des textes courts alternatifs aux images (balise Alt)
- ✦ Un code HTML ne faisant pas appel à des styles hébergés en dehors du mail ou déclarés en début de mail
- ✦ Pas de formulaires dans votre mail
- ✦ Des liens vers les pièces attachées plutôt que les pièces attachées (en plus ce sera plus facile d'en mesurer la consultation)
- ✦ Un objet en minuscule sans exclamation
- ✦ Une version texte
- ✦ Code HTML avec <TR> et <TD> uniquement

## Retenez votre chance en cas d'échec

Les logiciels antispam analysent également si suite à un échec de livraison (boîte aux lettres pleine, demande de renvois ultérieurs...), l'expéditeur réessaie d'envoyer l'email, car habituellement les spammeurs ne retiennent jamais. Il est donc important de s'appuyer sur une solution de routage professionnelle qui gère les tentatives de renvois automatiques de votre message.

## Les Webmail : des millions de douaniers

Les serveurs des principales messageries (Hotmail, gmail, Yahoo mail...) fonctionnent d'une façon un peu particulière. Si un trop grand nombre d'utilisateurs signale un expéditeur comme spammeur, alors, de façon automatisée, les serveurs sanctionnent l'expéditeur. Les sanctions varient selon les messageries. Cela peut aller d'une réduction du flux d'entrée (nombre d'emails acceptés provenant d'une même adresse IP), un blocage temporaire des emails, une demande d'envoi ultérieur jusqu'à un refus pur et simple de recevoir tout email provenant de ce nom de domaine ou cette adresse IP. L'ancienneté de l'adresse IP est aussi très importante. Si une messagerie comme Hotmail reçoit un nombre d'email trop important d'une adresse IP qui n'avait jusqu'alors envoyé aucun message, elle ne laisse alors rien passer car les risques d'être

confronté à un spammeur sont alors trop importants. L'enjeu pour un routeur professionnel est donc d'être au maximum en relation avec les responsables techniques de ces messageries pour éviter que leur nom de domaine ou leur adresse IP subissent des sanctions et faire en sorte d'être considéré comme un routeur « propre » pour atteindre une délivrabilité optimale.

A cela, il faut ajouter les anti-spam installés chez le destinataire. Il existe des anti-spam intégrés comme ceux sur Outlook, d'autres sont installables sur une machine lambda pour n'importe quelle messagerie.

Ces anti-Spam sont paramétrables selon les goûts de chacun (Refus de certains mots clés, de certains formats). Il existe un nombre illimité de paramétrage anti-spam, voilà pourquoi il est en réalité impossible d'atteindre une délivrabilité parfaite.

## **POUR RÉSUMER : LES 8 COMMANDEMENTS DE LA DÉLIVRABILITÉ**

- 1. Ma base d'adresses je stimulerai et mettrai à jour régulièrement**
- 2. De ma base je proscrirai les adresses douteuses ou non consentantes**
- 3. À mes nouvelles adresses je conseillerai de mettre l'email émettrice dans leur carnet d'adresses**
- 4. Mes messages, j'en soignerai le fond**
- 5. Mes messages, j'en soignerai la forme**
- 6. Mes messages, en html spécial emailing, je les intégrerai**
- 7. Mes messages, j'en vérifierai l'objet**
- 8. Via une plate-forme de routage fiable j'effectuerai mes envois**

## **ALLER PLUS LOIN : QUELQUES SOURCES D'INFORMATION**

### Normes

<http://www.faqs.org/rfcs/rfc1891.html>

<http://antispam.yahoo.com/domainkeys>

### Les recommandations de la CNIL sur la prospection électronique

<http://www.cnil.fr/index.php?id=1280>

### Les principales dispositions de la Loi sur la Confiance en l'Economie Numérique

[http://www.internet.gouv.fr/information/information/dossiers/loi-pour-confiance-dans-economie-numerique-len/les-principales-dispositions-len-41.html?var\\_recherche=LCEN](http://www.internet.gouv.fr/information/information/dossiers/loi-pour-confiance-dans-economie-numerique-len/les-principales-dispositions-len-41.html?var_recherche=LCEN)

### Le guide SNCD sur l'emailing en Europe

[http://www.sncd.org/guide\\_europe.php](http://www.sncd.org/guide_europe.php)

### Informations générales sur l'email, l'emailing et le e-marketing

<http://pignonsurmail.typepad.fr/>

<http://www.arobase.org/>

<http://www.abc-netmarketing.com/>

<http://emailing.typepad.fr/snipemail/>

<http://www.message-business-center.com/>

### Vérification de la réputation des adresses IP

<http://openrbl.org/>

[http://www.completewhois.com/cgi2/rbl\\_lookup.cgi?](http://www.completewhois.com/cgi2/rbl_lookup.cgi?)

<http://www.dnsbl.info/advanced.asp?>

<http://www.dnsbl.info/advanced.asp?>

<http://senderid.returnpath.net/how.php>

<http://vweb.nass.com.au/cgi-bin/dnslookup?>

[http://www.sendmail.com/sm/resources/tools/ip\\_reputation/](http://www.sendmail.com/sm/resources/tools/ip_reputation/)

## **DANS LES PROCHAINES EDITIONS DE « SUR LE FRONT »**

N°2 (décembre) : les bonnes pratiques de l'emailing : cibles, fond, forme, messages, méthodes...

## A PROPOS DE MESSAGE BUSINESS

### Le premier Libre Service du Marketing Électronique

(plate-forme logicielle hébergée sur Internet / Software As A Service)

- |   |  |
|---|--|
| <input type="checkbox"/> emailing         | <input type="checkbox"/> Location fichiers |
| <input type="checkbox"/> SMS              | <input type="checkbox"/> Enquête en ligne  |
| <input type="checkbox"/> Formulaires Web  | <input type="checkbox"/> RSS               |
| <input type="checkbox"/> Gestion contacts | <input type="checkbox"/> Blog              |

### 400 entreprises utilisatrices (octobre 2007)

### Une plate-forme novatrice récompensée et reconnue par:

- OSEO Anvar / Région Ile de France / Paris Développement
- Lauréat 2007 de Paris-Entreprendre
- Sélectionnée par Microsoft dans le cadre de son programme IDEES de soutien aux entreprises les plus innovantes du secteur du logiciel.

### Membre actif d'interprofessions motrices : SNCD / FING / AFDE

### Plus d'information sur [www.messagebusiness.com](http://www.messagebusiness.com) ou 0811 90 11 33

## DÉCOUVRIR MESSAGE BUSINESS ?

**Offre découverte 0€**  
**500 Emailings, 10 SMS, 1 Blog**  
**et 1 formulaire**

Testez Gratuitement et sans engagement notre solution d'emailing et d'envoi de newsletter maintenant.

Vous bénéficierez ainsi d'une période d'essai de deux mois . Pour Cela , il vous suffit de vous inscrire et vous pourrez utiliser notre plate-forme dans quelques secondes.

**Testez-nous**