

Optimiser la délivrabilité de vos e-mailings

LIVRE BLANC

Co-écrit avec Guillaume Fleureau



Sarbacane
SOFTWARE

Sommaire

Edito	5
Introduction	7
Contexte de l'e-mail marketing aujourd'hui	7
Comprendre les enjeux de la délivrabilité	9
Qu'est-ce que la délivrabilité ?	9
Objectifs et enjeux	10
Bien gérer sa base de contacts	11
Optimiser la collecte	11
Nettoyage de la base	13
Désabonnements et gestion des plaintes	13
NPAI et BOUNCES	16
Spamtraps	17
Utiliser une structure de routage professionnelle	19
Authentification des messages	19
Boucles de rétroaction	21
Gestion de votre e-réputation	22
Bonnes pratiques pour une meilleure délivrabilité	23
Choix des objets	23
Formats	24
Personnalisation des liens et du contenu	25
Bonnes pratiques de conception HTML	27
Gestion des images	27
Lien vers copie web	29
Utiliser l'inline CSS	29
Eviter les balises multimédia	30
Simplifier et nettoyer le code HTML	30
Liens	31
Tests de réception	31
E-mail rendering	33
Gestion de la fréquence d'envoi	33
Gestion des volumes d'envoi	34
Sarbacane et la délivrabilité	35
Présentation de Sarbacane	35
Une infrastructure professionnelle	36
Des traitements manuels pour plus de garanties	37
Sarbacane innove pour optimiser la délivrabilité	38
Conclusion	39



Mathieu Tarnus,

Directeur Général
de la société
Sarbacane Software

Edito

“Concevoir et envoyer un e-mailing a fortement évolué depuis le début des années 2000. Autrefois un outil de communication de masse, l’e-mail marketing s’est professionnalisé et a du s’adapter à un nouveau contexte de marché : surabondance d’envois d’e-mails, durcissement des règles de filtres antispam, mauvaise interprétation de la part des internautes du spam du message à caractère commercial non sollicité...”

Aujourd’hui, Il ne suffit plus de cliquer sur le bouton “envoi” pour que les messages aboutissent. La délivrabilité est devenue l’enjeu numéro un pour tous les professionnels du marketing et de la communication désireux de communiquer avec leur cible via le canal e-mail. La délivrabilité d’une campagne e-mailing commence désormais dès la réflexion, avant l’envoi définitif du message. Il s’agit aujourd’hui de cibler au maximum ses campagnes, nettoyer sa base, gérer habilement les désabonnements, concevoir son message selon certains gabarits, tester avant d’envoyer et surtout, rentrer dans l’esprit du destinataire afin de savoir comment le message que l’on envoie va être perçu par ce dernier.

Oui, l’e-mailing a plus qu’évolué, il s’est transformé en un véritable outil professionnel de communication directe. Les acteurs, dont Sarbacane fait partie, se doivent de prendre en compte ces enjeux dans leur offre logicielle et d’aiguiller au maximum leurs clients. C’est une chose que nous essayons de réaliser à travers ce livre blanc, qui a pour but de faire comprendre le cheminement d’un message entre son envoi et sa réception en boîte aux lettres, et aussi donner toutes les clés pour optimiser sa campagne afin qu’elle aboutisse en boîte de réception et qu’elle ne soit pas bloquée en tant que spam.

L’e-mailing a encore un bel avenir devant lui et les pratiques énoncées dans ce livre devraient lui permettre de rester un outil de communication et de marketing percutant et réactif !”

Introduction

CONTEXTE DE L'E-MAIL MARKETING AUJOURD'HUI

L'e-mail marketing est un outil de communication directe réactif caractérisé par son coût extrêmement faible et sa simplicité d'utilisation. Appelé également e-mailing, il s'adapte à tout type de communication, commerciale ou informative, et est un canal de communication efficace très plébiscité par les petites comme les grandes entreprises. Qu'il s'agisse d'acquérir de nouveaux clients, de les fidéliser ou d'augmenter les ventes, l'e-mail marketing suscite un intérêt croissant.

Mais de nos jours, les utilisateurs de ce moyen de communication doivent faire face à de nouveaux leviers de décisions d'ordres technique et marketing qui dépassent la simple action d'envoyer un message : rendu des e-mails (e-mail rendering), interaction avec les réseaux sociaux ou encore prise en compte des webphones. L'e-mail marketing nécessite une expertise pointue pour assurer de bonnes conditions de réception.

De plus, les fournisseurs d'accès internet tiennent un rôle indispensable : maintenir une protection anti-spam efficace afin de satisfaire leurs utilisateurs. Mais dans le même temps, les entreprises utilisant l'e-mail marketing ont un objectif : délivrer leurs messages dans les boîtes de réception de leurs destinataires. Dans ce contexte où le spam ne cesse de croître, où la publicité par e-mail est devenue légion, un nouvel enjeu est au cœur de toutes les préoccupations : la délivrabilité !

L'objectif de ce livre blanc est de vous aider à comprendre les enjeux de la délivrabilité des e-mails et les solutions pour parvenir à délivrer correctement vos campagnes d'e-mail marketing.

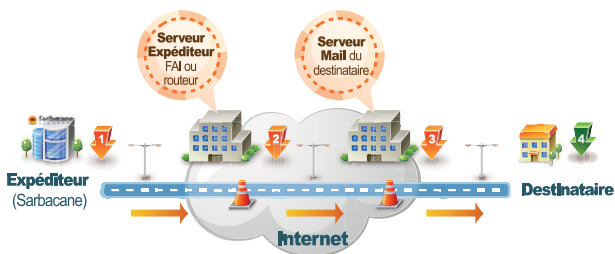
Comprendre les enjeux de la délivrabilité

QU'EST-CE QUE LA DÉLIVRABILITÉ ?

Il s'agit de la capacité à faire parvenir à ses destinataires des campagnes e-mailing en boîtes de réception.

La délivrabilité consistait à l'origine à s'assurer que les messages soient bien "acceptés" par les fournisseurs de messagerie. La délivrabilité était mesurée seulement grâce à l'analyse des bounces (ou NPAI), ces messages d'erreurs renvoyés pour cause par exemple d'adresses e-mails erronées ou de boîtes pleines.

Face à l'augmentation du spam, les fournisseurs de messageries ont renforcé leur politique de filtrage anti-spam et ont ajouté de nouvelles règles de "bonnes conduites" à respecter qui contraignent les émetteurs d'e-mailings à optimiser leurs envois et cela même pour ceux qui envoient pourtant des e-mails "légitimes". Dans ce contexte, les entreprises doivent mettre en œuvre des bonnes pratiques et utiliser des infrastructures professionnelles pour assurer une bonne délivrabilité de leurs messages afin que ces derniers arrivent directement dans les boîtes de réception de leurs destinataires.



LE TRAJET D'UN E-MAIL

OBJECTIFS ET ENJEUX

L'envoi d'e-mailings en masse est devenu un moyen de communiquer prisé de part son aspect économique et rapide. Mais le renforcement des règles de filtrage de la part des éditeurs de solutions anti-spam a rendu cette manière de communiquer complexe à gérer. Les acteurs du marché de l'e-mailing prennent au sérieux ce phénomène car il peut engendrer une perte de chiffre d'affaires, de rentabilité et même d'insatisfaction des destinataires.

Derrière le mot "délivrabilité" se cachent d'autres enjeux, notamment celui de l'e-réputation, la réputation d'une organisation qui expédie des e-mails.

L'e-réputation est étroitement liée à la proportion des e-mails envoyés par un émetteur qui sont considérés comme des spams suite au passage dans des filtres automatiques ou aux déclarations des destinataires. L'e-réputation indique le niveau de confiance accordé à l'entreprise expédiant les e-mails et permet, si celle-ci est bonne, d'assurer une délivrabilité optimale.

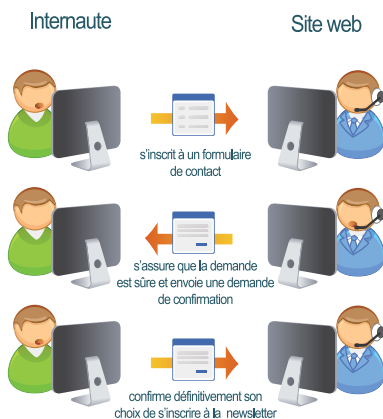
Une bonne délivrabilité est ainsi devenue un enjeu majeur pour réussir son marketing par e-mail. Mais pour l'optimiser, il est important de prendre en compte les deux formes de délivrabilité : celle que vous pouvez améliorer vous-même dans le travail de vos campagnes et celle dépendant de règles technologiques mises en œuvre par le routeur professionnel. Plusieurs bonnes pratiques aujourd'hui éprouvées permettent d'y parvenir. Découvrons-les à travers ce livre blanc.

Bien gérer sa base de contacts

OPTIMISER LA COLLECTE

La méthode de collecte des adresses e-mails constituant la base des destinataires est déterminante pour la délivrabilité. Il est donc essentiel de bien maîtriser les sources de recueil des adresses e-mails.

Pour optimiser votre délivrabilité, choisissez plutôt de collecter des adresses opt-in. On parle d'une adresse e-mail opt-in quand son propriétaire a donné son accord explicite à une organisation pour que cette dernière lui envoie des offres commerciales ou des informations à cette adresse.



PRINCIPE DU DOUBLE OPT-IN

Lors de la collecte d'e-mails, il est donc important de vous assurer du consentement à l'aide par exemple d'une case à cocher dans vos formulaires. D'autre part, n'oubliez pas de mettre en place des contrôles de saisie. Le plus souvent, les formulaires contiennent des contrôles qui vérifient la présence d'un @ et d'un point dans l'adresse. Ceci vous évitera d'importer des adresses erronées. Mais pour être certain de ne recueillir que des adresses e-mail correctes, il existe une méthode de collecte appelé "double opt-in".

Il s'agit d'une technique qui vous assure que les adresses e-mail sont réelles et que les propriétaires de ces adresses sont bien à l'origine de la saisie. Le double opt-in consiste à demander une confirmation à l'internaute par e-mail. Après la saisie de son adresse e-mail sur une page web, l'internaute reçoit un message automatique contenant un lien d'activation sur lequel il faut cliquer pour rendre l'inscription valide. Même si cette méthode vous garantit un taux de NPAI très faible, envoyer un e-mail de confirmation a un double effet : le message risque d'être noyé dans la masse des e-mails reçus au quotidien et donc supprimé, survolé, voire oublié... Vous aurez donc moins d'inscrits à votre liste mais une meilleure qualité en contrepartie.

D'un point de vue juridique, on retiendra qu'une communication à destination de particuliers nécessite leur consentement préalable (opt-in). Pour les communications à destination de professionnels le consentement préalable n'est pas obligatoire (opt-out), sauf si la communication vise directement ou indirectement une personne physique et que l'objet du mail n'a aucun lien avec le domaine d'activité de la dite personne. Enfin quel que soit le contexte, la loi impose le droit d'opposition des destinataires par une méthode automatisée, généralement, celle-ci se matérialise par un lien de désinscription dans le corps du message.

Certains prestataires proposent la vente de fichiers d'e-mails dits opt-in. L'achat de ce type de listes n'est pas recommandé car elles sont souvent issues de sources douteuses ou obsolètes. Concrètement, beaucoup de ces e-mails ne seront plus valides, voire utilisés comme spamtrap ou piège à pub (sujet traité en page 17). De plus, vos performances seront très faibles car ces personnes n'ont jamais demandé à recevoir explicitement les messages de votre organisation en particulier. Pire, la délivrabilité sur ce type de campagnes sera désastreuse compte tenu de la piètre qualité des adresses.

Il est important de rappeler que la qualité d'une base de contacts est bien plus importante que la seule quantité. Collecter des e-mails sans obtenir le consentement ne pourra que nuire aux performances. Un envoi non sollicité peut être très négatif sur l'image et l'internaute n'hésitera pas à considérer l'expéditeur comme spammeur.

Nettoyage de la base

DÉSABONNEMENTS ET GESTION DES PLAINTES

Bien gérer les désabonnements est indispensable pour accroître la délivrabilité de ses campagnes, et ce pour plusieurs raisons. Tout d'abord pour éviter les plaintes. En effet, si le désabonnement est inopérant ou fastidieux, les destinataires désireux de se désabonner chercheront d'autres façons de ne plus recevoir les

e-mailings. Ainsi, l'usage du bouton "Ceci est un spam" est bien souvent utilisé si le désabonnement n'est pas facilité. Si trop de destinataires agissent de la sorte, il y a de fortes chances pour que votre message arrive ensuite automatiquement dans le dossier des courriers indésirables. Si les clics sur le bouton «ceci est un spam» dépassent un certain seuil, le domaine de l'expéditeur peut être considéré comme spammeur par le fournisseur de messagerie.



Il existe plusieurs motivations qui peuvent justifier que les destinataires souhaitent se désabonner. Il est très important de les laisser libres de le faire par le biais d'un processus de désabonnement simple et efficace.

Les lecteurs ont parfois tendance à oublier pour quelle raison ils reçoivent vos messages. Ajoutez une ou deux phrases au début de votre contenu pour indiquer aux abonnés pourquoi ils sont abonnés à votre mailing-list. N'hésitez pas à placer votre lien de désabonnement au début de votre message afin de le rendre suffisamment visible. Par exemple, il est judicieux de placer une phrase de ce type au début du message : "Vous recevez ce message parce que vous vous êtes abonné à..."

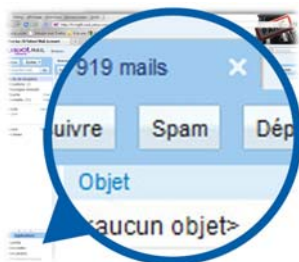
Si vous souhaitez vous désabonner suivez ce lien". Si le destinataire ne veut plus recevoir d'informations de votre part, il peut ainsi facilement annuler son inscription au lieu de cliquer sur le bouton SPAM. Le lien de désabonnement doit être facile à utiliser. On devrait pouvoir se désabonner en deux clics maximum. Si vous en avez la possibilité, profitez-en pour recueillir les raisons du désabonnement via une liste à choix multiples sur la page de confirmation.

Vous pouvez aussi proposer de réduire la fréquence d'envoi si vous êtes ensuite capable de gérer cette préférence.

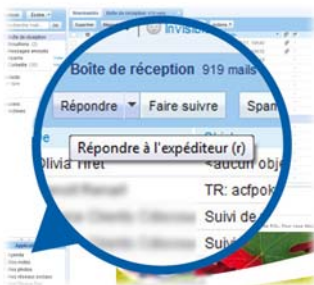
D'autre part, vérifiez toujours que le lien de désabonnement fonctionne et désabonne bien ceux qui le souhaitent. Si vous n'êtes pas équipé d'un système automatique de désabonnement, pensez à bien nettoyer votre base régulièrement suite à ces demandes. Sinon, le bouton SPAM sera utilisé comme dernier recours pour ne plus recevoir vos messages. Et puis, vous l'avez peut-être déjà vécu, rien n'est plus énervant qu'un lien de désabonnement erroné ou inefficace.

Par ailleurs, les destinataires peuvent se plaindre de diverses façons s'ils se sentent victimes de spam par exemple :

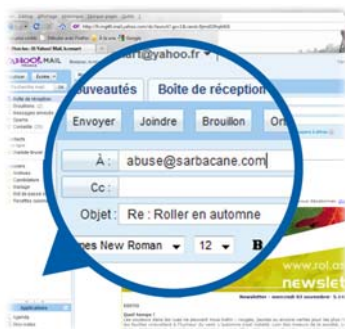
- Par un clic sur le bouton de déclaration en spam. Dans ce cas, il faut pouvoir recueillir les plaintes via les boucles de rétroaction (sujet traité page 21),



- Par l'envoi d'un message envoyé à l'adresse de réponse du message (reply-to). Il faut donc relever cette boîte afin de pouvoir éventuellement désabonner les plaignants.



- Un message envoyé aux adresses anti-abuse «abuse@sarbacane.com» ou «abuse@orange.fr» par exemple. Ici, c'est le routeur ou le webmail qui mènera des actions auprès de l'expéditeur.



Bien gérer les plaintes permet d'avoir un retour sur ses envois. Si vous constatez des pics de plaintes, il vous faudra analyser les raisons du mécontentement : augmentation de la fréquence d'envoi, contenu inadapté à la cible, import de nouveaux contacts dans la base, etc.

NPAI ET BOUNCES

La gestion des NPAI (N'habite Pas à l'Adresse Indiquée - c'est-à-dire les adresses qui n'existent pas ou plus) est très importante pour la délivrabilité. Ces adresses non valides, si elles sont trop nombreuses dans une base, expliquent parfois des ralentissements lors des envois et peuvent engendrer un blocage de l'émetteur chez certains FAI et webmails : c'est ce qu'on appelle le blacklistage. En effet, lorsqu'un expéditeur envoie des e-mails, il génère des erreurs pour chaque message non remis, appelées Bounces. Ces erreurs sont traitées par les messageries qui peuvent alors bloquer vos envois si vous en encombrez trop les serveurs avec beaucoup de Bounces. Il convient donc de soigner l'hygiène de sa base par des actions de nettoyage après chaque envoi car plus le taux de NPAI est élevé, plus le risque de blacklistage augmente.

On distingue différents types d'erreurs :

- 1/ **Les Hard Bounces** : messages d'erreurs définitifs qui indiquent que l'utilisateur sur ce nom de domaine n'existe pas ou plus. La recommandation sur le traitement à appliquer à ce type d'erreur est de supprimer les adresses de la base de données dès le premier retour.
- 2/ **Les Soft Bounces** : messages d'erreurs temporaires de type «boîte pleine» par exemple ; il faut pouvoir se redonner la possibilité d'écrire à nouveau à cette adresse. Il est conseillé de regarder régulièrement les Soft Bounces de façon à vérifier qu'il n'en reste pas un indéfiniment.
- 3/ **Les SpamFilter Bounces** : correspondent aux erreurs de rejets pour des problèmes de réputation de l'adresse IP émettrice. Les messages retournés dans ce cas sont souvent très explicites : rejet pour raison de blacklistage, rejet pour cause de contenu inapproprié, rejet pour problèmes de plaintes... Autant de raisons qui montrent des problèmes de mauvaise hygiène de base, de messages considérés comme indésirables (soit par le système de filtrage, soit par les remontées des internautes). Ce type de retour identifiant des problèmes doit donner lieu à des actions pour les résoudre.

Il est important de préciser qu'une livraison du message dans le dossier "spam" n'est pas considérée comme un Bounce.

Il est très rare de ne pas générer de Bounces lors d'un envoi. Pour minimiser les erreurs, il faut agir dès la collecte des données. Le double opt-in, dans le cas des collectes en ligne, est une bonne solution pour éviter les Hard Bounces. D'autre part, vous pouvez également tenter de corriger des adresses e-mail erronées pour faute de frappe. Outre la présence évidente du @ et du . dans l'adresse e-mail, il peut être bénéfique de corriger les noms de domaine connus (yaho.fr devient yahoo.fr par exemple). Suite à l'envoi de votre campagne, il est nécessaire de mettre à jour les adresses mail dès réception de message, comme un changement d'adresse ou de poste.



SPAMTRAPS

Les spamtraps (piège à spam aussi appelé honeypot) sont des adresses e-mail spécialement créées dans le but d'attirer des messages non-sollicités. Ces boîtes de réception sont détenues par les fournisseurs de messagerie ou éditeurs antispam et ont pour but de piéger les expéditeurs de spams. Ces adresses n'ayant jamais été inscrites à des listes d'envoi, tous les messages reçus sont par conséquent des spams.

Une fois les adresses mails factices créées, les spamtraps sont diffusés discrètement sur le web. Les spambots (systèmes collectant automatiquement les adresses e-mail sur la toile) utilisés par les spammeurs, aspirent ces adresses sans se douter du piège. Quand des spams seront reçus dans les adresses pièges, les solutions antispam analysent leur nombre et déclenchent plus ou moins automatiquement des options visant à blacklister l'expéditeur.

Soyez vigilant lors de l'acquisition de certaines listes d'adresses à bas prix collectées sauvagement sur Internet, qui contiennent parfois des spamtraps et peuvent donc nuire à votre délivrabilité.

Utiliser une structure de routage professionnelle



AUTHENTIFICATION DES MESSAGES

L'authentification regroupe plusieurs méthodes utilisées par les fournisseurs de messagerie pour vérifier l'identité de l'expéditeur d'un e-mail. L'authentification permet aux FAI et aux webmails de lutter principalement contre le spam et le phishing et permet aux expéditeurs de prouver qu'ils sont bien ceux qu'ils prétendent être.

Il existe différents systèmes d'authentification : SPF, DKIM et SenderID. De plus en plus de fournisseurs de messagerie, en particulier les principaux Webmails tels que Yahoo, Hotmail ou Gmail, incitent les expéditeurs à authentifier leurs envois via ces moyens. En utilisant l'authentification, vos envois ont une meilleure chance de parvenir à vos destinataires. De plus, certains fournisseurs tels que Yahoo ou Hotmail apposent une petite icône dans votre message indiquant au destinataire que vous êtes un expéditeur authentifié. Ceci améliore la confiance et peut influencer les taux d'ouverture de vos messages.

Il est important de préciser que l'authentification ne garantit pas la délivrabilité de vos messages. Elle contribue à son amélioration mais ne dispense pas d'autres optimisations essentielles décrites dans ce livre blanc.

Les fournisseurs de messageries proposent deux principales techniques d'authentification : la solution IP utilisée par les technologies SPF (Sender Policy Framework) et Sender ID, et la signature cryptographique utilisée par la technologie DKIM (Domain Keys Identified Mail).



Les technologies SPF et Sender ID nécessitent de déclarer les serveurs autorisés à envoyer des e-mails pour un domaine donné, et ce depuis la zone DNS. Aucune signature numérique ou de clé privée sur vos infrastructures n'est requise, une simple déclaration DNS de type TXT permet d'autoriser une machine à émettre du courrier pour votre domaine d'expédition.

La technologie DKIM fonctionne quant à elle par signature cryptographique, permettant à un domaine d'authentifier le début du message dans le flux du courrier. Comme son nom l'indique, ce sont des clés rattachées à des domaines d'expédition. Une clé correspond à un domaine d'expédition. Lorsque le serveur de messagerie envoie un e-mail, il signe son message avec la clé privée faisant référence au domaine d'expédition. Une clé publique est disponible (déclaration DNS), et permet de vérifier que la clé privée est correcte. Il y a donc deux clés, l'une privée sur le serveur expéditeur, et l'autre publique accessible à tous. L'une ne peut fonctionner sans l'autre. Ce processus d'envoi garantit le fait que le serveur de messagerie est bien autorisé à envoyer des courriers pour le domaine signé en question. Et à l'inverse, si quelqu'un essaie d'envoyer des campagnes avec un domaine ne lui appartenant pas, son accès sera refusé par les infrastructures destinataires utilisant cette norme, ou à défaut il subira une très mauvaise délivrabilité.

Qu'est ce que le DNS ?

Le DNS est un service administré en cascade par les institutions de l'Internet. Véritable carte d'identité, il définit l'ensemble des informations rattachées à un nom de domaine, comme l'adresse IP de son ou ses site(s) web, les adresses IP des serveurs de messagerie, les éventuelles clés de décryptage (DKIM) etc.

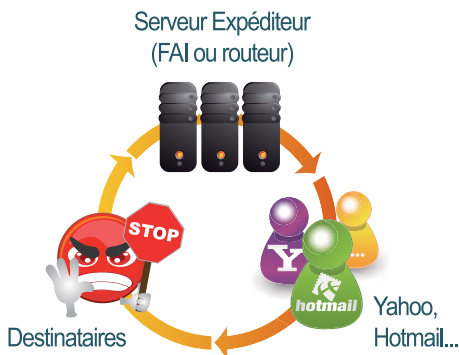
Les informations contenues dans le DNS sont publiques et gérées de manière hiérarchique par des serveurs dans le monde entier. Chaque serveur dispose d'un cache limité dans le temps. Lors d'une requête sur un nom de domaine, le serveur le plus proche de la requête (généralement celui du fournisseur d'accès de l'intéressé) vérifient s'il a les informations dans son cache, à défaut, il sollicite un serveur hiérarchiquement supérieur et ainsi de suite tant que ces informations ne sont pas connues. Une fois les informations obtenues, chaque serveur sollicité les enregistre dans son propre cache. Cette architecture garantit au réseau Internet une certaine continuité dans la résolution des noms de domaine, quelque soit la position de l'internaute et des machines hébergeant les services d'un nom de domaine.

BOUCLES DE RÉTROACTION

Les fournisseurs de messagerie ont donné le pouvoir à leurs utilisateurs en mettant à leur disposition un bouton permettant de signaler un message reçu comme SPAM. Ce bouton permet aux fournisseurs d'analyser et de mémoriser les plaintes afin d'améliorer leur service de filtrage.

Certains fournisseurs, dont Yahoo et Hotmail, ont mis en place des boucles de rétroaction. Elles servent à transmettre aux expéditeurs les plaintes afin qu'ils suppriment les adresses concernées des futurs envois. Pour recevoir les plaintes, il suffit à l'expéditeur de s'inscrire gratuitement pour recevoir les rapports.

Les boucles de rétroaction donnent aux expéditeurs la possibilité d'améliorer la qualité de leur contenu et contribuent à identifier les problèmes potentiels liés aux contenus envoyés, sources d'insatisfaction. Les destinataires ont de plus en plus tendance à cliquer directement sur ce type de bouton plutôt qu'à chercher le lien de désinscription. Il est donc primordial de prendre en compte ces boucles de rétroaction afin d'éviter le blacklistage. Le rôle du routeur professionnel est de gérer, pour ses domaines d'expédition, ces différentes boucles de rétroaction, soit en prenant des initiatives, soit en vous remontant les informations.



FONCTIONNEMENT DE LA BOUCLE DE RÉTROACTION

GESTION DE VOTRE E-RÉPUTATION

L'e-réputation est un élément clé dans la délivrabilité. Les fournisseurs de messagerie analysent la réputation des serveurs utilisés pour tous les envois vers leur service et attribuent un score à chacun de ces serveurs identifiés grâce à leur adresse IP. Grâce à ce score, ils jugent de la nature du message : e-mail légitime ou SPAM.

Il est donc important d'utiliser un service de routage professionnel disposant de serveurs d'envois de bonne réputation auprès des fournisseurs de messagerie. Les routeurs reconnus entretiennent habituellement des relations d'échange avec les fournisseurs de messagerie qui les identifient comme légitimes.

Par ailleurs, les liens présents dans l'e-mail sont également un élément à la e-reputation. Les liens trackés sont en effet souvent identiques pour tous les expéditeurs d'un même routeur. La personnalisation des liens est une bonne solution pour éviter de voir sa campagne non délivrée à cause de liens souffrant de mauvaise réputation. (Sujet traité page 25).

Bonnes pratiques pour une meilleure délivrabilité



CHOIX DES OBJETS

Le choix des objets est non seulement important pour obtenir de bonnes performances marketing, mais il est également déterminant pour la délivrabilité. En effet, les filtres anti-spam sont très exigeants sur le contenu des objets et ne pardonnent aucune erreur. Voyons quelques recommandations pour contourner ces filtres sans risques.

- Ne jamais envoyer une campagne avec un objet vide
- Ne pas employer de majuscules sur des mots entiers (exemple : DES PRIX INCROYABLES !)
- Ne pas abuser de la ponctuation et particulièrement des points d'interrogation et d'exclamation. Les filtres durcissent les règles en écartant parfois les envois contenant un seul point d'exclamation dans l'objet.
- Ne pas répéter plusieurs fois les mêmes mots dans l'objet
- Ne pas espacer les mots de l'objet déraisonnablement
- Eviter l'emploi des caractères spéciaux tels que % ou .
- Proscrire les spam words tels que : GRATUIT, CREDIT, CLIQUEZ... Les envois ayant pour thème l'argent, le sexe, les médicaments ou les jeux sont les plus sensibles. Soyez vigilants sur les termes à employer avec ces thèmes.



Notez que le choix des objets n'est pas une science exacte. La meilleure façon de s'assurer que l'objet ne posera pas de problèmes de réception est de tester des envois sur les principaux logiciels de messageries et webmails avant la diffusion.

FORMATS

Il existe deux formats pour la composition des e-mailings : le texte brut ou le HTML. Le format HTML donne la possibilité de mettre en forme le message en utilisant des styles (couleurs, polices...) et en insérant des images et des animations. Le format texte brut est quant à lui dépourvu de mise en forme et de créativité.

La plupart des e-mailings commerciaux sont aujourd'hui construits en HTML. Mais le format texte brut reste encore utilisé lorsqu'il n'est pas nécessaire d'embellir le message. Il est plus souvent utilisé par le secteur BtoB. Le texte brut offre un taux optimal de délivrabilité : très légers, ces messages sont plus faciles à analyser par les filtres antispam et s'affichent correctement sur toutes les messageries, contrairement au HTML qui pose parfois problème.

Face à ce dilemme, il existe une solution : le multipart. C'est une technique permettant d'insérer dans votre envoi un message au format HTML et en texte brut. C'est ensuite la messagerie du destinataire qui déterminera quel format afficher. Dans la plupart des cas, le format HTML sera lisible mais certains logiciels de messagerie utilisés en milieu professionnel ou encore sur les téléphones mobiles ne supportent pas le HTML.

D'autre part, sachez qu'on enregistre habituellement l'ouverture du message grâce au chargement d'une petite image invisible. Les images n'étant pas supportées par le format texte brut, l'information de l'ouverture de l'e-mail ne peut pas être collectée. Seul le format HTML permet d'obtenir le taux d'ouverture d'une campagne.

PERSONNALISATION DES LIENS ET DU CONTENU

La personnalisation des e-mails est un atout majeur pour une bonne délivrabilité.

Plus vos envois sont personnalisés, plus ils correspondent aux attentes de vos destinataires. En ajoutant la personnalisation à l'aide par exemple du nom et du prénom du destinataire, vous êtes davantage dans le dialogue que dans la communication de masse. Si vos destinataires se sentent considérés, les plaintes vont chuter, votre e-réputation s'améliorera, et donc votre délivrabilité sera meilleure !

Un autre point important est à prendre en compte : la personnalisation des URLs de suivi.



Dans un e-mailing, on insère régulièrement des liens hypertexte pour amener les destinataires du message vers une page web. Lorsqu'on veut suivre les résultats de ses envois, on met en place du tracking afin de détecter les clics sur ces liens. Les URL sont alors automatiquement modifiées lors de l'envoi par le prestataire e-mailing afin d'y intégrer un code comprenant des identifiants uniques et renvoyant dans un premier temps vers un serveur de tracking avant de rediriger vers la page de destination. Ce serveur permet de comptabiliser le nombre de clics pour le suivi.

Personnaliser les liens revient à choisir le nom de domaine Internet que l'on souhaite voir apparaître en lieu et place de ceux attribués automatiquement par le service. Cela permet donc de réaliser du tracking sur les clics, tout en gardant la possibilité de personnaliser une partie des URL avec son propre domaine web, comme par exemple : www.mon-site.com/ma-page.asp?xxxxxxx

La personnalisation des liens a une influence directe sur la bonne transmission du message chez les destinataires. Les URL de tracking créées automatiquement, si elles réfèrent à des serveurs d'envois mutualisés avec d'autres utilisateurs, peuvent être blacklistées par les fournisseurs de messagerie suite à un mauvais comportement d'un utilisateur d'un de ces serveurs. Des URL de tracking associées à des campagnes qui ont provoqué des taux de plaintes importants par le passé ont une mauvaise réputation, ce qui nuira à votre délivrabilité.

Les filtres antispam des fournisseurs de messageries sont extrêmement sensibles sur l'emploi des liens dans les e-mails à cause des nombreux cas de phishing qui sont diffusés. Le phishing vise à obtenir des informations confidentielles (coordonnées, numéro de carte bancaire...) en se faisant passer pour un expéditeur légitime. Pour cela, les usurpateurs vont notamment simuler des liens légitimes. Ils opèrent à l'aide de cette petite astuce HTML : `<a href="http://www.sitephishing.com">www.site de mabanque.com</a>` Avec ce code, les destinataires liront l'URL de confiance (www.site de mabanque.com) mais ne verront pas la véritable destination du lien (www.sitephishing.com).

Cette pratique est très surveillée par les fournisseurs de messagerie, qui ont donc renforcé les règles de filtrage. Or, dans vos campagnes légitimes, vous pouvez être amené à utiliser cette même technique involontairement ! Imaginez que vous ayez mis ce code dans votre e-mailing : `<a href="http://www.adressedemonsite.com">www.adresse demonsite.com</a>`

Avec le tracking des URL, votre service d'envoi d'e-mailing va modifier votre URL comme ceci : `<a href="http://www.urldetracking.com">www.adresse demonsite.com</a>`

En personnalisant vos liens avec votre nom de domaine, vous mettez toutes les chances de votre côté pour passer les barrières antispam.

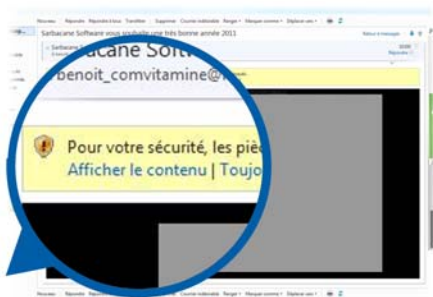
Cette technique offre aux envois de meilleures chances d'être considérés comme légitimes par les filtres antispam et assure ainsi une meilleure délivrabilité en boîte de réception, et donc un meilleur taux d'ouverture. Mais au-delà des aspects de délivrabilité, le fait que le destinataire se sente rassuré sur l'origine du nom de domaine, accroît de manière substantielle le taux de clic de la campagne.

Bonnes pratiques de conception HTML

Il existe un certain nombre de bonnes pratiques essentielles pour concevoir une campagne e-mailing en HTML et pour maximiser les chances de la faire parvenir en boîte de réception.

GESTION DES IMAGES

De plus en plus de boîtes mails n'affichent plus automatiquement les images contenues dans l'e-mailing. On demande aux utilisateurs de cliquer sur un lien pour que les images s'affichent. De plus, les e-mailings constitués uniquement d'images ont plus de chances de se retrouver dans la boîte "SPAM" car les filtres n'arrivent pas à analyser leur contenu. Dans le doute, ils les considèrent donc parfois comme SPAM. D'où l'importance de ne pas concevoir son message uniquement avec des images.



Respectez ces recommandations pour la gestion des images dans vos compositions :

- Mixez images et texte HTML : n'utilisez les images que pour des visuels ou des effets. Tout le reste peut être en texte HTML, auquel vous pouvez appliquer une mise en forme (taille de police, gras, couleur...). Il est encore fréquent de voir des expéditeurs légitimes concevoir leurs e-mails avec une seule ou plusieurs images. Quand vous réalisez des e-mails, testez toujours votre message sans charger les images. Si vous ne voyez rien avec les images désactivées, il faut revoir la conception pour y inclure du texte. Optez pour un ratio 60 % d'images (à héberger sur un serveur de préférence afin d'alléger le poids du message) et 40 % de texte. Cette technique vous permettra de proposer un message attractif et léger, permettant de communiquer selon vos envies et sans contraintes ! Par ailleurs, ce ratio a l'avantage de disposer d'un bon niveau de délivrabilité.
- Privilégiez l'utilisation de plusieurs petites images à une seule
- Renseignez les balises ALT de vos images (elles seront lisibles par certaines messageries à l'emplacement de vos images avant leur chargement, et surtout dans le cas où celles-ci sont remplacées par une croix car non affichées)
- Fixez les dimensions de vos images (attributs width et height). Le gabarit de votre e-mailing sera alors correctement défini même si les images ne sont pas visibles.

LIEN VERS UNE COPIE WEB

Proposez systématiquement un lien en haut de votre message vers une copie web de votre e-mailing, consultable dans un navigateur Internet.

Cette version en ligne vous assure qu'un destinataire, qui ne parvient pas à visualiser le contenu html de votre message ou à télécharger les images, a toujours la possibilité, s'il le souhaite, de vous lire via son navigateur web en conditions optimales.

UTILISEZ L'INLINE CSS

Le CSS, qui permet traditionnellement la mise en forme des textes sur des pages web, n'est pas à bannir des e-mailings. Mais il faut l'utiliser avec parcimonie et en suivant certaines règles :

- Positionnez vos CSS directement dans les éléments HTML : dans les balises `<td>`, `<span>`, `<font>`. L'utilisation des balises `<STYLE>` n'est pas supportée par toutes les messageries
- Ne mettez aucune classe CSS entre `<head></head>` car beaucoup de messageries suppriment les éléments qui se trouvent entre ces balises
- N'utilisez pas les balises de type `<LINK>` contenant un lien externe vers une feuille CSS, ceci ne fonctionnera pas.

EVITEZ LES BALISES MULTIMÉDIA

Vous pourriez être tenté d'utiliser des éléments multimédia pour agrémenter vos e-mailings. Oubliez ! Les vidéos ou encore le format Flash ne s'affichent pas dans toutes les messageries pour le moment. Les balises à proscrire sont donc :

- <OBJECT>
- <EMBED>
- <APPLET>

N'utilisez pas non plus de Javascript ou de DHTML.

Si malgré tout vous souhaitez insérer un extrait vidéo, le mieux est d'utiliser une petite séquence en GIF animé qui redirige vers la véritable vidéo hébergée sur votre site.

Par ailleurs, il est extrêmement déconseillé d'insérer des pièces jointes, surtout pour les envois massifs. Privilégiez l'utilisation de liens vers des documents hébergés.

SIMPLIFIEZ ET NETTOYEZ LE CODE HTML

- Respectez la norme W3C HTML 4 pour le montage HTML des e-mailings.
- N'utilisez pas de liens "map" HTML sur les images
- Supprimez les commentaires HTML
- Utilisez un découpage de votre composition en tranches et assemblez-les à l'aide des tableaux HTML. Evitez d'imbriquer les tableaux.

LIENS

- Privilégiez des liens courts
- Bannissez les liens vers des adresses IP. Ces liens sont surtout utilisés par les spammeurs. Il est donc toujours préférable d'utiliser des noms de domaines.
- Vérifiez que tous les liens sont fonctionnels

TESTS DE RÉCEPTION

Les tests de réception sont essentiels pour vérifier la délivrabilité de vos e-mails. Pour ce faire, il vous faut au préalable déterminer les services de messageries les plus utilisés dans votre base.

Vous pouvez effectuer cette répartition en analysant les noms de domaines des e-mails (yahoo.fr, hotmail.com, etc.) présents dans votre liste de contacts. Ensuite, il suffit de créer des adresses e-mails à des fins de test dans les différents webmails afin de pouvoir tester la délivrabilité avant vos envois. Votre message arrive-t-il correctement ? Est-il présent dans les courriers indésirables ? En fonction des résultats obtenus, il faudra alors agir sur le contenu de la campagne et vérifier la réputation du serveur d'envoi.



E-mail rendering

L'une des difficultés de l'e-mail marketing est de parvenir à rendre ses e-mailings lisibles correctement sur la multitude de clients de messageries aujourd'hui disponibles sur le marché. Même si les bonnes pratiques HTML décrites dans ce livre blanc permettent de rendre l'e-mail le plus homogène possible sur l'ensemble des messageries, autant en être sûr grâce à l'e-mail rendering.

L'e-mail rendering est une technique consistant à tester le rendu des e-mailings sur les principaux terminaux de messagerie, qu'il s'agisse de webmails ou de logiciels de messagerie. Cette technique vous fait gagner beaucoup de temps car c'est un programme automatique qui restitue le rendu de vos e-mailings dans les différents environnements. C'est grâce à ces résultats que vous pouvez ensuite agir sur le code HTML pour en optimiser l'affichage. Etant donné l'importance de la conception HTML dans la délivrabilité, ce service est désormais plus qu'indispensable !

GESTION DE LA FRÉQUENCE D'ENVOI

La fréquence d'envoi de vos campagnes est un facteur qui peut influencer sur votre délivrabilité. Ne harcelez pas vos destinataires avec des e-mailings quotidiens (sauf s'ils l'ont expressément accepté ou demandé). Mais vous ne devez pas non plus espacer trop vos envois au risque que vos destinataires vous oublient ! La fréquence dépend aussi beaucoup de votre marché. Si votre liste est constituée de "prospects chauds" qui sont en phase de recherche avant achat, vous avez tout intérêt à communiquer rapidement et à intervalles courts. Le mieux est encore de prévenir de la fréquence d'envoi lors de l'inscription et si vous pouvez permettre à vos clients de choisir parmi plusieurs fréquences.



Essayez d'être constant dans la fréquence d'envoi. Ceci vous permettra d'habituer l'abonné à recevoir vos messages à intervalles réguliers. La stabilité de la fréquence améliore votre réputation auprès des fournisseurs de messagerie et vous minimisez ainsi les plaintes et les désabonnements.

Si toutefois un destinataire souhaite se désabonner à cause du nombre d'envois, vous pouvez lui proposer une fréquence moindre, vous éviterez une part non négligeable de désabonnements.

GESTION DES VOLUMES D'ENVOI

Certaines campagnes peuvent se retrouver bloquées si elles sont envoyées à un trop grand nombre d'abonnés. Les spammeurs effectuent souvent des envois massifs sans se préoccuper de la régulation du flux. Les fournisseurs de messagerie contrôlent le volume d'e-mails envoyés pour une adresse IP donnée.

Un volume d'envois conséquent et non étalé dans le temps est un motif de blocage temporaire voire même parfois définitif. Ceci peut avoir une conséquence majeure sur la délivrabilité des envois. La campagne en cours n'est pas délivrée dans les temps, ce qui peut parfois engendrer un impact marketing et la réputation de l'expéditeur peut s'en trouver affectée.

Il est donc recommandé de réguler ses flux d'envoi en étalant la quantité de messages à envoyer dans le temps. Evitez ce type de pratique qui impactera négativement la délivrabilité de vos messages et donc la performance de vos campagnes.

Pour éviter ces blocages, utilisez un prestataire qui envoie votre campagne en flux continu qui permet ainsi une meilleure délivrabilité.

Sarbacane et la délivrabilité

PRÉSENTATION DE SARBACANE

Sarbacane Software, filiale du groupe GOTO Software fondé en 1982, développe et édite des logiciels et services permettant d'accompagner les entreprises dans la création et la gestion de campagnes e-mailing.

L'activité Sarbacane débute en 2001 lorsque l'e-mailing n'en était encore qu'à ses balbutiements. Rapidement, celle-ci a rencontré un grand succès auprès des petites et moyennes entreprises, notamment grâce à la prise en main du logiciel d'une grande simplicité. Sarbacane compte aujourd'hui près de 5 000 clients actifs en France.

Le logiciel Sarbacane figure parmi les pionniers des solutions e-mailing et s'enrichit année après année de nouvelles fonctionnalités innovantes, afin d'offrir à ses clients l'outil e-mailing le plus complet et le plus performant du marché. L'interface du logiciel Sarbacane a été conçue dans un souci de grande intuitivité. L'objectif étant que l'utilisateur se concentre dans la création artistique et marketing de sa campagne e-mailing.

Aujourd'hui, Sarbacane est leader sur le marché français de l'e-mailing en nombre de clients.



UNE INFRASTRUCTURE PROFESSIONNELLE

Avec près de 5 000 clients utilisateurs actifs de la troisième version de sa solution d'e-mailing, Sarbacane prend le sujet de la délivrabilité très au sérieux. Plusieurs millions d'e-mails sont envoyés tous les jours via le SRP (Service de Routage Professionnel), une infrastructure totalement sécurisée et spécifiquement étudiée pour accélérer et optimiser la délivrabilité des campagnes e-mailing. En 2010, ce sont plus de 600 millions de mails qui ont été envoyés via Sarbacane 3.

Cette plateforme utilise l'ensemble des dernières techniques d'authentification (Sender ID, SPF, Domain Keys, DKIM). Des techniques désormais requises pour garantir une bonne réception chez de nombreux fournisseurs.

Par ailleurs, les adresses NPAI (N'habitent Pas ou Plus à l'Adresse Indiquée) sont détectées au niveau du protocole d'envoi par la plateforme de routage lors de l'émission des campagnes. Au lancement du logiciel Sarbacane, toutes les adresses NPAI détectées à l'occasion d'envois réalisés avec le Service de Routage Professionnel sont automatiquement téléchargées et ajoutées dans les filtres pour nettoyer les adresses erronées, falsifiées ou obsolètes.

Et en parallèle, une équipe technique dédiée, en charge du Service de Routage Professionnel au quotidien, est en mesure d'intervenir à tout moment. Chaque élément de la plateforme fait l'objet d'un monitoring précis et continu.

L'ensemble de ces techniques et mesures font que Sarbacane Software profite d'un statut privilégié auprès des nombreux fournisseurs d'accès Internet.

Des relations étroites sont entretenues avec la plupart de ces fournisseurs Internet français et européens, ce qui accroît considérablement le niveau de délivrabilité des e-mails envoyés depuis la plateforme.

DES TRAITEMENTS MANUELS POUR PLUS DE GARANTIES

Sarbacane dispose d'une cellule dédiée qui procède à une modération manuelle de toutes les campagnes 24h/24 et ce, même le week-end. Pour garantir une bonne délivrabilité à tous ses clients, Sarbacane vérifie que chaque envoi est conforme à la charte d'utilisation du logiciel et notamment que le lien de désabonnement obligatoire pour chaque campagne est bien présent. Cette modération est menée dans l'intérêt général de tous les utilisateurs.

En cas d'abus de l'un des clients concernant le contenu de son message, le manquement ou le dysfonctionnement du principe de désabonnement, la méthode de collecte ou plus généralement tout autre manquement aux obligations légales et réglementaires applicables en la matière, les internautes sont invités à contacter le service Abuse de Sarbacane à l'adresse abuse@sarbacane.com. Toutes les plaintes adressées à cette boîte sont traitées avec la plus grande attention et les actions sont menées rapidement. Sarbacane a également mis en place des boucles de rétroaction avec des fournisseurs de messagerie qui permettent de détecter et d'agir auprès des expéditeurs non légitimes.

SARBACANE INNOVE POUR OPTIMISER LA DÉLIVRABILITÉ

Sarbacane offre la possibilité de personnaliser ses URL de Suivi Comportemental avec son propre nom de domaine et non plus celui commun à tous les utilisateurs et attribué par défaut. Cette innovation présente le double avantage de paraître plus cohérent dans les communications, de rassurer les destinataires, et bien sûr d'augmenter l'efficacité et la délivrabilité des campagnes.

Par ailleurs, face à la multitude de messageries disponibles, il est de plus en plus délicat de tester le rendu et la lisibilité de ses e-mailings sur tous les environnements. Or, la bonne conception HTML du message est essentielle pour la délivrabilité. Les équipes R&D de Sarbacane Software ont développé une nouvelle fonctionnalité de prévisualisation des messages avant l'envoi définitif, disponible pour les clients Premium, c'est-à-dire ceux utilisant la plateforme SRP (Service de Routage Professionnel).

Les utilisateurs peuvent ainsi envoyer un exemplaire substitué de leur campagne directement depuis le logiciel et visualiser le rendu final sur Outlook 2003, Outlook 2007 SP2, Outlook Express 6, Outlook 2010, Windows Live Mail, Windows Mail, Hotmail, Thunderbird et Orange. D'autres logiciels et webmails enrichiront cette liste dans les mois à venir.

Cette fonctionnalité permet à l'utilisateur de rectifier si nécessaire tout ou partie de son message avant que celui-ci ne soit routé définitivement.

Conclusion

La délivrabilité est un vaste sujet incontournable et fait partie intégrante de l'e-mail marketing. L'enjeu est tel que chaque personne désireuse d'envoyer des campagnes e-mailing doit désormais s'y intéresser sérieusement avant de se lancer dans l'aventure.

Nous espérons que ce livre blanc vous aura été utile. Les équipes de Sarbacane restent à votre disposition pour répondre à toutes vos questions sur l'e-mail marketing.

www.sarbacane.com

SARBACANE Software - S.A.S. au capital de 167 817 € - RCS Roubaix-Tourcoing 509 568 598

Siège social : 3, avenue Antoine Pinay - Parc des 4 vents - 59510 HEM - FRANCE

www.sarbacane.com

Février 2011

Co-écrit avec Guillaume Fleureau
expert e-mailing et blogueur spécialisé dans l'e-marketing
www.guillaumefleureau.com

Toute reproduction commerciale sans l'autorisation expresse de SARBACANE SOFTWARE est strictement interdite. La marque SARBACANE est protégée par les droits de propriété industrielle.