



Livre Blanc

**La délivrabilité
des emails marketing
et ses enjeux**

Neolane

David Letemple
Consultant Produit Neolane

CONTEXTE	3
LES CHIFFRES	3
LES AXES POUR AMELIORER LA DELIVRABILITE DES EMAILS	3
PAR OU COMMENCER ?	4
SOIGNEZ VOTRE ACCUEIL	4
ENRICHISSEZ VOS DONNEES	4
AVEZ-VOUS DU CONTENU ?	4
LA FORME IMPORTE	5
DES LIENS UTILES	6
MAITRISER LA PRESSION	6
ET POUR L'HTML	6
VOLUMES CONTROLES	7
ROUTAGE ADAPTE	7
QUELLE EST VOTRE E-REPUTATION ?	8
GERER LES PLAINTES	8
LANCEMENT DES CAMPAGNES	9
STATISTIQUES ET MONITORING	9
QUELQUES LIENS	10
GLOSSAIRE	11

Contexte

Aujourd'hui la délivrabilité des emails est un sujet à part entière et incontournable de tout projet de communication.

Du statut de préoccupation technique, dont la solution est dans les mains des DSI, la délivrabilité des emails est clairement entrée dans le champ du marketing et de la communication. Avec des impacts forts tant sur le plan de la rentabilité des campagnes que sur celui de l'image de l'entreprise, la délivrabilité est affaire de logiciel, de bonnes pratiques et de confiance.

Avec une bonne qualité de liste de contacts et des pratiques marketing adaptées, Neolane obtient plus de 99 % de taux de délivrabilité.

En 2008, Neolane a envoyé plus de 8 milliards d'emails et réservé plus de 500 adresses IP pour assurer l'exécution des campagnes de ses clients.

Qu'entend-on par délivrabilité d'un email ? C'est l'ensemble des caractéristiques qui vont déterminer sa capacité à parvenir à son destinataire, via une adresse mail personnelle, dans un court délai avec une qualité conforme à ce qui était prévu à la fois sur le contenu et sur la forme. Quel que soit le volume de diffusions, de quelques centaines d'emails à plusieurs milliards, la question est ardue...

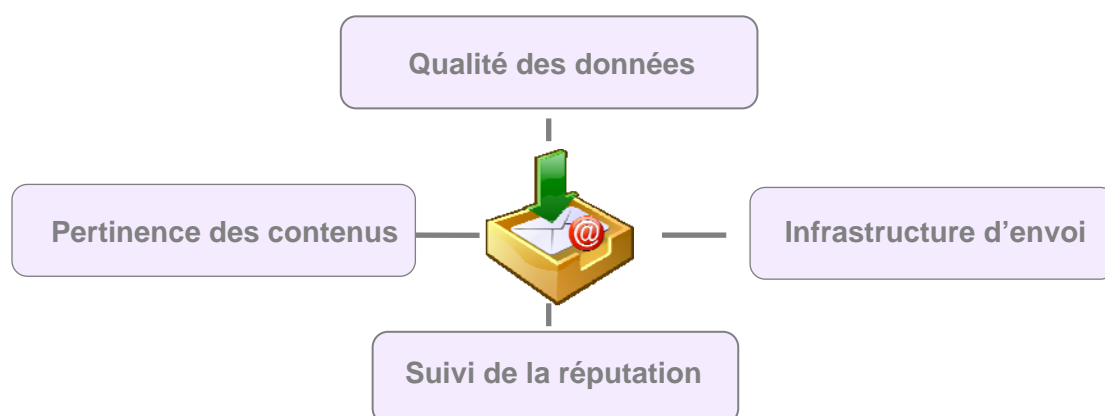
Les chiffres

- Au premier semestre trimestre 2009, la part des messages non sollicités (spam) a représenté en moyenne près de 85,5% du volume du courrier mondial (*source Viruslist.com*).
- 70% des causes de baisse de délivrabilité sont liées à des plaintes des destinataires et mènent à un blacklistage des annonceurs

Neolane a publié une charte antispam qui regroupe des règles de bonne conduite en matière de communication avec des tiers.

<http://www.neolane.com/france/charte-anti-spam.htm>

Les axes pour améliorer la délivrabilité des emails



Par où commencer ?

Qualifiez vos adresses : Le moteur de règles Neolane qualifie automatiquement les retours serveurs SMTP en gérant 2 types d'erreur (hard et soft). Les adresses en erreur seront ainsi exclues de vos prochaines diffusions.

La permission marketing est le point de départ de toute communication, qu'elle soit de type online ou offline. Un consentement actif de vos destinataires est obligatoire "Je souhaite recevoir des offres commerciales venant de tel annonceur à l'adresse mail suivante", et je coche la case du formulaire correspondante. C'est ce qu'on appelle l'opt-in.

Soignez votre accueil

Vérifier le caractère actif de l'adresse email peut s'avérer utile ; en moyenne nous avons 3 adresses mails que nous destinons à des usages différents, certaines d'entre elles sont parfois inactives. Pour cela, vous envoyez un message de confirmation à votre destinataire lui demandant de valider son adresse, généralement en cliquant sur un lien (double opt-in). Ensuite adressez-lui un message de bienvenue pour établir un premier contact et poser les bases d'une relation de confiance et surtout ne communiquez jamais son adresse à un tiers sans son consentement...explicite.

Enrichissez vos données

Régulièrement, vérifiez et éliminez de vos bases de données les doublons, les NP@I et toutes les adresses mails qui ne sont pas actives ou qui vous semblent douteuses. Si vous achetez ou louez des fichiers, assurez-vous de leur provenance et de leur "label opt-in" et procédez à quelques envois tests sur un petit nombre d'adresses pour voir comment elles réagissent. Cent adresses qualifiées valent bien plus en termes de potentiel marketing que mille adresses non qualifiées. Quand un destinataire s'est désabonné, il est impératif de pouvoir conserver cette information dans votre base de données afin de ne pas le solliciter à nouveau et s'exposer à des plaintes qui vont entacher votre réputation marketing.

Avez-vous du contenu ?

Vous avez passé du temps à qualifier vos contacts, ne gâchez pas votre communication en négligeant le contenu, votre interlocuteur vous a donné sa permission pour recevoir des messages en rapport avec ses centres d'intérêt et non pour faire office de cobaye. Imaginez un abonné du journal "Le Monde" qui recevrait à la place "ParuVendu"...

"65% des lecteurs se désabonnent lorsqu'un mail ne les intéresse pas ..."

(étude Email Marketing Attitude 2008, SNCD)

En fonction de votre stratégie de communication (acquisition, fidélisation, vente flash, promotion commerciale, message à caractère informatif), il peut être judicieux d'associer à votre campagne d'emailing d'autres canaux de communication : SMS, courrier, site Web...

Par défaut, les webmails bloqueront les images et les liens contenus dans vos messages. Si votre image n'est pas visualisée : le sens de votre message est perdu. Pensez à renseigner le ALT, la hauteur et la largeur de votre image pour préserver la mise en forme de votre email.

La délivrabilité des emails marketing et ses enjeux

L'emploi de certains termes est à exclure (gratuit, \$, € sexe...), l'usage de points d'exclamation dans le corps du message ou dans l'objet doit être mesuré. Dans tous les cas, un Bon à Tirer est indispensable.

Neolane fournit en standard un formulaire de désinscription, sous la forme d'un bloc de personnalisation à insérer dans vos modèles de diffusion ou vos emails.

Utilisez le standard "list-unsubscribe" qui affichera un bouton "Désinscription" directement dans l'interface du webmail. Vérifiez que votre lien de désinscription fonctionne : testez-le.

La qualité du contenu de votre communication est intimement liée à la connaissance que vous avez de votre destinataire, plus votre compréhension de ses appétences est fine, plus votre communication sera pertinente. Dans le cas contraire, il est préférable de s'abstenir sous peine de véhiculer une image négative de votre entreprise. Avant d'envoyer des messages, la première des questions à se poser est : "Ai-je une bonne connaissance des mes contacts et de leurs attentes ?". D'où l'intérêt de disposer d'une solution logicielle qui vous permette de rassembler, d'enrichir et d'exploiter cette connaissance au fil de vos communications.

La forme importe

La forme est autant à soigner que le fond : beaucoup des filtres antispam utilisés par les messageries bloquent les emails qui contiennent une grande quantité d'images. Vous avez fait réaliser une superbe création par votre agence de communication et elle va finir à la poubelle...

Il est préférable d'équilibrer votre contenu entre textes (2/3) et images (1/3). L'envoi en "multipart" vous permet d'envoyer une version html et une version texte de votre message, vous maximisez ainsi vos chances de voir aboutir votre communication. Charge au logiciel de mail du destinataire d'opter pour l'un ou l'autre des formats.

Il est indispensable pour votre interlocuteur de pouvoir vous identifier dès la réception du mail sans avoir à l'ouvrir, l'expéditeur doit donc être clairement reconnaissable et votre marque mise en avant. L'objet de votre mail ne devrait pas contenir plus de 30 caractères et son contenu motiver le destinataire à ouvrir le mail !

Le sujet indiqué dans l'objet doit annoncer le contenu du mail et non le dissimuler...A ce propos il est utile de rappeler que dans le cas contraire le destinataire de votre mail peut porter plainte.

Le message sera personnalisé : *"Bonjour Monsieur Dujardin", "Bonjour Eric", "Dear John",* ...

En dehors du fait de localiser votre message, il y a des règles à respecter en fonctions des pays, aux USA l'adresse postale de votre société doit figurer au bas de votre message pour être conforme au CAN SPAM Act.

Il est également important de rappeler l'objet de votre communication, nous sommes tous très sollicités et votre interlocuteur n'a pas la mémoire de tous les sites web auxquels il a laissé ses coordonnées pour recevoir de l'information et/ou des offres commerciales. *"Vous recevez ce message suite à votre inscription sur le site ..."*

Des liens utiles

Chacun de vos messages doit contenir la possibilité pour le destinataire de se désinscrire. Il suffira d'ajouter un lien visible et simple à utiliser, généralement en début de mail pour ne pas obliger votre interlocuteur à parcourir tout le mail pour se désabonner. Notre recommandation est une désinscription en un clic avec un message de confirmation. Il est opportun de prévoir des adresses mails valides si le destinataire utilise le bouton "répondre" pour demander sa désinscription au lieu du lien prévu à cet effet.

En complément, vous pouvez proposer à votre destinataire de vous ajouter à son carnet d'adresses afin de fluidifier vos communications futures. *"Pour être sûr(e) de recevoir tous nos emails, merci d'ajouter marketing@societe.com à votre carnet d'adresses emails".*

Maîtriser la pression

Un quidam vient vous demander pour la n^{ième} fois "Hé t'as pas un euro à me donner ?". C'est ce qu'on appelle la pression commerciale, solliciter plusieurs fois une personne en vue de l'amener à céder. Pour gérer et rentabiliser ses campagnes de communication sur du long terme, il est essentiel de maîtriser la pression commerciale afin de ne pas sur-solliciter ses contacts, qui une fois perdus ne reviennent qu'au prix souvent cher payé d'un nouvel effort d'acquisition. Une solution capable de gérer en temps réel ce paramètre est un avantage indéniable : savoir que tel contact a déjà été sollicité 3 fois le mois dernier pour tels messages permet d'optimiser ses campagnes, tout en préservant son image.

Et pour l'HTML

Il est essentiel de vérifier la syntaxe de votre fichier html et sa conformité aux normes W3C si vous souhaitez des communications accessibles, portables et utilisables. La diversité des navigateurs et des appareils utilisés (ordinateurs, PDA, smartphones, mobiles, WebTV...) suppose d'utiliser des standards de communication afin de garantir une accessibilité universelle aux contenus numériques.

Dans le cadre de la mise au point d'une campagne, il est avantageux de vérifier le contenu du code html avec l'"inbox rendering". Cette fonctionnalité permet de tester le rendu d'un contenu html en simulant l'envoi de la campagne auprès des principaux FAI (Fournisseur d'Accès Internet) du marché. Cette fonctionnalité renvoie un rapport avec une prévisualisation de l'email pour chacun des FAI. Des options de correction du code viennent compléter le dispositif.

L'"inbox scoring" va appliquer une série de tests afin de déterminer les risques que votre email soit identifié comme un message non sollicité. Le résultat du test attribue un score qui détermine si votre email est classé en spam.

Gérez la granularité de vos communications en ajustant la fréquence d'envoi de vos messages selon leur type (commercial, newsletter...).

Grâce au "whitelist", vos diffusions peuvent s'affranchir du filtre de contenu.

Neolane intègre de façon automatique et gratuite un filtre antispam. Les scores obtenus sont analysés et expliqués.

Volumes contrôlés

Grâce au "whitelist", vos diffusions peuvent s'affranchir du "throttling".

Les FAI ont mis en place un mécanisme, connu sous le nom de "throttling", afin de contrôler le volume des échanges qui transitent dans leurs "tuyaux". À partir d'un certain seuil la réception des messages est bloquée. Ce seuil est basé sur le nombre de connexions entre le serveur d'envoi et le serveur de réception, sur le nombre de messages par connexion et la quantité de messages par unité de temps.

Si vous tentez d'ouvrir un trop grand nombre de connexions SMTP simultanément ou d'envoyer un trop grand nombre d'emails sur une courte période, vous avez de grandes chances d'obtenir des erreurs du type "timeout" (délai dépassé) – "server has exceeded the rate limit allowed" (la limite du serveur est dépassée) – "too many connections from your IP" (trop de connexions sur cette adresse IP).

A noter : la réputation des adresses IP utilisées peut contribuer grandement à faire varier ces limites.

Routage adapté

Votre système de routage doit être capable de s'adapter afin de respecter les règles énoncées dans les pages postmaster des FAI :

- le nombre de connexions par adresse IP d'envoi,
- le nombre de messages par session,
- la vitesse d'émission,
- les principes d'authentification

Nous vous recommandons de procéder de la manière suivante, tant que vos IPs n'ont pas acquis de réputation :

- commencez par router un faible volume,
- diminuez la vitesse d'émission,
- prévoyez un nombre d'adresses IP plus important (ratio quantité envoyée/adresse IP),
- ajustez le nombre de reprises d'envoi afin d'augmenter le taux de messages aboutis

En parallèle, le taux de plainte, le nombre d'adresses pièges et le taux d'adresses invalides doivent être minimales.

Construire sa réputation est affaire de temps et de bonnes pratiques. Les fréquences d'envoi et les volumes diffusés doivent être stables. Les volumes conséquents bénéficient d'un meilleur score. Les pics d'envoi sont à éviter.

Quelle est votre e-réputation ?

L'option délivrabilité : le monitoring technique de vos campagnes vous donne accès à un rapport sur le statut de vos IPs/domaines sur les principales RBL.

Votre e-réputation est votre passeport pour voyager sereinement sur Internet. L'e-réputation est l'image que vous projetez de votre entreprise sur Internet, du courrier électronique au web en passant par les media sociaux.

La réputation des adresses IP influe largement sur votre capacité à délivrer correctement vos messages : les FAI bloquent les communications qui utilisent des IP dont la réputation est inexistante ou mauvaise.

Les adresses IP qui ne routent pas régulièrement avec des volumes constants ont généralement plus de mal à établir leur réputation. A l'inverse une bonne réputation permettra d'élargir les limites du "throttling".

Il est essentiel de contrôler et d'interpréter les résultats de vos campagnes.

Pour suivre votre réputation, vous pouvez vous référer aux principales RBL (Real Time BlackHole List) : SpamCop, SpamHaus...Les RBL établissent une liste d'adresses IP et/ou de domaines réputés comme expéditeurs de spam.

Les "whitelists" permettent d'identifier les expéditeurs d'emails reconnus, ce qui constitue un avantage certain car vos emails auront un traitement de faveur et ne seront pas bloqués sur la base de leur contenu. Il existe plusieurs manières de se faire référencer sur une "whitelist" :

- Enregistrement gratuit (AOL, Yahoo, United Online)
- Certification payante par un tiers (Goodmail, Sender Score)

Neolane vous propose des rapports de synthèse sur chacune de vos campagnes de communication pour suivre :

- le taux de réactivité
- le taux d'ouverture et de clics
- la répartition des erreurs
- le taux d'échec par domaine

Neolane produit des rapports d'erreurs pour vous permettre de surveiller :
- l'hygiène de la base d'utilisateurs (taux de contacts inconnus)
- la réputation (nombre de messages refusés et nombres d'inatteignables).

Gérer les plaintes

Même si vos pratiques sont professionnelles, vous n'êtes pas à l'abri d'un faux pas et la gestion des plaintes de vos destinataires est un élément à prendre en considération. Pour cela, vous pouvez mettre en place une "feedback loop" : une boucle de rétroaction qui vous informe des plaintes reçues par votre FAI suite à l'envoi de vos campagnes. Une fois la demande acceptée par votre FAI, Neolane est en mesure d'automatiser le traitement des plaintes en plaçant les adresses emails en quarantaine, prévenant ainsi toute communication future avec les plaignants. Dans la même optique, relevez les messages reçus dans les boîtes mails suivantes : postmaster@societe.com, abuse@societe.com

Lancement des campagnes

L'authentification repose sur des principes différents selon les webmails utilisés. Il existe 4 normes qui vérifient que l'adresse IP/domaine a bien le droit d'envoyer des emails :

- SPF (Sender Policy Framework)
- Domain Keys
- DKIM (Domain Keys Identified Mail)
- Sender Id

Si les volumes le permettent, segmentez vos flux de communications en séparant les adresses IP utilisées pour les messages transactionnels (alerte, confirmation de commande) des adresses IP utilisées pour les messages commerciaux.

Neolane vous préconise le rétro-planning suivant pour la mise en œuvre de vos campagnes de communication :

3 mois

Enregistrez les domaines utilisés pour l'envoi des mails (reverse DNS/domaine technique) et le tracking. Un domaine trop récent peut être considéré comme spammeur.

6 semaines

Mettre en place la configuration réseau

- reverse DNS de vos adresses IP d'envoi
- record SPF autorisant vos IPs

3 semaines

Mettre en place les paramètres d'authentification

- DK/DKIM et effectuer les tests d'envoi sur les différents webmails
- Demandez l'activation des "feedback loop" auprès de vos FAI, l'accès aux données SNDS pour vos adresses IP d'envoi (service Microsoft)
- Commencez à collecter les informations pour les demandes de "whitelist"

1 semaine

- Nous vous recommandons d'importer vos quarantaines dans la table des adresses Neolane.
- Ajoutez votre plateforme au service de monitoring technique.

Lancement

- Démarrez avec un nombre de destinataires et un débit de diffusion réduits (ex : 100 000).
- Vous augmenterez le débit au fur et à mesure de la campagne après une qualification de vos contacts et une réputation établie.
- Surveillez les premières diffusions

Après lancement

Si les taux d'erreur et de plainte le permettent, vous pouvez demander un référencement en "whitelist" auprès de Yahoo, d'AOL...

Statistiques et monitoring

Tout au long de la campagne et après chaque diffusion, il est important de suivre le taux de mails délivrés afin de réajuster les paramètres. Surveiller la progression de la campagne en termes de messages diffusés par heure et de nombre de retours NP@I permet de rectifier le tir et surtout de préserver sa réputation.

Quelques liens

<http://postmaster.comcast.net>

<http://www.w3.org/WAI/>

http://postmaster.aol.com/tools/whitelist_guides.html

<http://help.yahoo.com/l/us/yahoo/mail/postmaster/index.html>

<https://www.senderscore.org/>

http://en.wikipedia.org/wiki/CAN-SPAM_Act_of_2003

<http://en.wikipedia.org/wiki/DNSBL>

<http://www.returnpath.net/commercialsender/certification/>

<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164&dateTexte=>

Glossaire

BAT	<p>Littéralement Bon à Tirer.</p> <p>En imprimerie, l'épreuve contractuelle est la dernière étape avant l'impression : on effectue une simulation de l'impression d'après les éléments finalisés.</p> <p>Epreuve soumise au client pour pouvoir vérifier la conformité de la mise en page, des textes, des images pour approbation.</p> <p>Appliquée au mail par extension.</p>
Blacklist	<p>Liste contenant les adresses emails ou IP qui seront automatiquement rejetées par le serveur de courrier.</p>
B2B	<p>L'expression business to business (B2B) désigne l'ensemble des activités d'une entreprise visant une clientèle d'entreprises.</p>
B2C	<p>L'expression business to consumer (B2C) désigne l'ensemble des activités d'une entreprise visant une clientèle de particuliers.</p>
CAN Spam Act	<p>Au 31 décembre 2003, 36 des 50 États américains avaient adopté une loi spécifique réglementant l'envoi de messages électroniques commerciaux non sollicités, ou "spam". Parallèlement, en 2003, le Congrès des Etats-Unis a adopté la première loi fédérale visant à combattre le spam : le CAN-Spam Act de 2003 (Controlling the Assault of Non-Solicited Pornography and Marketing Act). Cette loi fédérale est entrée en vigueur le 1er janvier 2004. Le CAN-Spam Act est basé sur le modèle de l'opt-out.</p>
DK/DKIM	<p>DKIM (DomainKeys Identified Mail) est une norme d'authentification fiable du nom de domaine de l'expéditeur d'un courrier électronique. Elle constitue une protection efficace contre le spam et l'hameçonnage. En effet, DKIM fonctionne par signature cryptographique du corps du message et d'une partie de ses en-têtes. Une signature DKIM vérifie donc l'authenticité du domaine expéditeur et garantit l'intégrité du message.</p>
DNS	<p>Le Domain Name System (ou système de noms de domaine) est un service permettant d'établir une correspondance entre une adresse IP et un nom de domaine et, plus généralement, de trouver une information à partir d'un nom de domaine.</p>
Goodmail	<p>Editeur de logiciels qui offre une solution permettant de certifier des emails et ainsi leur éviter d'être considérés comme des spam.</p>

LCEN	<p>A l'origine LSI (Loi sur la Société de l'Information), couramment appelée LEN (Loi sur l'Economie Numérique), elle a été baptisée LCEN (Loi sur la Confiance dans l'Economie Numérique) afin d'y imprimer l'idée de " confiance " dans l'espace numérique. Le texte de la LCEN a été adopté le 13 mai 2004.</p>
Multipart	<p>Multipurpose Internet Mail Extensions (<i>MIME</i>) est un standard internet qui étend le format de données des emails pour supporter des textes en différents codage de caractères autres que l'ASCII, des contenus non textuels, des contenus multiples, et des informations d'en-tête en d'autres codages que l'ASCII.</p> <p>Grâce au type MIME "multipart" le standard MIME permet de définir des messages composites, c'est-à-dire des messages comportant plusieurs pièces jointes, éventuellement emboîtées.</p>
Permission marketing	<p>La permission marketing a été inventée et popularisée par Seth Godin, ancien responsable du marketing direct de Yahoo, dans son ouvrage <i>Permission Marketing</i>. La finalité de la permission marketing est d'inciter le client à entrer puis à accepter des niveaux croissants de permission, c'est-à-dire de consentement vis-à-vis d'une marque ou d'un produit, via un programme de marketing relationnel.</p>
RBL	<p>Les Realtime Blackhole List ont comme mandat de fournir une liste de serveurs réputés comme grands envoyeurs de spams, et de lister les grands polluposteurs. Il s'agit en fait d'une grande liste noire généralisée. Le principe d'utilisation est simple : lorsqu'un filtre reçoit un email, il vérifie si le serveur d'envoi est contenu dans un RBL. Si oui, l'email est catégorisé comme spam.</p>
Sender Id	<p>Norme d'authentification fiable du nom de domaine de l'expéditeur d'un email.</p>
SenderScore	<p>Le programme d'accréditation "Sender Score Certified" de Return Path fonctionne comme une liste blanche, ou "whitelist".</p> <p>Les FAI considèrent les emails envoyés depuis les adresses IP authentifiées par Sender Score Certified comme légitimes et pouvant être ouverts en toute sécurité.</p>

SMS	Short Message Service. Permet de transmettre de courts messages textuels, c'est un service proposé conjointement à la téléphonie mobile, voire à d'autres appareils mobiles comme le Pocket PC.
SMTP	Le Simple Mail Transfer Protocol (littéralement "Protocole simple de transfert de courrier"), généralement abrégé SMTP, est un protocole de communication utilisé pour transférer le courrier électronique vers les serveurs de messagerie électronique.
SNDS	Cet outil Microsoft permet d'obtenir de nombreuses statistiques, comme le nombre de mails issus d'une même adresse IP, ou encore de savoir le pourcentage d'emails classé comme spam par les filtres automatiques d'Hotmail.
SpamAssassin	Projet libre mené par la Apache Software Foundation, Le but de ce logiciel est de filtrer le trafic des emails pour éradiquer les emails reconnus comme spams ou emails non sollicités.
SPF	Sender Policy Framework est une norme d'authentification fiable du nom de domaine de l'expéditeur d'un courrier électronique.
Throttling	Méthode utilisée par les FAI pour limiter l'usage de la bande passante, la CPU des serveurs, diminuer l'utilisation de services P2P et ainsi prévenir les risques de congestion.
Whitelist	Liste contenant les adresses emails ou IP qui seront automatiquement acceptées par le serveur de courrier.

Pour en savoir plus sur notre offre ou une démonstration produit, visitez notre site web : www.neolane.com ou contactez nous :

Neolane SA

**45 – 47 avenue Carnot
94230 Cachan
France
Tél : +33 1 41 98 35 35
Email : info@neolane.fr**

À propos de Neolane

Neolane est un éditeur de logiciels qui répond aux enjeux stratégiques des directions marketing et communication grâce à la seule plate-forme marketing intégrée permettant l'orchestration, la personnalisation, l'automatisation, l'exécution et la mesure de toutes les communications sur l'ensemble des canaux traditionnels et mobiles.