WHITEPAPER

Délivrabilité en email marketing

Comment assurer la fiabilité de votre envoi

L'EMAIL MARKETING.
AUX COTES DES CLIENTS.

inxmail

Introduction

Pourquoi la délivrabilité est-elle si essentielle dans l'Email Marketing? Imaginez que vous rédigiez les newsletters les plus pertinentes qui soient et qu'elles n'arrivent jamais dans la boîte de réception de vos destinataires. Les bénéficiaires ne pourront pas en prendre connaissance et réagir selon leurs besoins.

En ~~s'~~abonnant, le destinataire fait part de son souhait de recevoir cette newsletter et l'attend. Plus grave encore : un client attend un email transactionnel important, comme une confirmation de commande ou d'annulation. Et ne la reçoit pas.

Cela a non seulement un impact négatif sur le succès des campagnes d'Email Marketing, mais peut également avoir un impact négatif sur la confiance dans l'expéditeur ou dans sa marque. Et cela pourrait à son tour se traduire par une baisse des ventes. Techniquement parlant, votre réputation en tant qu'expéditeur en souffre. Mais comment tout cela est-il lié ? Et quelles solutions pouvez-vous mettre en place pour que vos emailings atteignent leurs objectifs et que votre réputation soit renforcée ? Nous vous expliquons cela de façon détaillée dans ce livre blanc et nous vous présentons les mesures que vous pouvez prendre pour protéger et renforcer votre marque à long terme.

Les fournisseurs de services d'Email Marketing doivent aussi remplir certaines conditions et exigences pour assurer cette délivrabilité. Nous vous présenterons donc les critères à considérer dans le choix de sélection d'un routeur d'emailing professionnel.

CONTENU

Chapitre 1: Délivrabilité et autres termes **4**
Le processus de contrôle-étape par étape 5
Illustration : Processus de vérification lors de la livraison 7
Influence de la délivrabilité sur la marque et la confiance 8
La réputation et sa corrélation avec la délivrabilité 8
Le taux de délivrabilité et ses pièges 9
De nombreux rebonds sont mauvais pour la réputation 10
Les procédures d'authentification des emails renforcent la réputation 11

Chapitre 2: Ce que les responsables marketing peuvent faire pour améliorer la délivrabilité **14**
Configuration technique 15
Email Marketing conforme à la législation 18
Effets du contenu et de l'expédition des Emailings sur la délivrabilité 21
Checkliste 26

Partie 3: Caractéristiques de délivrabilité et de qualité des fournisseurs d'Email Marketing **27**
Critères qualitatifs 28
Exigences techniques 30
Illustration: DMARC et Domain Alignment 35

Conclusion **38**
Sur Inxmail 40

Chapitre 1:
Délivrabilité et autres termes

Derrière le terme technique de "délivrabilité", existe une multitude de mesures et de techniques différentes - toutes ayant un objectif commun : garantir qu'un email envoyé arrive dans la boîte de réception du destinataire. Pour garantir que les newsletters et les emails transactionnels ne soient pas éliminés directement par le serveur de distribution ou ne finissent dans le filtre anti-spam, une bonne réputation et le respect des directives sont essentiels pour un email marketing conforme à la loi. Les expéditeurs reconnus et les routeurs d'email marketing utilisent, entre autres, les listes blanches et plusieurs méthodes d'authentification des envois de mailings.

Dans ce livre blanc, nous examinerons chaque point particulier du processus et nous formulerons des recommandations. Vous vous familiariserez avec tous les termes liés au processus de délivrance et acquerrez une solide connaissance technique de base. Après avoir lu ce document, vous saurez quels sont vos défis en matière de délivrabilité et ce que vous pouvez attendre de votre fournisseur d'email marketing.

Le processus de contrôle- étape par étape

Afin de mieux comprendre la problématique de la délivrabilité, nous regarderons les différentes étapes du processus de livraison que doit franchir le mail et les contrôles qu'il subit.

Tout d'abord, le serveur mail de distribution filtre le mail entrant en utilisant différentes méthodes. Pour s'assurer que l'expéditeur n'usurpe pas l'identité d'un autre annonceur, la plupart des routeurs d'email authentifient l'expéditeur dans un premier temps. Pour ce faire, le serveur de messagerie et le domaine de l'adresse bounce sont analysés. L'identité de l'expéditeur est vérifiée par différents systèmes d'authentification. Les méthodes les plus courantes sont le Sender Policy Framework (SPF), le Domain Keys Identified Mail (DKIM) ou le Domain-based Message Authentication, Reporting and Conformance (DMARC).

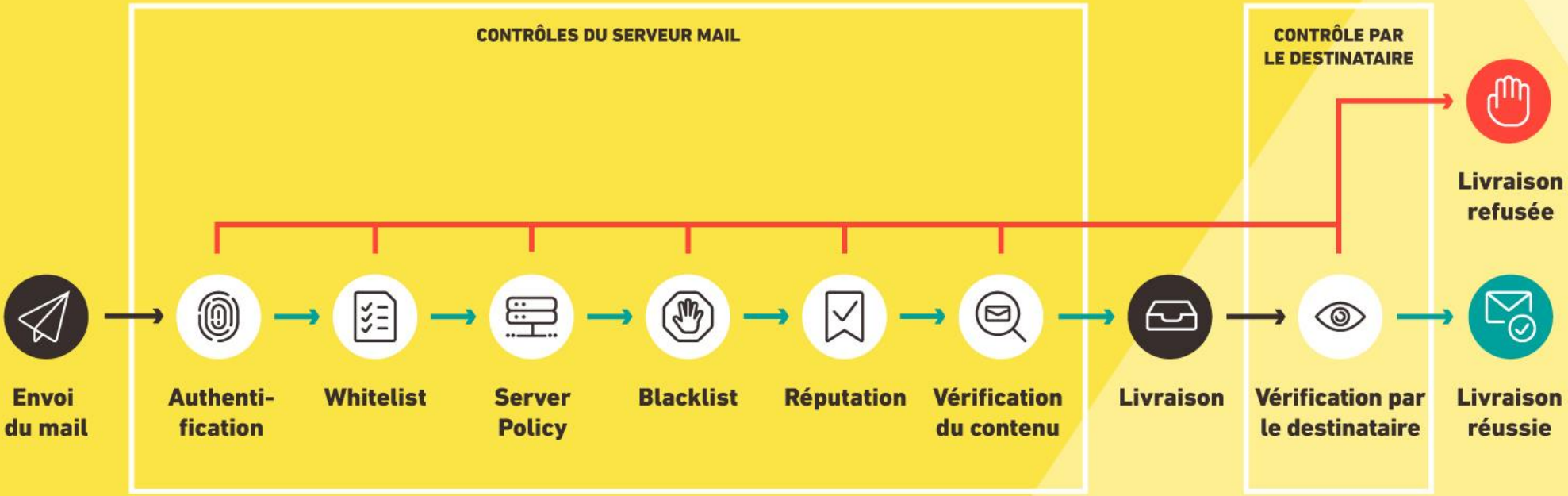
Si l'expéditeur est clairement identifié, la deuxième étape consiste à vérifier s'il figure sur une liste blanche. La « Sender Policy » décrit la configuration du serveur et en particulier son protocole de sécurité.

Après un retour positif du serveur, le courrier est finalement livré au destinataire. Il peut être récupéré par un client email installé

localement. Toutefois, le processus de vérification n'est pas encore terminé. La plupart des programmes d'emails sont dotés de leurs propres filtres anti spam pour vérifier côté client. L'envoi parvient dans la boîte aux lettres du destinataire après validation par ce filtre anti spam.

Malgré la complexité de la procédure, des mesures techniques peuvent être mises en place pour chaque étape du process et ainsi améliorer votre capacité à délivrer vos emails. Cela ne concerne pas seulement la configuration technique du fournisseur par lequel l'envoi est envoyé mais aussi la configuration de l'infrastructure de l'entreprise expéditrice. A partir de là, vous pourrez construire votre propre réputation, renforcer votre marque et garder le contrôle de votre propre domaine. Mais comment renforcer votre marque et la confiance en votre marque lors de vos envois?

Illustration : Processus de vérification lors de la livraison



Influence de la délivrabilité sur la marque et la confiance

Du fait du volume croissant de spam, il ne suffit plus de se protéger contre les abus mais il faut intervenir et renforcer votre propre réputation. Examinons cela de plus près à l'aide d'un exemple.

Vous commandez régulièrement des articles auprès d'un fournisseur avec lequel vous avez eu des expériences positives et en qui vous avez confiance. Récemment, vous recevez de plus en plus de demandes de paiement pour des opérations que vous n'avez pas effectuées.

Il s'agit clairement de spam, comme le montre un coup d'œil sur votre compte client. Vous n'avez pas effectué cet achat et vous n'êtes pas en retard de paiement. En fait, tout va bien - mais seulement à première vue. Parce que votre confiance dans le fournisseur ou sa marque en souffre un peu. Il ne s'agit en aucun cas d'une utilisation abusive des données et le fournisseur est toujours aussi sérieux, digne de confiance et fiable qu'auparavant. Mais un spammeur ou un cybercriminel envoie des mailings non qualifiés au nom du fournisseur. Et crée ainsi l'incertitude. Cette insécurité provoque la méfiance des destinataires et donc la méfiance envers la marque. C'est précisément pour cette raison qu'il est important que vous construisiez votre propre réputation en tant qu'expéditeur, que vous rendiez votre marque visible et que vous la renforciez ainsi. C'est ainsi que vous pourrez mettre un terme aux cybercriminels à l'avenir. L'exemple montre que la délivrabilité et la réputation sont étroitement liées. Mais que signifie la réputation en détail ? Et la réputation peut-elle être mesurée, et si oui, comment?

La réputation et sa corrélation avec la délivrabilité

La plupart des problèmes de délivrabilité sont liés à la réputation de l'expéditeur, la réputation étant le facteur clé pour déterminer si le mail passe ou non les contrôles dans le processus de livraison. Au départ, la réputation était principalement déterminée par ce que l'on appelle le "Score de l'expéditeur" de Return Path. Il permet de prévoir les taux de filtrage du spam et la probabilité de distribution.

Aujourd'hui, la plupart des fournisseurs d'accès Internet (FAI) disposent de leur propre base de données de réputation, qui est tenue à jour à l'aide de règles et de mesures individuelles.

Dans les deuxième et troisième parties, vous apprendrez en détail quels facteurs ont un impact positif et négatif sur votre réputation. La réputation et la capacité de livraison s'influencent mutuellement : une bonne réputation garantit que les envois peuvent être livrés rapidement. Une mauvaise délivrabilité (par exemple, en raison de nombreux rebonds) a un effet négatif sur la réputation. Si la réputation est mauvaise, cela a un effet négatif sur la capacité de livraison.

Les différentes étapes du processus de livraison ont permis de clarifier les facteurs qui influencent la délivrabilité. Mais quels sont les liens entre délivrabilité et taux de délivrabilité?

Le taux de délivrabilité et ses pièges

Le taux de délivrabilité indique le rapport en pourcentage entre le nombre d'emails livrés et la quantité envoyée. Ce taux est donc l'exact opposé du taux de rebond et doit donc être aussi élevé que possible, idéalement supérieur à 95 %.

Le taux de délivrabilité se calcule comme suit:

$$\textbf{Taux de délivrabilité } [\%] = \frac{\textbf{nombre d'envoi - Bounces}}{\textbf{Nombre d'envois}} * 100\%$$

La quantité d'envoi décrit le nombre total d'emails envoyés. Les rebonds sont tous des emails non distribués. L'interprétation du ratio doit être traitée avec prudence. Le taux de délivrabilité ne révèle que le pourcentage d'emails qui n'ont pas été rejetés comme bounce ou le pourcentage d'emails qui ont été reçus par le serveur de messagerie du destinataire. Néanmoins, tous les courriers électroniques restants ne finissent pas nécessairement dans la boîte de réception. Les emails livrés peuvent encore être bloqués par des filtres anti-spam. Ou bien ils sont rejetés directement par des fournisseurs d'accès Internet en raison de la mauvaise réputation de l'expéditeur. Le terme "taux de délivrabilité" est donc en fait quelque peu trompeur.

De nombreux rebonds sont mauvais pour la réputation

Une newsletter atteint rarement tous ses destinataires. Les tentatives de livraison non abouties se terminent par des « rebonds". Un rebond est un message d'erreur qui est généré par le serveur de messagerie en réponse à un envoi non distribuable et renvoyé à l'expéditeur. Il existe deux types de rebonds : hard bounces et soft bounces.

Si un destinataire est indisponible en permanence, par exemple parce que l'une adresse électronique est non valide, on parle de "hard bounce".Les soft bounces, en revanche, sont des problèmes temporaires, comme une boîte aux lettres trop pleine.

Les Hard Bounces sont donc synonymes d'erreurs permanentes. Cela signifie que l'adresse électronique rejetée ne sera pas accessible, même en cas de nouvelles tentatives de livraison. En bref : l'adresse électronique concernée n'est pas valide.

Les Soft Bounces, en revanche, indiquent des problèmes temporaires. Ils sont causés, par exemple, par des boîtes aux lettres trop pleines ou des pièces jointes trop volumineuses qui sont refusées par le serveur de messagerie du destinataire. Des problèmes temporaires de serveur peuvent également produire des Soft Bounces. Toutefois, comme les adresses électroniques concernées existent, elles peuvent être adressées ultérieurement.

Le taux de bounce décrit le pourcentage de mails non délivrés par rapport au nombre total de mails envoyés. Il s'agit donc d'un indicateur de la qualité des adresses de la liste de destinataires.

Le taux de bounces est calculé ainsi:

$$\textbf{Taux de Bounces } [\%] = \frac{\textbf{Nombre de Bounces}}{\textbf{Nombre de mails envoyés}} * 100\%$$

La quantité d'envoi décrit le nombre total d'emails envoyés. Le Nombre de Bounces, la quantité de rebonds signalés.

Il est normal que des rebonds se produisent après l'envoi d'un emailing. En particulier au premier envoi d'une liste de diffusion, c'est un critère de qualité de ses adresses. Cependant, si le taux de rebond est en permanence supérieur à cinq pour cent, il faut alors s'en préoccuper et analyser les causes.

La gestion automatisée des rebonds - telle qu'elle est proposée par les prestataires d'emailing- est naturellement conforme aux règles de la Certified Senders Alliance (CSA), du projet Whitelist de la DDV et de eco-Verband : Après une tentative de livraison non aboutie, une adresse électronique doit être retirée de la liste de diffusion et ne peut plus être utilisée pour communiquer par email.

Une gestion efficace des rebonds garantit un faible taux de rebond et des listes de diffusion de bonne qualité

Les marketeurs ne peuvent pas ne pas traiter les informations que remontent la gestion des rebonds. Des taux de rebond élevés entraînent non seulement des frais d'envois élevés, mais ils affaiblissent également la réputation du serveur de messagerie utilisé auprès des fournisseurs accès à Internet. En effet, des taux de bounces élevés sont une caractéristique de spam. Si la réputation souffre, le taux de livraison baisse. Cette situation peut conduire à la non livraison à des adresses valides de mailings provenant de cet expéditeur.

Les procédures d'authentification des emails renforcent la réputation

L'origine d'un email peut facilement être falsifiée. Sans authentification de l'email, il n'est pas possible de déterminer de manière sûre si le message provient réellement de l'expéditeur dont il prétend avoir été envoyé. C'est pourquoi les routeurs d'email marketing ont mis au point diverses méthodes d'authentification pour protéger les destinataires. Les expéditeurs qui recourent à ces méthodes améliorent leur réputation d'expéditeurs fiables auprès des routeurs et augmentent ainsi leur taux de livraison. Pour ces raisons, il est important de maîtriser ces aspects techniques et complexes.

Sender Policy Framework (SPF)

La procédure SPF vise à empêcher la falsification des adresses d'expéditeurs d'emails. Il aide le serveur de réception d'email à reconnaître des emails envoyés par un serveur de mail non autorisé.

La méthode SPF est utilisée pour valider le courrier électronique à l'aide de l'adresse IP du serveur de courrier électronique d'envoi et donc exclusivement pour vérifier l'expéditeur, ou plus précisément le domaine de l'expéditeur. Le problème ici est que l'on peut vérifier l'expéditeur et non le courrier électronique lui-même. Pour cela, le Standard Domain Keys Identified Mail doit être utilisé.

Domain Keys Identified Mail (DKIM)

La norme DKIM est une méthode avancée d'authentification de l'expéditeur et, comme le SPF, elle est utilisée pour garantir l'authenticité des expéditeurs d'emails. L'utilisation de DKIM vise à

garantir que le contenu du courrier électronique envoyé n'a pas été manipulé pendant son acheminement vers le destinataire.

DKIM est basé sur une procédure cryptographique asymétrique dans laquelle le système d'envoi utilise une clé privée pour fournir aux messages sortants une signature numérique. Le système récepteur vérifie alors le message reçu par rapport à la clé publique librement disponible dans le système de noms de domaine (DNS) et correspondant à l'adresse de l'expéditeur. Si l'authentification échoue, le système récepteur peut décider de rejeter le message.

Une signature DKIM correcte atteste de trois points :

- Le contenu d'un email n'a pas été manipulé pendant son acheminement vers le destinataire,
- Les lignes d'en-tête de l'email n'ont pas été manipulées sur le chemin du destinataire,
- L'expéditeur est le propriétaire du domaine ou a été autorisé à signer le courrier électronique via DKIM.

Le DKIM et le SPF font tous deux partie des spécifications de DMARC.

Domain-based Message Authentication, Reporting and Conformance (DMARC)

La spécification DMARC (Domain-based message authentication, reporting and compliance) est conçue pour empêcher l'utilisation abusive d'adresses d'expéditeurs d'emails. La DMARC étend les normes déjà connues SPF et DKIM pour l'authentification et la vérification des emails. La DMARC, en tant que recommandation, suggère aux fournisseurs d'accès à Internet (FAI) comment traiter les messages lorsque l'authentification par SPF et DKIM échoue. Les courriers électroniques concernés sont supprimés, rejetés ou déplacés dans le dossier "spam" en fonction de l'entrée DMARC. De plus, le propriétaire du domaine peut également spécifier une adresse électronique pour des notifications. Le propriétaire du domaine sera ainsi automatiquement informé de tout problème d'authentification par les routeurs supportant la norme DMARC. Ainsi, les spams et les attaques de phishing utilisant son domaine peuvent être détectés rapidement.

Si vous utilisez les trois méthodes SPF, DKIM et DMARC séparément, la protection contre le spam, le phishing et le spoofing n'est pas suffisante. Les soit-disant "spoofers" peuvent toujours envoyer des messages qui prétendent provenir de votre domaine. Chaque méthode possède son propre mécanisme d'authentification ou de vérification à un certain niveau. Seule la convergence des 3

méthodes garantit une protection efficace contre la contrefaçon et les abus et donc une identification claire de la marque pour le destinataire. Le concept d'alignement de domaines joue un rôle essentiel dans ce contexte, que nous expliquerons plus en détail dans la troisième partie.

Après cette présentation des termes du processus de délivrabilité, nous vous montrons au chapitre suivant les mesures à prendre pour améliorer votre réputation et votre taux de livraison à long terme.

Chapitre 2:
Ce que les responsables marketing peuvent faire pour améliorer la délivrabilité

De la théorie à la pratique : Dans la section suivante, nous vous montrerons les mesures à prendre en tant que marketeur pour un niveau de délivrabilité maximal et une bonne réputation. Les aspects techniques, juridiques et de contenu seront présentés.

Configuration technique

Mettre en place un sous-domaine distinct pour l'envoi

Le domaine principal, que les entreprises utilisent par exemple pour la communication professionnelle entre les employés ou pour les contacts externes, ne doit pas être utilisé à d'autres usages comme l'envoi de newsletter ou de mails transactionnels. Nous recommandons de créer un sous-domaine distinct pour l'envoi de chaque type d'emails : Chaque domaine ou sous-domaine est la principale composante d'un processus de filtrage de spam et a sa propre réputation. Si le domaine principal est utilisé pour toutes les communications, y compris l'envoi d'emails publicitaires, une éventuelle perte de réputation peut avoir un effet négatif sur les échanges professionnels par emails. Il est donc préférable d'utiliser un domaine par newsletter ou emails transactionnels en créant et utilisant un sous-domaine dédié. Le sous-domaine sélectionné doit toujours être attribué de manière unique à thématique. Pour notre domaine "exemple.com", les sous-domaines suivants sont possibles :

Newsletter	Mails transactionnels
newsletter.example.com	service.example.com
news.example.com	shop.example.com
mail.example.com	

Vous devez éviter de modifier les adresses ou les domaines expéditeurs. En effet, ce signal est considéré comme un spam et le domaine de l'expéditeur est soudainement inconnu des FAI. De plus, l'adresse actuelle a déjà été reconnue et est synonyme de confiance. Les filtres mis en place par les destinataires ne fonctionneraient plus en cas de changement

En utilisant votre propre sous-domaine pour l'envoi, le domaine du fournisseur d'e-mail marketing ne s'affiche pas dans la boite de réception des destinataires, comme c'est le cas dans les clients de messagerie d'Outlook, Hotmail ou Gmail. L'expéditeur rend ainsi sa marque visible, construit sa propre réputation et améliore sa délivrabilité à long terme. Cet avantage est dû à ce qu'on appelle

l'alignement de domaine, que nous expliquons plus en détail dans le troisième chapitre et qui constitue la condition de base pour l'étape suivante : l'authentification par Domain-based Message Authentication, Reporting and Conformance (DMARC).

Une fois le domaine d'expédition créé, nous vous recommandons de confier votre sous-domaine à votre fournisseur d'e-mail marketing pour une configuration et une authentification supplémentaires. De plus, vous pouvez faire enregistrer ce domaine comme domaine de suivi auprès de votre fournisseur d'email marketing. Ainsi, tout pointera vers votre domaine.

Mettre en place une authentification pour le domaine d'envoi

Pour une communication par email réussie et sécurisée, vous devez authentifier le sous-domaine utilisé via le Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) et DMARC.

Seule l'interaction de ce trio garantit que le domaine est correctement configuré, authentifié et reconnu par les FAI. Par ce moyen, les annonceurs consolident leur réputation et leur crédibilité vis-à-vis des FAI.

L'authentification DMARC nécessite un alignement de domaine. Comment ? Très simple : Envoyez des courriers authentifiés. Pour que votre fournisseur de marketing par email puisse envoyer vos newsletters signées et authentifiées en votre nom, il doit avoir l'autorisation appropriée pour votre sous-domaine via un enregistrement dans le système de noms de domaine (DNS). Comme le DMARC est basé sur SPF et DKIM, l'expéditeur et le contenu du courrier sont tous deux authentifiés. C'est la seule façon pour l'expéditeur de se construire sa réputation.

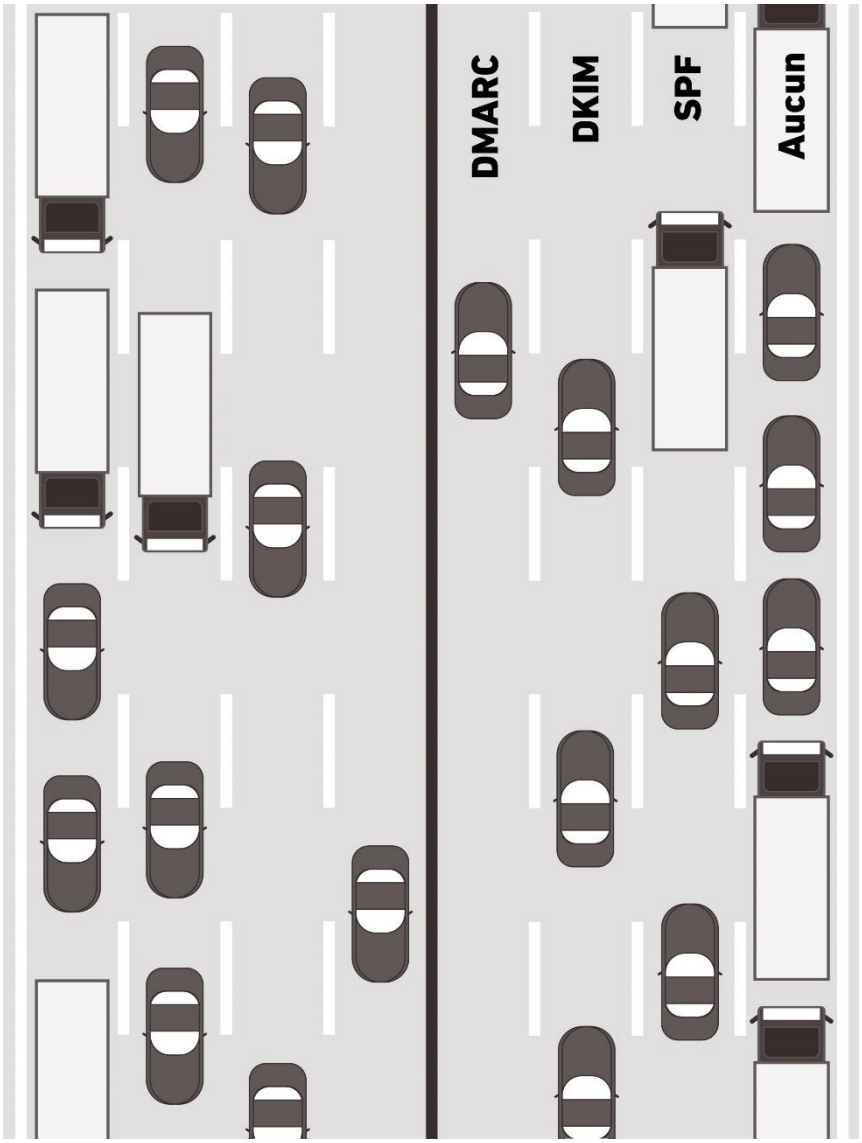
Comment ces trois spécifications SPF, DKIM et DMARC peuvent être comparées à une autoroute :

- Si vous n'utilisez aucune des trois spécifications, vous serez bloqué dans un embouteillage.
- Le SPF est représenté par la voie de droite et donc la plus lente : Cette procédure ne vérifie qu'un seul critère, à savoir l'authenticité de l'adresse de l'expéditeur, mais n'est pas exclusif.
- DKIM représente la voie du milieu : Cette norme permet non seulement de vérifier l'authenticité de l'adresse de l'expéditeur, mais aussi de s'assurer que le contenu du courrier et certaines informations de l'en-tête n'ont pas été manipulés.
- DMARC représente la gauche, c'est-à-dire la voie la plus rapide : La spécificité du DMARC est qu'il combine les deux autres et qu'il est plus explicite. Il définit exactement ce qu'il adviendra du courrier si le SPF et le DKIM échouent. Avec le DMARC, vous

roulez sur la voie de gauche, aussi longtemps que la réputation de votre domaine est positive.

En résumé, la meilleure façon de garantir la réussite et la sécurité des communications par email est d'utiliser les trois méthodes d'authentification SPF, DKIM et DMARC et d'utiliser des sous-domaines pour l'envoi.

Et une remarque : un commerçant sans DMARC est encore plus mal loti qu'un spammeur. Parce qu'ils utilisent également les trois mécanismes. Cependant, ils échouent rapidement en raison de la réputation.



SPF, DKIM et DMARC l'exemple de l'autoroute

Email Marketing conforme à la législation

La configuration technique effectuée, que peuvent faire les marketeurs pour s'assurer que leurs emails se retrouvent bien dans la boîte de réception de leurs destinataires ? Dans ce qui suit, nous avons compilé des mesures pour un Email Marketing conforme à la loi.

Pas d'achat d'adresses

L'achat d'adresses email peut sembler tentant, mais il doit être évité si possible - pour les raisons suivantes :

› L'achat d'adresses est illégal : il viole les règles de protection des données, car les personnes contactées ne peuvent pas révoquer efficacement leur consentement.

› L'achat d'adresses ne permet pas au commerçant de disposer d'adresses de haute qualité : Souvent, les adresses achetées sont non seulement anciennes ou non valides, mais elles peuvent aussi contenir des pièges à spam qui conduisent à l'inscription sur une liste noire. Nous expliquerons plus en détail le terme "liste noire" dans les paragraphes suivants.

› L'achat d'adresses n'est pas efficace : aucun commerçant n'a besoin dans sa liste de diffusion de destinataires non concernés par son secteur et qui n'ont aucune appétence pour ses produits ou services.

La location d'adresses et la Co-Registration ou co-sponsoring sont des options éventuelles pour la mise en place d'une liste de diffusion. Bien qu'elle soit autorisée sous certaines conditions, la location d'adresses ne vous donne pas accès aux données elles-mêmes - si elle le fait, elle est contraire à la protection des données. Dans les deux cas, la qualité de la liste de diffusion, défini par un groupe cible ou qualifiée, est incertaine. En outre, la confiance dans les partenaires contractuels est fondamentale.

Liste de diffusion et Opt In

Il est plus efficace d'utiliser le marketing de permission pour constituer votre propre liste de diffusion. C'est plus exigeant, mais aussi plus efficace à long terme. Nous vous recommandons de mettre en place un formulaire d'inscription à newsletter attrayant avec une procédure de double opt-in conforme à la législation.

Comme son nom l'indique, deux étapes sont nécessaires pour l'abonnement en double opt-in : Après avoir rempli le formulaire d'inscription, l'intéressé recevra un email avec un lien de confirmation. Ce n'est que lorsqu'il a cliqué sur ce lien qu'il est inscrit

sur la liste de diffusion et que son consentement est effectif. Cela permet non seulement de vérifier si l'adresse électronique est valide, mais aussi d'éviter les erreurs de frappe et les abus. En outre, les rebonds inutiles sont évités. Naturellement, seules les adresses avec confirmation en double opt-in doivent être adressées par email. Les professionnels marketing doivent construire eux-mêmes leur base d'adresses. Qu'il s'agisse d'une demande en ligne par le biais d'une case à cocher dans différents points de contact avec les clients, d'une demande hors ligne dans des documents imprimés ou des réunions avec des clients, il existe de nombreux moyens conformes à la loi pour promouvoir l'inscription à la newsletter.

Procédure de désinscription simple

Cela semble paradoxal, mais faites-en sorte que vos destinataires puissent se désabonner le plus facilement possible de la lettre d'information. Avec une procédure de désabonnement compliquée, il semble souvent plus facile pour les abonnés de classer le courrier comme spam en un seul clic. Si plusieurs destinataires choisissent cette option, la réputation de l'expéditeur en souffre, ce qui a un effet négatif sur le taux de livraison. En outre, le risque d'être classé comme spammeur augmente. C'est la raison pour laquelle nous vous recommandons un désabonnement en un Single Opt out.

Cela signifie que le destinataire doit pouvoir se désinscrire de la liste de diffusion à tout moment en un seul clic. Un lien de désabonnement doit faire partie de chaque newsletter - c'est une obligation légale. En outre, la fonctionnalité List Unsuscribe Header- dont nous parlerons plus en détail dans la troisième partie de ce livre blanc - est un moyen de se désabonner de la newsletter. Si le suivi personnel est utilisé, l'envoi doit également contenir le lien vers l'autorisation de suivi afin que le destinataire puisse la révoquer si nécessaire. Des systèmes professionnels d'Email Marketing peuvent vérifier automatiquement si le lien de désabonnement, le List Unsuscribe Header et le lien de permission de suivi sont présents dans le mailing avant de l'envoyer.

Les adresses désinscrites ne doivent pas être adressées par email, même accidentellement, à un nouveau destinataire importé. Des listes noires internes ou des Black List dans les systèmes d'Email Marketing permettent d'éviter cela.

Entretien de listes et gestion des rebonds

La création et la gestion de votre propre liste de diffusion grâce à un marketing de permission est la clé de voûte d'un Email Marketing efficace. Mais quelle que soit la qualité d'une liste de diffusion, les rebonds ne peuvent être complètement évités. Dans la

première partie de ce livre blanc, nous avons déjà expliqué l'importance de la gestion automatisée des rebonds de la solution d'Email Marketing utilisée. Quelles autres mesures pouvez-vous prendre en tant que marketeur pour maintenir le taux de rebond le plus bas possible ?

Si un système CRM est utilisé pour gérer les données des destinataires, un contrôle syntaxique doit être effectué pour s'assurer que les adresses électroniques sont correctes avant de les transférer à la solution d'Email Marketing. Les solutions d'Email Marketing professionnelles effectuent automatiquement cette vérification avant chaque importation. Les adresses électroniques incorrectes, par exemple sans signe @ ou avec des caractères non valables, ne sont pas enregistrées dans la liste de diffusion.

Une fois envoyées, les informations sur les rebonds ne sont pas seulement pertinentes pour l'Email Marketing, mais aussi pour la communication globale avec les clients. Il est donc recommandé de comparer les rebonds avec votre propre CRM ou d'autres bases de données d'adresses utilisées dans votre entreprise. Un conseil : si un fournisseur internet vous renvoie un nombre important de Hard et Soft bounces, cela peut signifier qu'il vous bloque comme expéditeur. Dans ce cas, contactez ce fournisseur de messagerie électronique ou votre routeur d'Email Marketing. Important : les adresses bloquées ne doivent pas être contactées à nouveau.

Effets du contenu et de l'expédition des Emailings sur la délivrabilité

Dans cette section, nous expliquons comment les professionnels marketing peuvent agir sur leur réputation et leur capacité de livraison en créant et envoyant leurs mailings

Les mots, les images et leurs interactions

L'Email Marketing sérieux exige un contenu pertinent. Que devez-vous donc prendre en considération pour choisir les mots et les images ?

Afin de ne pas déclencher les filtres anti-spam, il est important de toujours saisir l'adresse complète de l'expéditeur et de ne pas utiliser de domaines tels que ".biz" ou ".info".

Dans l'objet ainsi que dans le reste des textes de la newsletter, il est important d'éviter les termes de spam : Des mots tels que "gratuit" et "argent" ou des expressions telles que "votre famille", "votre travail" sont souvent associés à des courriers indésirables douteux par les filtres antispam et triés en conséquence. Même les phrases qui utilisent à la fois des points d'interrogation et des points d'exclamation sont sanctionnées par certains filtres antispam. Il en va de même pour les longues chaînes de caractères en majuscules et les symboles et caractères spéciaux trop utilisés, tels que le symbole du dollar ou de l'euro. Il convient également d'éviter les textes dont la taille de la police est trop petite ou trop grande.

Nous recommandons d'insérer principalement des images appelées car le risque de spam est plus faible qu'avec les images intégrées. Les images appelées n'influencent pas la taille de l'envoi or les filtres antispam sont toujours plus attentifs pour emails volumineux, car ils peuvent contenir des pièces jointes cachées. Le risque d'être classé comme spam augmente avec la taille de l'email. En outre, le faible volume d'un email permet un envoi plus rapide, des temps de chargement plus courts et un espace de stockage réduit dans la boîte de réception du destinataire. En revanche, le contenu des images appelées n'est visible qu'après rechargement. Ainsi, les images essentielles à la reconnaissance, telles que le logo de l'entreprise, doivent de préférence être intégrées dans la partie supérieure de l'email.

Un rapport texte-image équilibré est un critère important pour les filtres anti-spam et doit être adapté au secteur d'activité concerné (B2C, B2B), à la marque et à l'objectif du mailing (communiqué de

presse, présentation du produit, etc.). Un trop grand nombre d'images donne rapidement l'impression que la newsletter est surchargée et peut entraîner des temps de chargement et des volumes de données excessifs, en particulier pour les destinataires mobiles. Par conséquent, la partie textuelle d'un envoi doit toujours être prédominante. Lors de la conception de la mise en page, il est également important de veiller à ce qu'il y ait un contraste suffisant entre la police et la couleur de fond.

En outre, la pertinence joue un rôle important. L'ensemble du contenu doit être adapté au groupe cible et être compréhensible. La règle suivante s'applique ici : plus le courrier électronique est individuel et personnel, plus il a du succès. Les éléments de conception utilisés doivent faire directement référence au texte et représenter un avantage supplémentaire pour le lecteur. Si un abonné ne peut rien faire avec le contenu de l'email, il est plus enclin à cliquer sur le bouton "spam".

De même, les raccourcisseurs d'URL ne sont pas un outil approprié pour raccourcir les URL longs.

Souvent, ces domaines sont mis sur liste noire parce qu'ils sont également utilisés par les spammeurs. Il est plus judicieux d'utiliser votre propre domaine.

Tests de qualité avant l'expédition

Afin d'éliminer d'éventuelles sources d'erreur avant l'envoi, il est essentiel de tester la qualité d'un email. De nombreuses solutions d'Email Marketing proposent divers tests de qualité et, en fonction des résultats, indiquent un éventuel besoin de correction.

Ci-dessous, nous avons examiné les tests de qualité qu'Inxmail Professional propose en standard. Ils peuvent varier en fonction du fournisseur d'Email Marketing:

Le **test de délivrabilité** vérifie la possibilité que le mailing soit livré. En d'autres termes, le test vérifie s'il existe un enregistrement SPF pour le serveur de messagerie dans le serveur DNS du domaine. Si l'entrée du SPF est positive, le serveur de messagerie est autorisé à envoyer des mailings sous ce domaine et le mailing est envoyé. En cas d'entrée négative du SPF, l'envoi via ce serveur de messagerie est interdit. Si le serveur de messagerie n'est même pas mentionné dans l'entrée SPF, l'envoi du courrier n'est pas empêché. Toutefois, il est possible que certains fournisseurs donnent une note négative au message ou rejettent l'envoi. S'il n'y a pas d'entrée SPF pour le domaine, l'expéditeur doit être accepté. Le courrier est envoyé. Certains fournisseurs donnent des points bonus pour une entrée correcte et existante dans le SPF. Le **test antispam** est également

important pour la délivrabilité. Car même si une entrée SPF valide est présente, le courrier peut toujours se retrouver dans le dossier spam du destinataire. Le contenu de l'envoi en est responsable. Ce test vérifie donc le contenu et l'objet à la recherche d'éléments relevant de spam.

EXPOSE

Le spam (en anglais, "trash" ou "junk") est l'envoi de courrier électronique non sollicité. Un courrier électronique est considéré comme indésirable s'il est envoyé au destinataire sans son consentement explicite ou du moins présumé. Les expéditeurs douteux finissent sur des listes noires publiques. Outre les listes blanches, il existe également des bases de filtrage des emails côté serveur et client. Ils comprennent des serveurs de messagerie inconnus ou peu fiables dont les emails sont ensuite immédiatement filtrés et rejetés. En plus des listes noires publiques, les fournisseurs et les destinataires d'emails peuvent établir leurs propres listes noires. Les fournisseurs d'emailing demandent la suppression d' entrées en liste noire, moyennant des frais et pour une raison plausible.

Le **test anti-phishing** examine les liens de l'envoi pour détecter les caractéristiques de phishing. Le phishing est une tentative d'accès aux données d'un internaute par le biais de fausses adresses www. L'adresse réelle est cachée. Par conséquent, ne donnez jamais une adresse web comme description d'un lien, mais un texte descriptif du lien.

Le **test d'affichage** ne doit pas non plus être négligé. Il vérifie l'affichage du courrier à envoyer dans différents clients de messagerie. Par exemple, si un email ne s'affiche pas correctement sur un appareil mobile, le destinataire a tendance à appuyer sur le bouton "spam".

En outre, ces tests doivent aussi être effectués avant l'envoi:

- Le test de liens vérifie si tous les liens de l'email sont actifs et redirigent vers la page cible souhaitée.
- Le test de taille détermine la taille que l'envoi aura dans la boîte de réception du destinataire.
- Le test de désinscription vérifie si le lien de désinscription obligatoire est présent et, éventuellement, si l'en-tête List-Unsubscribe est défini.
- Si le suivi personnel est utilisé, le test de révocation de l'autorisation de suivi vérifie si le lien obligatoire existe dans l'email

afin que les destinataires puissent annuler leur consentement à ce suivi.

Les profils de test peuvent également être utilisés pour tester l'exactitude de contenus personnalisés spécifiques à un groupe cible, comme la forme de l'adresse.

TESTS DE QUALITÉ AVEC INXMAIL PROFESSIONAL

Comme mentionné au début de cette section, vous pouvez effectuer tous ces tests de qualité en standard dans Inxmail Professional avant l'envoi. Ils sont intégrés directement dans le workflow afin de ne pas être oubliés. En quelques étapes seulement, vous serez guidé à travers le processus de test, qui garantit que tous les liens fonctionnent, que l'envoi est conforme aux exigences légales et qu'il parvient à vos destinataires rapidement et en toute sécurité. Et si un résultat de test nécessite des modifications de l'envoi, le système vous le signalera.

Tester Inxmail Professional :
www.inxmail.fr/test-gratuit

Au sujet de l'envoi et Throttling

› La fréquence d'envoi peut avoir une forte influence sur la liste de diffusion de votre newsletter La fréquence d'envois ne doit en tout cas pas être trop élevée afin de ne pas irriter le destinataire et être sanctionnée par une désinscription. En effet, c'est une des premières causes de désinscription. Pire encore, si la fréquence de vos envois incommode trop votre destinataire, celui-ci appuiera sur le bouton spam. Comment pouvez-vous empêcher cela ?

› Pertinence des mots-clés : N'envoyez que si vous avez quelque chose à dire.

› Contrôle de la pression marketing : les systèmes modernes d'Email Marketing permettent de réguler automatiquement la fréquence des emails. Ceci est particulièrement utile si un lecteur s'est abonné à plusieurs newsletter via un même portail.

› Profil de l'utilisateur : le lecteur doit pouvoir définir la fréquence à laquelle il souhaite recevoir les mailings - idéalement, il peut le faire dès son inscription à la newsletter et à tout moment par la suite.

› Maintenir des intervalles de temps : Si vous avez promis un rythme d'envois de 14 jours lors de l'inscription à la newsletter, par exemple, vous devez vous y tenir.

› Tester : il est difficile généraliser sur la fréquence optimale d'expédition. Vous pouvez utiliser des split tests pour évaluer la fréquence préférée de votre lectorat ou vous pouvez exploiter les préférences données lors de l'inscription.

En ce qui concerne **l'heure d'envoi**, nous vous déconseillons l'envoi de campagnes d'emailing à heure pleine. En effet, de nombreux expéditeurs peuvent envoyer à ce moment et entraîner une surcharge des mail serveurs de réception. Ceci retardera la livraison de vos emails. Il est préférable d'envoyer de manière contracyclique.

Le **volume des envois** joue également un rôle dans la classification en tant qu'expéditeur de bonne réputation. Il convient d'éviter les fluctuations trop importantes dans le volume des envois, cela peut être un indicateur de spam pour les FAI. Essayez de maintenir un volume stable d'emails. Si un volume plus important est nécessaire, par exemple lors d'occasions spéciales, il est conseillé d'augmenter lentement et régulièrement votre volume d'envoi.

Throttling (français Réduction) peut également augmenter le risque d'être classé comme spammeur. Par cette méthode, les routeurs d'Email Marketing fixent un nombre maximum possible d'emails par expéditeur pour un laps de temps donné. Par exemple, si une liste de distribution contient de nombreuses adresses Yahoo et que la limite d'emails du routeur est dépassée lors de l'envoi, les emails peuvent être bloqués ou se retrouver directement dans le dossier de courrier indésirable du destinataire. Ici, elle peut également contribuer à réduire le volume et/ou la fréquence des envois ou à les sélectionner en fonction des groupes cibles et à leur écrire de manière différée et " petit à petit ".

Checkliste

Avez-vous pensé à tout ? Consultez notre checklist, qui récapitule les critères les plus importants que vous devez prendre en considération en tant que marketeur :

TECHNIQUE

- ☐ Créer un sous-domaine spécifique par type de mailing, par exemple pour les newsletters ou les emails transactionnels
- ☐ Indiquer au fournisseur d'email marketing le sous-domaine dédié pour l'authentification et le faire enregistrer comme domaine de suivi auprès du prestataire d'email marketing
- ☐ Mettre en place SPF, DKIM et DMARC pour le sous-domaine dédié
- ☐ Une fois qu'un sous-domaine dédié a été créé et que les SPF, DKIM et DMARC ont été mis en place, il est souhaitable de ne pas changer les adresses ou les domaines d'expéditeurs

DROIT

- ☐ Pas d'achat d'adresses
- ☐ Lise de diffusion avec consentement et procédure de double opt-in
- ☐ Bonne visibilité du lien de désabonnement dans l'email, si nécessaire également un lien d'autorisation de suivi
- ☐ Vérifiez que la fonction List-unsuscribe est disponible
- ☐ N'envoyer qu'à des adresses avec consentement par double opt-in et non à celles qui ont été désinscrites ou bouncées
- ☐ Utiliser un logiciel d'Email Marketing avec gestion intégrée des rebonds

CONTENU

- ☐ Éviter les mots et les caractères qui pourraient alerter les filtres anti-spam
- ☐ Créer un lien avec les images plutôt que les intégrer
- ☐ Rapport texte/image équilibré
- ☐ Contenu pertinent
- ☐ Ne pas utiliser de raccourcisseurs d'URL
- ☐ Effectuer des tests de qualité avant l'envoi
- ☐ Trouvez la fréquence d'envoi et respectez-la sans exception.
- ☐ Ne pas envoyer de campagne en heure pleine
- ☐ Éviter les fortes fluctuations des volumes d'envoi
- ☐ Envisager de réduire la vitesse d'envoi

Partie 3: Caractéristiques de délivrabilité et de qualité des fournisseurs d'Email Marketing

Critères qualitatifs

Les points suivants sont à considérer dans le choix du prestataire d'emailing

- Reconnu comme expéditeur sérieux par tous les fournisseurs d'accès Internet (FAI) pertinents au niveau international.
- Contact direct du fournisseur d'emailing avec les fournisseurs d'accès internet internationaux.
- Connexion sécurisée aux serveurs de messagerie et bases de données.
- Contrôle proactif des envois par le fournisseur d'emailing.
- Formulation de recommandations spécifiques sur les mesures à prendre si des problèmes de délivrabilité sont constatés.

Inxmail répond à toutes les caractéristiques de qualité ci-dessus. Nous considérons que la collaboration avec des clients et des partenaires de bonne réputation et une bonne installation technique vont de soi. Nous répondons aux exigences strictes des FAI et respectons les directives relatives aux expéditeurs de Google, Orange, Microsoft, Verizon Media et United Internet Media, entre autres. Afin d'offrir à nos clients la plus grande fiabilité de livraison possible, nous sommes en contact avec les plus importants fournisseurs d'accès Internet dans le monde. Nous surveillons l'expédition et sommes vigilants sur les listes noires et les évaluations Sender-Score. Si nous constatons un besoin d'optimisation, nous agissons immédiatement. Nos clients reçoivent des recommandations individuelles sur les mesures à prendre si nous constatons des problèmes de délivrabilité.

Whitelisting et le rôle du CSA

Le Certified Senders Alliance (CSA) a été créé en 2004. Il s'agit d'un projet de l'association de l'industrie allemande de l'Internet eco e. V. et de l'association allemande de marketing de dialogue (DDV). L'objectif du projet est de s'assurer que l'email envoyé par un prestataire d'Email Marketing réputé avec le consentement du

destinataire parvient effectivement à ce dernier. En d'autres termes : l'envoi ne doit pas être bloqué dans le filtre anti-spam du fournisseur d'accès au courrier électronique.

Les membres du CSA sont automatiquement inscrits sur les listes blanches des plus importants fournisseurs d'accès Internet internationaux. L'adhésion est payante, mais elle est essentielle pour les expéditeurs professionnels d'emails. En effet, de nombreux fournisseurs d'accès à internet ont délégué au CSA la gestion de leur liste blanche.

Pour être inclus dans la liste, certains critères doivent être remplis. Le respect de ces lignes directrices est contrôlé par un organe de surveillance. L'avantage de cette liste centrale est que vous ne vous inscrivez qu'une seule fois pour figurer sur la liste blanche de tous les prestataires participants.

Inxmail est certifié comme un expéditeur réputé par les plus importants fournisseurs de services Internet. Les serveurs Inxmail sont inscrits sur les listes blanches des fournisseurs les plus connus. Nous sommes, entre autres, un expéditeur certifié et un membre fondateur du CSA, le premier projet Whitelisting à l'échelle de l'Allemagne. Cela signifie que nous remplissons toutes les conditions fixées par le CSA pour l'adhésion et l'affiliation. Nos services vont de la conformité RFC des emails, de l'authentification DKIM, des en-têtes de désabonnement de liste au respect de divers quotas concernant les rebonds, le spam et la réputation. Les critères d'adhésion détaillés peuvent être téléchargés et consultés directement auprès du CSA.

Une association mondiale : Messaging Malware Mobile Anti-Abuse Working Group (M3AAWG)

Avec plus de 200 membres dans le monde entier, le M3AAWG est la plus grande association sectorielle mondiale qui lutte contre les botnets, les malwares, le spam, les virus, les attaques par déni de service et d'autres formes d'abus sur Internet. Le M3AAWG rassemble des acteurs de la communauté digitale en un forum

d'échanges ouverts et confidentiels et développe des approches collaboratives pour lutter contre les abus en ligne. Le M3AAWG a été fondé en 2004 et est un organisme de travail indépendant de toute technologie et de toute politique.

Les membres se réunissent trois fois par an pour un échange d'informations, principalement pour lutter contre les abus dans la distribution d'emails. Des experts du monde entier élaborent des solutions et des recommandations pour lutter contre les menaces actuelles et mettent en œuvre ce qui a été discuté lors des conférences.

Inxmail est un membre officiel du M3AAWG depuis octobre 2019. En tant que fournisseur de routage réputé, nous considérons qu'il est de notre devoir de prendre des mesures actives, à l'échelle mondiale, contre les nouveaux abus dans la communication par email. L'échange international et régulier d'informations nous permet d'être toujours au fait des nouveaux enjeux et menaces et d'en tirer rapidement des contre-mesures appropriées.

Exigences techniques

En ce qui concerne les exigences techniques en termes de délivrabilité maximale, les points suivants doivent notamment être pris en compte pour les envois d'email marketing :

- Le système d'expédition devrait fournir des informations sur la gestion des rebonds et l'état des emails livrés et non livrés.
- La solution d'email marketing doit permettre l'insertion d'un List-Unsubscribe-Header pour la désinscription à la newsletter.
- Domaines d'expédition librement paramétrables et authentification avec les procédures les plus courantes telles que SPF, DKIM et DMARC ainsi qu'un alignement (complet) des domaines.

Les Feedback Loops et la gestion des rebonds garantissent une liste de destinataires propre

De nombreux FAI proposent à leurs utilisateurs de classer un email non sollicité dans leur boîte aux lettres comme "spam". Grâce à ces informations, les FAI essaient de configurer leurs filtres anti-spam en fonction des utilisateurs afin de les protéger contre d'autres spams. Il arrive qu'un utilisateur clique sur ce

bouton par erreur ou ne fasse pas confiance au lien de désabonnement dans la newsletter et clique sur "Spam" au lieu de se désabonner. Et dans ce cas, l'expéditeur ne sait pas que le destinataire ne veut plus recevoir sa newsletter et continue à l'adresser.

Certains FAI offrent la possibilité de signaler à l'expéditeur le classement de l'email comme spam par un destinataire. Ce mécanisme s'appelle Feedback Loop. Pour une gestion efficace des rebonds et, là encore, pour protéger la réputation, l'expéditeur saisit ces informations et retire le destinataire de la liste de diffusion. Dans le meilleur des cas, la boucle de rétroaction (Feedback Loop) est enregistrée de manière centralisée, documentée et traitée automatiquement par l'expéditeur.

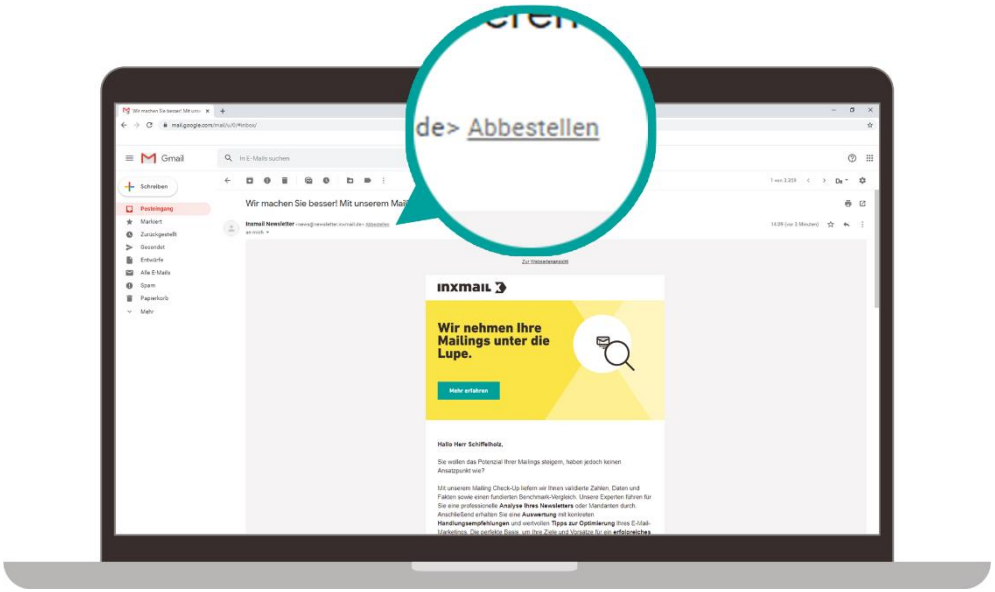
Les clients d'Inxmail n'ont pas à se soucier de l'enregistrement ou de la configuration des boucles de rétroaction (Feedback Loops). En tant qu'expéditeur technique, nous recevons un retour d'information de tous les FAI qui proposent des boucles de rétroaction. Celles-ci sont traitées automatiquement : Les destinataires concernés sont marqués comme "non disponibles" et exclus des envois ultérieurs. Cela protège votre réputation en tant qu'expéditeur et a un effet positif sur vos chiffres clés.

Les règles en constante évolution pour le traitement des rebonds et le filtrage du spam sont toujours prises en compte dans notre solution d'Email Marketing pour la gestion des rebonds et les tests de qualité. Nous aidons ainsi nos clients à maintenir le taux de délivrabilité de leurs envois à un niveau élevé.

List-Unsubscribe-Header pour le désabonnement à la newsletter

En plus du lien de désabonnement et de l'email de désabonnement, le List-Unsubscribe-Header est une autre façon de se désabonner de la newsletter. Si le client de messagerie du destinataire prend en charge cette fonction, un bouton permettant de se désabonner de la newsletter s'affiche dans l'interface utilisateur. Si le destinataire clique dessus, il sera retiré de la liste de diffusion. Les informations supplémentaires de désabonnement non visibles par le destinataire sont transférées dans le code source du courriel. L'en-tête de désabonnement à la liste n'a aucun effet sur la conception de la newsletter et est pris en charge par de nombreux grands fournisseurs d'emails tels que Outlook.com, GMX, Yahoo,

AOL et Gmail.



List-Unsubscribe dans Gmail

Pour les destinataires, le List-Unsubscribe-Header signifie avant tout un gain de commodité grâce au placement uniforme du bouton. Contrairement au lien de désabonnement classique dans le pied de page, il n'est pas nécessaire d'ouvrir et de faire défiler le mailing jusqu'à la fin.

Dans le passé, des liens de désabonnement difficiles à trouver ont souvent amené les destinataires à marquer les emails comme spam au lieu de se désabonner normalement. Dans certains cas, cela a pu amener à rejeter certaines informations attendues. Ce marquage a un effet négatif sur la réputation de l'expéditeur et la délivrabilité de la newsletter.

Le CSA exige de ses membres et de leurs clients qu'ils incluent un "List-Unsubscribe" dans l'en-tête de l'email. Dans notre solution d'Email Marketing, cette fonction est disponible en standard.

Authentification de l'email au niveau de l'expéditeur technique

Nous avons déjà présenté en détail les différentes procédures d'authentification du courrier électronique (SPF, DKIM et DMARC) dans la première et la deuxième partie. L'authentification de l'adresse de l'expéditeur aide les FAI à filtrer les courriers électroniques en spam et non-spam et garantit que les emails ne sont pas rejetés par erreur. Les avantages sont un taux de délivrabilité élevé et une bonne réputation du domaine.

Les routeurs d'emailing certifiés CSA sont tenus d'authentifier tous les emails sortants à l'aide des techniques d'authentification SPF et DKIM. Toute personne qui enfreint cette obligation est susceptible d'être temporairement exclue du CSA. En règle générale, cela signifie que tous les serveurs de messagerie enregistrés chez l'expéditeur sont retirés de la liste blanche du CSA.

L'alignement des domaines est indispensable lors de l'envoi via les routeurs d'emails

Quiconque veut utiliser le DMARC comme méthode d'authentification ne peut se passer de l'alignement de domaine. Avant de pouvoir expliquer le terme "alignement de domaine", il faut d'abord comprendre que les emails ont toujours deux adresses d'expéditeur.

L'adresse « From" fait référence à l'adresse qui est affichée au destinataire dans sa messagerie. L'adresse "Mail From" est stockée dans l'en-tête de l'email en tant que "Return Path". Par rapport à une lettre classique, l'adresse « From" décrit l'auteur de la lettre, qui est indiqué dans l'en-tête de la lettre. L'adresse "Mail From" se trouve en tant qu'expéditeur sur l'enveloppe utilisée pour envoyer la lettre. Si la Poste ne peut pas livrer la lettre au destinataire, la lettre sera renvoyée à l'expéditeur désigné sur l'enveloppe. Appliqué au marketing par email, cela signifie que la notification de la non-livraison du courrier électronique est envoyée à l'adresse "Mail From".

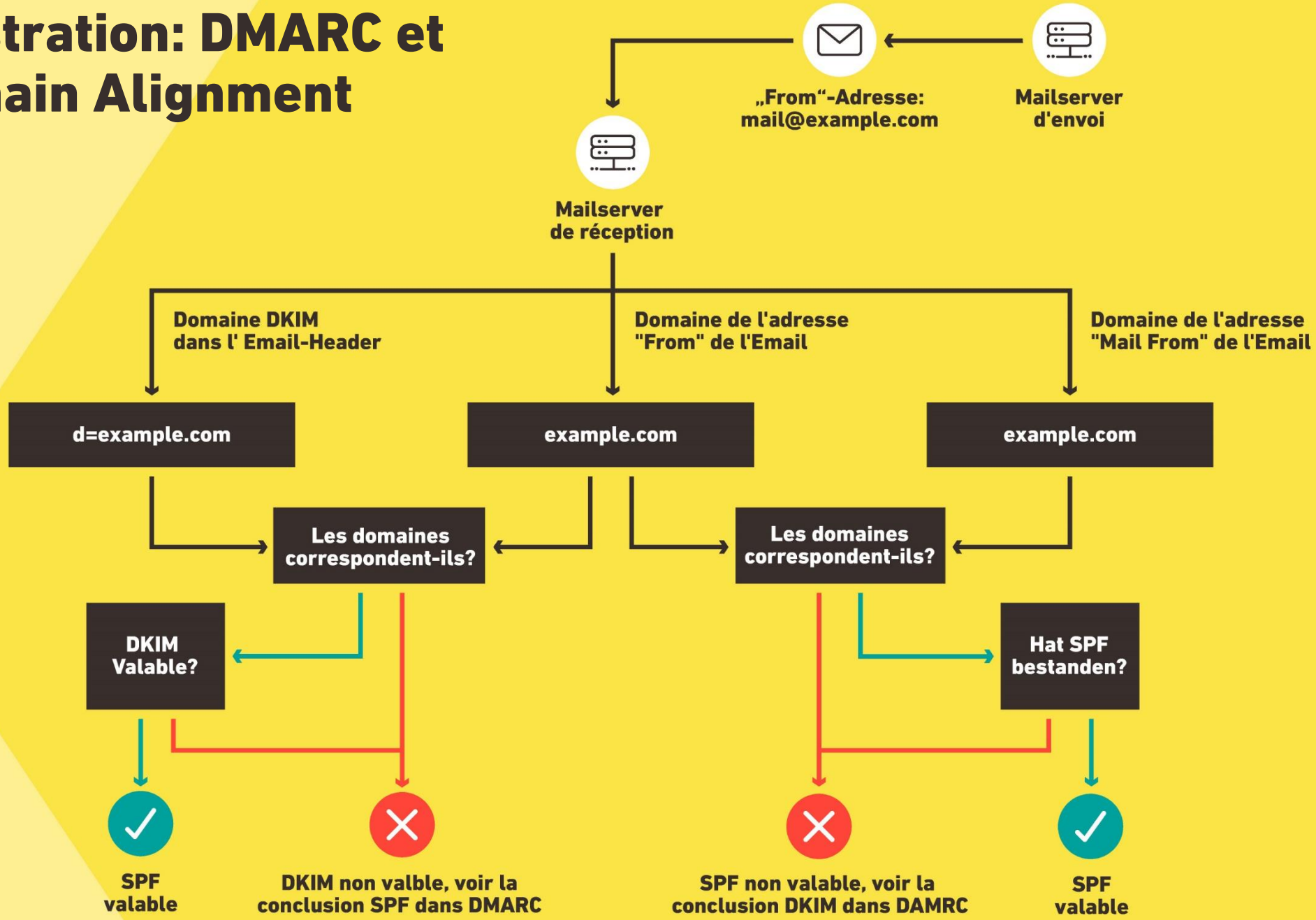
L'alignement des domaines signifie que les domaines utilisés dans SPF et DKIM doivent partiellement correspondre à l'adresse "From" du courriel. Appliqué à notre distribution classique du courrier, cela signifie que l'expéditeur de l'enveloppe doit correspondre à l'expéditeur de la lettre ainsi qu'à la signature de la lettre (le domaine DKIM). De cette façon, le destinataire reconnaît qu'il peut classer l'expéditeur comme étant digne de confiance.

À première vue, cela semble évident. Alors pourquoi l'alignement est-il si important ? De nombreuses entreprises font appel à des routeurs professionnels pour leur Email Marketing. Et il est donc évident que dans cette constellation, l'adresse "de" du courrier électronique et l'adresse physique ne correspondent plus. Un alignement de domaine n'est plus assuré.

Les filtres antispam réagissent à différentes spécifications de domaines dans un email, comme l'adresse « From" et "Mail From" et le domaine de suivi des liens. Pour une délivrabilité élevée, il est donc important que votre fournisseur d'Email Marketing puisse configurer le même domaine pour les différents paramètres. L'alignement de domaine ou l'alignement complet de domaine (comprend également le domaine de suivi de lien utilisé) rend tous les paramètres dans l'email avec votre nom de marque visible et reconnaissable. Elle garantit également que votre identité n'est pas utilisée de manière abusive sur internet.

Inxmail permet à ses clients de réaliser l'alignement de domaine ou l'alignement complet de domaine.

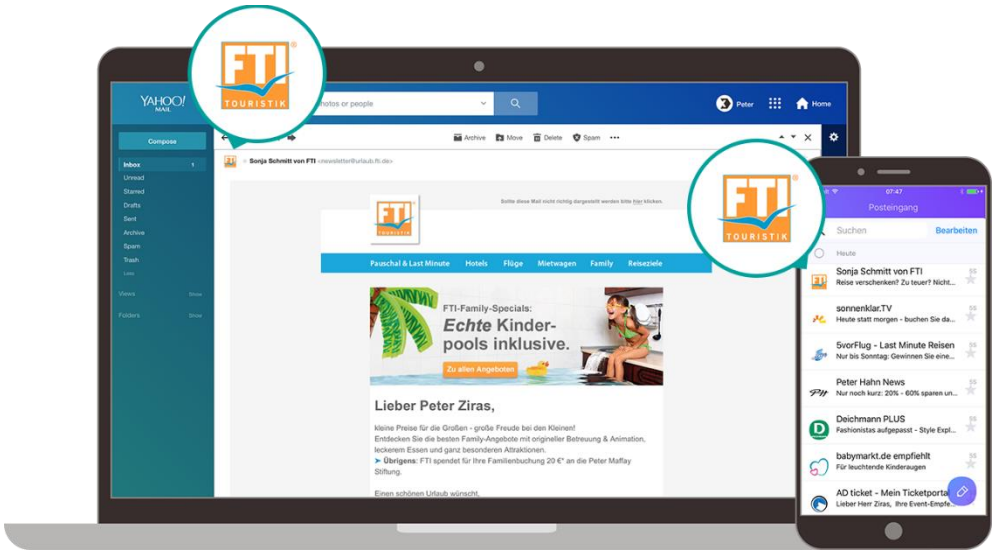
Illustration: DMARC et Domain Alignment



Augmentez votre visibilité en utilisant Brand Indicators for Message Identification

Une procédure supplémentaire permet aux consommateurs de détecter plus facilement les emails frauduleux dans leur boîte de réception. Avec les Brand Indicators for Message Identification (BIMI), une initiative des plus grands fournisseurs de messagerie du monde, comme Yahoo, introduit une norme intersectorielle dans l'Email Marketing. Il apparaît que de plus en plus de clients de messageries électroniques et de FAI soutiendront cette norme à l'avenir. Après l'affiliation de Google à l'été 2020, d'autres fournisseurs suivront probablement et le BIMI s'imposera comme la norme. Grâce au BIMI et à l'affichage du logo de la marque, les destinataires peuvent voir dans leur boîte de réception, au premier coup d'œil, si un courriel provient réellement de l'expéditeur spécifié. Il est ainsi plus facile pour eux de voir s'il s'agit d'une tentative d'hameçonnage. Le phishing est d'ailleurs un email frauduleux qui imite des expéditeurs de confiance tels que des banques ou des boutiques en ligne afin d'accéder à des données sensibles.

Le préjudice est causé aux destinataires, mais aussi aux entreprises, car les plaintes pour spam ont un impact négatif sur la réputation du domaine de la marque.



Une plus grande visibilité de la marque dans la boîte de réception grâce au processus BIMI

Si le BIMI est utilisé par l'expéditeur, le serveur de réception vérifie si l'email provient d'un serveur d'expédition autorisé et, si le résultat est positif, affiche le logo de la marque à côté de l'adresse de l'expéditeur de l'email. Une condition préalable est que le client de messagerie électronique de réception supporte également le BIMI.

Le BIMI s'appuie sur des bases anti-spam telles que le SPF, le DKIM et le DMARC. L'expéditeur est vérifié dans le BIMI à l'aide du DMARC. Les clients de messagerie emails récepteurs peuvent récupérer le logo via l'entrée DMARC du domaine d'envoi et une entrée DNS BIMI spéciale et l'afficher dans la boîte de réception.

Avec le BIMI, les entreprises bénéficient de moins de plaintes pour spam et renforcent leur réputation d'expéditeurs sérieux. En affichant le logo de la marque dans la boîte de réception, ils renforcent la confiance des destinataires et obtiennent une plus grande visibilité. Et cela conduit également à un taux d'ouverture plus élevé.

Inxmail a été le premier fournisseur d'Email Marketing au monde à mettre en œuvre avec succès le BIMI auprès de clients sélectionnés. Il s'agit notamment de FTI, Lidl, Deichmann et Peter Hahn. Avec nos clients, nous apportons ainsi une contribution importante à un marketing par email équitable et à la protection des destinataires.

Critères qualitatifs concernant la délivrabilité lors du choix d'un fournisseur d'Email Marketing:

- ☐ Certification en tant qu'expéditeur réputé, par exemple auprès du CSA
- ☐ Contact direct avec les principaux FAI internationaux
- ☐ Connexion sécurisée au serveur de messagerie et à la base de données
- ☐ Hébergement européen
- ☐ Suivi proactif de la distribution
- ☐ Fourniture de recommandations individuelles d'action en cas de problèmes de livraisons

Exigences techniques concernant la délivrabilité lors de la sélection d'une solution d'Email Marketing:

- ☐ Mise en place d'une gestion des rebonds et d'un traitement automatique des Feedback Loops
- ☐ Mise en place d'un en-tête "List-Unsubscribe" pour la désinscription aux newsletters
- ☐ Domaines d'expédition librement sélectionnables, authentification avec les procédures SPF, DKIM et DMARC et réalisation de l'alignement (complet) des domaines

Conclusion

Une bonne réputation et une bonne crédibilité sont essentielles à la réussite en Email Marketing. La réputation a une influence directe sur la délivrabilité des mailings. Grâce à diverses mesures, tant techniques que qualitatives, les entreprises peuvent s'assurer que leurs marques ne sont pas abusivement utilisées et altérées.

Lorsque vous choisissez et utilisez un système d'Email Marketing, faites attention au statut juridique et technique - qu'il s'agisse d'adhésions certifiées, de procédures d'authentification implémentables ou de fonctions importantes dans le logiciel.

Avec un fournisseur professionnel d'email marketing à vos côtés, les petits obstacles techniques lors de l'installation sont rapidement surmontés. Du marketing de permission, de la gestion des rebonds et de la conception du contenu aux tests de qualité avant l'envoi - vous aussi pouvez faire beaucoup pour que vos courriers parviennent à vos destinataires en toute sécurité.

En résumé : de nombreux facteurs influent sur la sécurité de vos envois et leur distribution aux destinataires. L'interaction de tous les facteurs et participants est importante pour atteindre des taux de livraison élevés. Les partenaires doivent se faire confiance, mais doivent également authentifier officiellement cette confiance afin qu'elle puisse être techniquement contrôlée.

Sur Inxmail

En tant que spécialiste de l'Email Marketing, nous sommes connus pour nos solutions logicielles puissantes et nos excellents services, du conseil à la mise en œuvre. Plus de 2 000 clients dans le monde entier utilisent notre logiciel pour créer des newsletters personnalisées, des campagnes automatisées et des emails transactionnels. Ils s'appuient sur la fiabilité des emails et la sécurité des données. Grâce à des interfaces de programmation, nos logiciels peuvent être mis en réseau avec de nombreux systèmes spécialisés tels que des outils de gestion de la relation client (CRM), de boutique en ligne et de gestion de campagnes.

NOUS SERONS HEUREUX DE VOUS CONSEILLER PERSONNELLEMENT!|

+33 3 59 40 02 10

contact@inxmail.fr

www.inxmail.fr/contact

Inxmail France S.A.S. 2A Avenue Auguste Wicky. 68100 Mulhouse. France

INXMAIL