Amazon Simple Email Service
Bonnes pratiques concernant l'envoi d'emails

Juillet 2012

(Veuillez consulter http://aws.amazon.com/whitepapers/
pour obtenir la dernière version de ce document)

Table des matières

Résumé

Faire en sorte que vos emails arrivent dans les boîtes de réception de vos cibles représente parfois un défi. De nombreux facteurs, notamment votre contenu, la qualité de votre liste et l'infrastructure entre vous (l'expéditeur) et votre destinataire cible, peuvent influencer la livraison de l'email. Ce document explique ces facteurs et fournit nombre de bonnes pratiques et recommandations qui augmenteront la probabilité que votre email atteigne sa cible.

Introduction

Vous pouvez envoyer un email pour différente raisons, notamment pour améliorer votre relation avec un client, faire une campagne marketing sur de nouveaux produits, apporter des conseils à un groupe de personne partageant un intérêt commun ou avertir des clients d'un événement. Voici quelques exemples :

- Des lettres d'informations (par exemple, la recette du mois pour un club culinaire)
- Des reçus (par exemple, des confirmations d'achat)
- Des itinéraires de voyage (par exemple, des billets d'avion)
- Des notifications de compte (par exemple, des réinitialisations de mot de passe)
- Des avis juridiques (par exemple, des changements dans une politique de confidentialité)

Vous pouvez qualifier de *programme de messagerie* la manière dont vous gérez la communication électronique avec vos destinataires par email.

Pour assurer le succès d'un programme de messagerie, vous devez être conscient de certains points qui peuvent affecter la livraison de vos emails et donc votre impact sur les destinataires des emails. Nous allons commencer par présenter la valeur attribuée à vos emails par vos destinataires et les fournisseurs de service Internet (ISP) responsables de la protection de leurs boîtes de réception. Ensuite, nous expliquerons à quoi ressemble le processus d'envoi des emails, quelles personnes sont impliquées et quels sont leurs rôles. Enfin, vous apprendrez à optimiser et augmenter la valeur de ces emails grâce à quelques bonnes pratiques que nous avons compilées.

Lorsque vous aurez fini de lire ce document, vous devriez disposer de bon nombre d'outils qui vous aideront à faire de votre programme de messagerie un succès !

Comment vos emails sont-ils livrés

Avez-vous déjà réfléchi à la manière dont vos emails sont livrés et pourquoi ? La *délivrabilité* fait référence à la probabilité qu'un message électronique que vous envoyez arrive effectivement à sa destination prévue. Les emails n'arrivent pas toujours jusqu'à la boîte de réception du destinataire prévu. Ils peuvent être livrés dans le *répertoire junk* (parfois appelé *dossier du courrier indésirable*), être rejetés par l'infrastructure de la messagerie du destinataire (généralement sous la forme d'un *retour à l'expéditeur*) ou complètement disparaître (par exemple, lorsque le système récepteur supprime le message sans en informer l'expéditeur ou le destinataire). Certains ISP ont créé des dossiers par défaut en fonction de l'implication de l'utilisateur pour aider les destinataires à mieux organiser leurs messages, et l'email sera livré dans ces dossiers et non dans la boîte de réception.

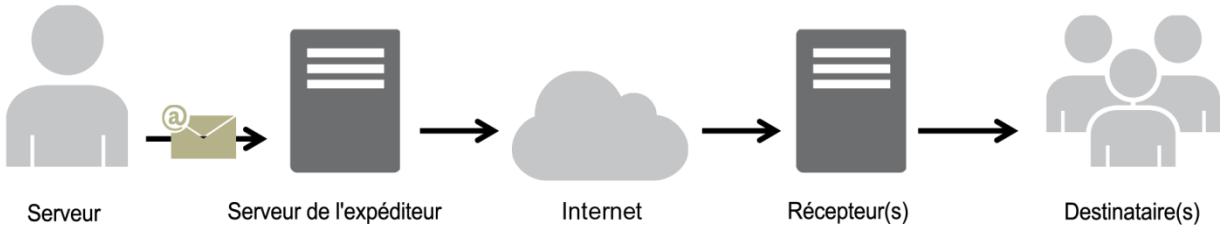
En tant qu'expéditeur, vous souhaitez que le plus de messages possibles soient livrés dans les boîtes de réception des destinataires. La meilleure manière d'améliorer la livraison consiste à envoyer un email de haute qualité, c'est-à-dire, un email que les destinataires jugent utile. Les destinataires veulent uniquement recevoir votre email s'ils peuvent tirer de la valeur de son message. Cette valeur peut se présenter sous de nombreuses formes, par exemple, des offres, des confirmations de commande, des notifications de tirage au sort, ou même des communications de réseaux sociaux. Bien sûr, le mot « valeur » peut avoir de nombreuses significations, car différentes personnes attachent de la valeur à des emails pour les raisons les plus diverses.

La *qualité d'un email* correspond à la valeur que lui attribue son destinataire. Malgré sa subjectivité, les ISP essayent de prévoir la qualité d'un email de manière aussi précise que possible à l'aide de différentes métriques pour mesurer si un message est désiré (et a donc de la valeur) ou non désiré (il est considéré alors comme un courrier indésirable, ou spam). Ces métriques incluent différents calculs internes basés sur des technologies anti-spam et les entrées du destinataire que l'ISP essaye de quantifier.

En tant qu'expéditeur, vous instaurez une relation de confiance avec un *récepteur* (la personne ou le système qui se cache derrière l'adresse de destination) en envoyant des emails de qualité au fil du temps. Cette confiance est qualifiée dans le secteur de *réputation.* Les récepteurs utilisent des métriques pour évaluer la valeur de l'email d'un expéditeur. Ces métriques sont souvent combinées en scores et correspondent généralement à la réputation d'un expéditeur.

Flux des emails

Le diagramme ci-dessous décrit les entités impliquées dans l'envoi et la réception des emails.



Récepteurs d'email et livraison des emails

Les récepteurs d'email décident si vos emails seront livrés. Ils sont constitués par la totalité de la fédération de systèmes, logiciels et stratégies réseau qui gèrent la livraison des emails. Il existe différentes classes de récepteurs d'email, et vous devez connaître la classe du récepteur auquel vous envoyez les emails pour optimiser la déliverabilité de votre programme de messagerie.

Fournisseur de service Internet (ISP)

Un ISP (fournisseur de service Internet) héberge généralement des services de messagerie pour des abonnés. Généralement, les emails B2C (entreprise à consommateur) sont envoyés à des adresses hébergées chez des ISP. Des sites comme Yahoo!, Gmail et Comcast entrent dans cette catégorie. Ces grands fournisseurs prennent des décisions sur des millions de boîtes de réception pour déterminer si votre email est un courrier indésirable, et ils basent ces décisions sur les retours des destinataires.

La plupart du temps, ces retours prennent la forme d'une plainte (lorsqu'un destinataire marque un message comme un courrier indésirable dans son client de messagerie), mais cela peut également inclure le fait que des destinataires ouvrent ou cliquent sur votre email. La quantité de retours des destinataires à la disposition d'un ISP pour les calculs de réputation est généralement élevée, mais les ISP ont tendance à implémenter un système de réputation universel pouvant être facilement déployé sur toutes les boîtes de réception.

Systèmes d'entreprise

Un système d'entreprise fait généralement référence à un système de messagerie hébergé de manière indépendante et utilisé par des employés, des étudiants, des organismes gouvernementaux, ou certaines associations à but lucratif ou non. Ce système est généralement qualifié de B2B (entreprise à entreprise). Un système d'entreprise peut également inclure les services de messagerie hébergés proposés par des ISP pour exécuter les systèmes de messagerie entrante. Souvent, les règles pour éviter le courrier indésirable sont définies par le service informatique interne, ou il s'agit des règles par défaut fournies par la solution Mail Transfer Agent (MTA) de réception d'email, comme Microsoft Exchange.

Systèmes maison

Si une boîte de réception n'est pas gérée par un service informatique, il est fort probable qu'elle fonctionne dans le cloud ou sur un serveur personnel (par exemple, installé dans le garage de quelqu'un). Un tel système maison implique que vous devez gérer un ensemble de règles non standards qui peuvent être configurées *ad hoc* par le propriétaire du serveur. Si vous souhaitez que vos emails arrivent jusqu'à la personne derrière un serveur de messagerie personnel, vous devez vous conformer à sa définition spécifique d'un email de haute qualité.

Toutes les classes de récepteurs ci-dessus utilisent plusieurs moyens de défense contre les emails non désirés. Amazon Simple Email Service (Amazon SES) gère la plupart de ces défenses pour les expéditeurs au niveau de la couche d'infrastructure (par exemple, configuration de DNS de messagerie, taux d'envoi, limitation de bande passante, nouvelles tentatives automatiques, etc.). Cependant, vous devez connaître la classe de récepteurs à laquelle vous envoyez vos emails pour respecter aux mieux ses règles de messageries et faire en sorte que vous messages arrivent dans les boîtes de réception de vos destinataires.

Pour résumer, ces sont les **destinataires qui décident !** N'importe qui peut envoyer un email, mais la livraison d'un email dans une boîte de réception est un privilège réservé aux expéditeurs qui savent respecter le destinataire.

Métriques qui définissent votre réussite

La liste de métriques suivante n'est pas conçue pour être exhaustive. Elle indique simplement des domaines dans lesquels des problèmes pourraient avoir lieu pour votre programme de messagerie. N'allez surtout pas penser qu'il suffit de gérer les métriques de ces domaines problématiques pour garantir la livraison de vos messages. N'oubliez pas que c'est vous qui connaissez le mieux vos clients.

Taux de retours à l'expéditeur

Un retour à l'expéditeur (bounce) indique le statut d'échec de la tentative de livraison. Il s'agit d'un élément d'informations utile qu'un récepteur vous renvoie.

Les récepteurs génèrent des erreurs d'adresse mail incorrecte ou inexistante, et des messages d'erreur ou d'échec provisoire. Les *erreurs d'adresse mail incorrecte ou inexistante* sont des échecs de livraison persistants (par exemple, « La boîte aux lettres n'existe pas »), alors que les *messages d'erreur ou d'échec provisoires* sont des échecs d'envoi temporaire (par exemple, « Boîte aux lettres pleine »). Les retours à l'expéditeur peuvent être synchrones ou asynchrones. Si les retours à l'expéditeur sont *synchrones*, ils sont envoyés pendant que les serveurs de messagerie communiquent. Les retours à l'expéditeur sont *asynchrones* s'ils sont envoyés après que le message a été initialement accepté pour livraison par le récepteur. Dans Amazon SES, vous ne verrez pas de réponses de succès renvoyées (c'est-à-dire, « 250 OK »). Amazon SES traite automatiquement les messages d'erreur ou d'échec provisoire en faisant de nouvelles tentatives avec les paramètres optimaux pour le domaine vers lequel vous effectuez l'envoi. Les erreurs d'adresse mail incorrecte ou inexistante sont générées en mode synchrone ou asynchrone et vous sont renvoyées automatiquement. Pour en savoir plus, consultez la section relative aux notifications de retour à l'expéditeur et de plainte dans le *manuel du développeur Amazon Simple Email Service*.

Un taux élevé d'erreurs d'adresse mail incorrecte ou inexistante indique aux récepteurs d'email que vous ne connaissez pas bien vos destinataires. Par conséquent, un taux élevé d'erreurs d'adresse mail incorrecte ou inexistante peut avoir un impact négatif sur votre déliverabilité. Vous trouverez ci-dessous des suggestions sur la façon de réduire le nombre d'erreurs d'adresse mail incorrecte ou inexistante.

Taux de plaintes

Lorsque le destinataire d'un email marque ce dernier comme étant indésirable en cliquant sur le bouton « Marquer comme courrier indésirable » dans le client de messagerie Web, l'ISP enregistre l'événement en tant que plainte. S ces événements de plainte sont trop nombreux, l'ISP décidera probablement que vous envoyez du courrier indésirable. Certains ISP permettent aux expéditeurs d'avoir plus de transparence sur ce que font leurs destinataires en fournissant des *boucles de rétroaction* dans lesquelles l'ISP indique à l'expéditeur qu'un destinataire s'est plaint d'un message. Amazon SES vous fait suivre automatiquement les plaintes à partir des ISP qui offrent des boucles de rétroaction. Pour plus d'informations, voyez comment Amazon SES traite les emails dans le *manuel du développeur Amazon Simple Email Service*.

Comme vous pouvez l'imaginer, un trop grand nombre de plaintes entraîne une mauvaise déliverabilité. **Un taux élevé de plaintes indique aux récepteurs d'email que vous envoyez des emails non désirés par les destinataires.** Vous trouverez ci-dessous des suggestions sur la façon de réduire le nombre de plaintes.

Problèmes de contenu

Le contenu de l'email fournit la communication ou message. Les récepteurs d'email se sont attaqués aux communications malveillantes des spammers (comme le hameçonnage, les programmes malveillants ou la diffusion de virus ou les messages frauduleux) en implémentant de solides *filtres de contenus.* Ces filtres de contenus effectuent des vérifications automatisées du contenu des messages pour rechercher les emails non désirés. D'un point de vue technique, les utilisateurs avisés font confiance à des filtres de contenus open source comme Apache Spam Assassin. Les entreprises ont plus tendance à s'appuyer sur des filtres de contenus comme Postini de Google ou BrightMail de Symantec. Amazon SES utilise des technologies de filtrage de contenu pour aider à détecter et à bloquer les messages contenant des virus ou des programmes malveillants avant qu'ils ne soient envoyés**.**

Si le filtre de contenus du récepteur a déterminé que votre contenu présente des caractéristiques de courrier indésirable, celui-ci sera probablement marqué comme tel et écarté de la boîte de réception d'un destinataire. Vous trouverez ci-dessous des suggestions sur la façon d'éviter que vos contenus d'email soient interceptés dans des filtres.

Bonnes pratiques recommandées

Même si vous gardez à l'esprit les intérêts de vos destinataires, il peut s'avérer compliqué d'affiner votre programme pour un impact optimal. Nous avons réuni quelques conseils pour vous permettre de faire facilement ce qu'il faut selon vos destinataires, et donc les ISP.

Recommandations générales

- Mettez-vous à la place du destinataire. Posez-vous les questions suivantes : « Est-ce que c'est quelque chose que j'aimerais recevoir dans *ma* boîte de réception ? ». Si la réponse n'est pas « Oui », vous ne devriez probablement pas envoyer cet email.
- Soyez prévenu. C'est malheureux pour ceux qui font bien leur travail, mais certains secteurs ont la réputation d'adopter des pratiques de messagerie de mauvaise qualité. C'est aussi simple que ça. Si vous faites partie des secteurs suivants, vous devez étroitement surveiller les métriques de votre réputation pour rectifier immédiatement les problèmes.
    - Prêts hypothécaires
    - Crédit
    - Industrie pharmaceutique
    - Tabac
    - Boissons alcoolisées
    - Divertissement pour adulte
    - Jeu
    - Programmes de travail à domicile

Considérations relatives au domaine et à l'adresse « De »

- Réfléchissez bien aux adresses à partir desquelles vous envoyez vos emails. L'adresse « De » ne sera pas seulement visible pour les destinataires dans le client de messagerie (y compris le volet d'aperçu), mais permettra également à certains ISP de collecter des réputations. Cette adresse, avec la ligne d'objet, constitue la première impression qu'un destinataire se fait de votre email.
- Réfléchissez bien au domaine de la ou des adresses à partir duquel vous envoyez vos emails. Ceci pour deux raisons :
    - Les ISP se font une idée d'une réputation sur tous les emails envoyés à partir d'un domaine, quelle que soit la manière dont vous divisez vos envois.
    - Les destinataires doivent pouvoir reconnaître votre domaine. Vous ne devez pas collecter une adresse email à partir d'un formulaire web hébergé sur *www.exemple-foo.com* puis envoyer un email à partir de *expéditeur@exemple-bar.com*. Vous ne serez plus reconnu et vous inciterez ainsi les destinataires à cliquer sur le bouton de courrier indésirable.
- Si vous envoyez des volumes significatifs d'emails, ne les envoyez pas *depuis* une adresse email basée sur un ISP, telle que *expéditeur@hotmail.com*. Par exemple, si Yahoo! remarque un volume significatif de messages entrants provenant de *expéditeur@hotmail.com*, cet email sera traité différemment que s'il était issu d'un domaine d'envoi d'email sortant approprié (c'est-à-dire un domaine que vous possédez).

- Incluez des informations WHOIS correctes pour votre domaine afin que les récepteurs puissent consulter des détails à propos du propriétaire de votre domaine d'envoi. Le serveur d'inscription de votre domaine fournira des instructions sur la façon de configurer un enregistrement WHOIS. Les récepteurs font plus confiance aux domaines établis et transparents pleinement répertoriés dans le registre Internet qu'aux autres domaines.

Authentification

- Assurez-vous que votre domaine est authentifié avec **Sender Policy Framework (SPF)** et **SenderID.** Ces méthodes d'authentification apportent de la crédibilité à votre domaine d'envoi en confirmant aux destinataires qu'un email provient effectivement du domaine indiqué. Pour plus d'informations, consultez la section relative à l'authentification de votre adresse email dans le *manuel du développeur d'Amazon Simple Email Service*. Testez vos paramètres d'authentification en envoyant un email à une boîte de réception d'ISP que vous possédez (par exemple, un compte Gmail) et en consultant les en-têtes dans la source du message. Les en-têtes vous indiqueront si vos tentatives d'authentification ont réussi.
- Vous devez également utiliser la norme **DomainKeys** ou **DomainKeys Identified Mail (DKIM)** pour signer votre email sortant. Cette étape d'authentification apportera de la crédibilité à votre email en confirmant aux destinataires que le contenu n'a pas été changé pendant le transit de l'expéditeur au récepteur. Pour une courte explication de la différence entre SPF et DKIM, consultez l'article de Wikipedia concernant l'authentification des emails. Testez vos paramètres d'authentification en envoyant un email à une boîte de réception d'ISP que vous possédez (par exemple, un compte Gmail) et en consultant les en-têtes dans la source du message. Les en-têtes vous indiqueront si votre tentative d'authentification a réussi.

SPF ET SENDERID DANS AMAZON SES

Amazon SES est fourni prêt à être utilisé avec des enregistrements DNS préconfigurés. De plus, Amazon SES dispose de SPF configuré ; tous les envois d'adresses IP depuis amazonses.com sont authentifiés via SPF. Cependant, nous vous recommandons d'également authentifier avec SenderID en ajoutant un pointeur vers notre domaine dans votre enregistrement TXT

Création et gestion de votre liste

- Faites attention à la façon dont vous collectez des adresses email. Très souvent dans les formulaires en ligne ou les autres inscriptions, des personnes fournissent de fausses adresses email qui lorsque vous leur enverrez un email génèreront des erreurs d'adresse mail incorrecte ou inexistante et apparaîtront du point de vue de l'ISP comme un envoi sans réponse.
- Si votre formulaire continue de recueillir des erreurs d'adresse mail incorrecte ou inexistante, assurez-vous que le destinataire confirme l'adresse qu'il entre. Présentez l'adresse pour confirmation, exigez des champs en double pour l'adresse email pour vous assurer que les entrées correspondent et désactivez la saisie automatique côté client si possible.
- Vous pouvez utiliser une *confirmation de l'acceptation* (en envoyant l'email à une adresse dont le propriétaire a cliqué sur un lien de vérification) pour vous assurer de ne pas envoyer à plusieurs reprises des emails à une adresse incorrecte.
- Vous pouvez utiliser des fournisseurs tiers pour vérifier la viabilité d'une adresse email avant d'envoyer des emails à celle-ci.
- Vous pouvez également vérifier la syntaxe d'une adresse email pour vous assurer qu'elle est raisonnablement correcte (par exemple, l'adresse est-elle constituée correctement avec un partie locale et le symbole @ ? L'adresse est-elle résolue en un domaine avec un enregistrement MX ?).

- Vous devez faire attention à ne pas permettre qu'une entrée définie par l'utilisateur soit transmise sans être vérifiée à Amazon SES et les ISP. Les forums et les soumissions de formulaires peuvent s'avérer spécialement délicats car le contenu peut être entièrement généré par l'utilisateur (et des spammers peuvent remplir des formulaires avec leur contenu), mais les récepteurs d'email ne s'en soucient pas : il est de votre responsabilité de veiller à n'envoyer que des emails avec un contenu de qualité.
- Il est très improbable qu'un alias standard (comme postmaster@, abuse@ ou noc@) s'inscrive volontairement pour vos emails. Vous devez pouvoir contrôler la manière dont vous acquérez des adresses email et envoyer des emails uniquement aux adresses qui appartiennent à une personne réelle qui souhaite recevoir vos emails. Cela s'applique tout spécialement aux comptes de rôle qui sont généralement réservés à la surveillance des emails. Des comptes de rôle peuvent être ajoutés de façon malveillante à votre liste comme forme de sabotage Internet pour vous bloquer. Assurez-vous que votre liste n'inclut aucun alias de compte de rôle. Pour obtenir une liste complète des comptes de rôle que vous devez surveiller, consultez Mailbox Names for Common Services, Roles and Functions.
- N'envoyez pas d'email à des listes tierces (achetées, louées, ou collectées de toute autre manière en dehors de votre périmètre). Lorsque vous envoyez des emails à une listes tierce, vous prenez des risques liés à des adresses d'une origine inconnue. Cela pourrait entraîner des mesures de la part des ISP s'il s'avère que la liste contient des *spamtraps* (adresses spéciales configurées par des ISP pour surveiller les emails non sollicités), des adresses entraînant des retours à l'expéditeur ou des destinataires qui se plaignent. Même si les adresses email de la liste tierce sont valides, vous ne savez pas si les destinataires souhaitent effectivement recevoir votre email et donc s'ils vont le considérer comme un courrier indésirable. Vous devez collecter les adresses email vous-même, directement à partir des destinataires.

Conformité

- Que vous envoyiez des emails à des destinataires aux États-Unis ou dans d'autres pays, il vous incombe de respecter la législation et la réglementation applicables à vos pratiques de messagerie. Le présent guide ne traite pas les problèmes de conformité. Vous devez prendre connaissance et suivre la législation applicable.

Éviter les retours à l'expéditeur

- De manière générale, vous devez maintenir votre taux de retours à l'expéditeur en-dessous de 5 %. C'est une façon de prouver aux ISP que vous disposez d'une liste propre (vous connaissez l'état des adresses de vos destinataires). Ce pourcentage peut varier selon les tendances de votre secteur et n'est pas universel pour tous les ISP, mais il s'agit d'une règle de base raisonnable.
- Si vous disposez d'une vieille liste que vous n'avez pas utilisée pour vos envois depuis un moment, n'envoyez pas d'email à cette liste via un fournisseur qui limite vos taux de retours à l'expéditeur (ce qui inclut Amazon SES), à moins de vérifier l'état des adresses (par exemple, en contrôlant l'activité de connexion sur votre site, votre historique d'achats, etc.). Sinon, vous pouvez faire l'objet de nombreux retours à l'expéditeur de la part d'anciennes adresses email non utilisées pendant que vous essayez de nettoyer votre liste, et vous courrez le risque d'être bloqué par des ISP et Amazon SES.
- Si vous fournissez des informations stratégiques à vos clients, par exemple, une réinitialisation de mot de passe, fournissez une autre forme de communication en plus des emails, pour le cas où les adresses mail génèreraient des retours à l'expéditeur. Les alternatives peuvent inclure des questions secrètes intégrées au navigateur, des courriers postaux ou des SMS. Vous devez également afficher l'adresse vers laquelle vous effectuez l'envoi et permettre aux destinataires de choisir un autre flux de travail, comme un SMS, si l'adresse email s'avère incorrecte.

Gérer les retours à l'expéditeur

- N'effectuez pas d'envoi à une adresse email donnant lieu à une erreur d'adresse mail incorrecte ou inexistante en raison d'un échec de livraison permanent. S'il s'agit d'une véritable erreur de livraison permanente, des tentatives répétées ne livreront pas le message, mais les retours à l'expéditeur vont s'accumuler et nuire à votre réputation auprès des ISP.
- Ne faites pas pointer votre adresse de soumission de retour à l'expéditeur vers une boîte de réception donnant elle-même lieu à des retours à l'expéditeur. Assurez-vous que celle-ci peut recevoir les emails. De plus, si vous sous-traitez votre système de messagerie sortante à un ISP, au lieu de recevoir les emails via vos propres serveurs internes, sachez qu'un flux de retours à l'expéditeur peut atterrir dans votre dossier de courrier indésirable ou être complètement supprimé. Dans l'idéal, vous ne devez pas utiliser une adresse email hébergée pour recevoir les retours à l'expéditeur. Si vous devez néanmoins en utiliser une, vérifiez souvent le dossier de courrier indésirable et ne marquez pas les messages de retour à l'expéditeur comme du courrier indésirable. Dans Amazon SES, vous pouvez spécifier l'adresse à laquelle envoyer les retours à l'expéditeur. Pour en savoir plus, consultez la section relative aux notifications de retour à l'expéditeur et de plainte dans le *manuel du développeur Amazon Simple Email Service*.
- En règle générale, un retour à l'expéditeur fournira l'adresse de la boîte de réception qui refuse la livraison. Toutefois, si vous avez besoin de données plus détaillées pour faire correspondre une adresse de destinataire à une campagne d'email particulière, incluez un en-tête X avec une valeur permettant de la suivre dans votre système de suivi interne. Pour en savoir plus, consultez l'annexe relative aux champs d'en-tête dans le *manuel du développeur Amazon Simple Email Service*.

Éviter les plaintes

- De manière générale, vous devez maintenir votre taux de plaintes en-dessous de 0,1 %. Il s'agit d'une façon de prouver aux ISP que vous envoyez des emails appréciés. Ce taux peut varier selon les tendances de votre secteur et n'est pas universel pour tous les ISP, mais il s'agit d'une règle de base raisonnable.
- Ne continuez pas envoyer à un destinataire le même type d'email que celui qui a généré une plainte. Par exemple, vous ne devez plus envoyer des emails de marketing à quelqu'un qui s'est plaint d'un email de marketing, mais vous pouvez continuer à envoyer des emails transactionnels à cette adresse si le destinataire a effectué un achat sur votre site. Un nouvel envoi du même type d'email ne fera que générer d'autres plaintes qui vont s'accumuler au fil du temps et amplifier votre taux de plaintes. Enlevez simplement les adresses des listes appropriées.
- Comme avec les retours à l'expéditeur, si vous disposez d'une liste que vous n'avez pas utilisée pour vos envois depuis un moment (par exemple, si vous êtes un nouveau client Amazon SES), assurez-vous que vos destinataires savent pourquoi ils reçoivent un email. Il est fortement recommandé d'envoyer un message de bienvenue, ou de rappeler d'une quelconque autre façon aux destinataires qui vous êtes pour éviter tout problème de plainte avec les ISP et Amazon SES.

Gérer les plaintes

- Comme avec les retours à l'expéditeur, ne faites pas pointer votre adresse de soumission de plainte vers une boîte de réception donnant lieu à des retours à l'expéditeur. Assurez-vous que celle-ci peut recevoir les emails. De plus, si vous sous-traitez votre système de messagerie sortante à un ISP, au lieu de recevoir les emails via vos propres serveurs internes, sachez qu'un flux de retours à l'expéditeur peuvent atterrir dans le dossier de courrier indésirable ou être complètement supprimé. Il est recommandé de ne pas utiliser une adresse email hébergée pour recevoir les plaintes. Si vous devez néanmoins en utiliser une, vérifiez souvent le dossier de courrier indésirable et ne marquez pas les messages de plainte comme du courrier indésirable. Lorsque vous utilisez Amazon SES, vous pouvez spécifier l'adresse à laquelle envoyer les plaintes. Pour en savoir plus, consultez la section relative aux notifications de retour à l'expéditeur et de plainte dans le *manuel du développeur Amazon Simple Email Service*.
- Un message de plainte contiendra généralement le contenu de l'email (contrairement à un message de retour à l'expéditeur qui ne contiendra que des en-têtes). Cependant, les plaintes incluront souvent l'adresse de la plainte d'origine en raison des préoccupations de confidentialité des ISP. Il vous incombe de vous assurer via l'utilisation d'un en-tête X personnalisé ou d'une valeur incluse dans le contenu que vous puissiez faire correspondre la plainte avec l'adresse email qui a soumis la plainte.

Créer un contenu de qualité

- De nos jours, la plupart des filtres sont complets ; ils examinent l'aspect du contenu au lieu de suivre des règles rapides et figées. Il y a quelques années, une ponctuation ou uniquement des majuscules dans une ligne d'objet impliquait que votre email avait toutes les chances d'atterrir directement dans le dossier de courrier indésirable. À présent, il s'agit plutôt d'une combinaison de différentes caractéristiques du contenu et de si cette combinaison a été couramment considérée comme du courrier indésirable. Vous pouvez utiliser Spam Assassin ou un service de réputation tiers comme Return Path pour vous aider à identifier les problèmes de contenu.
- Vérifier les URL que vous utilisez dans vos emails par rapport aux listes noires peut fournir des informations précieuses, parce que certains ISP bloqueront les emails avec des liens en liste noire. URIBL.com et SURBL.org sont deux sites très utiles qui vous permettent de déterminer si vos liens sont répertoriés. Pensez à vérifier les liens qui vous sont fournis par un tiers ou les raccourcisseurs de lien qui sont devenus de plus en plus dangereux parce qu'ils masquent le domaine final.
- Évitez les liens rompus dans vos emails ; assurez-vous qu'il existe effectivement des pages derrière vos liens. Si vous avez un lien non inscrit, vérifiez qu'il fonctionne. Vous pouvez facilement oublier de tester chaque lien lorsque vous créez de nouveaux programmes de messagerie ou changez des templates d'email existants.
- Assurez-vous que les pages relatives à la confidentialité et aux conditions d'utilisation fonctionnent. Les destinataires risquent de ne pas faire confiance à votre email s'ils ne trouvent pas ce type d'informations standards sur votre site, ce qui va diminuer la valeur de votre email et son potentiel de déliverabilité.
- Si vous envoyez du contenu à haute fréquence (par exemple, des offres quotidiennes), veillez à ce que celui-ci soit différent chaque jour. Avec des emails très fréquents, vous devez encore plus vous assurer que le contenu est à jour et pertinent.

Réflexions finales

Malgré les difficultés inhérentes à la navigation dans différents systèmes entre vos destinataires cibles et vous-même, les emails peuvent constituer un mécanisme de communication extrêmement efficace si vous les utilisez correctement. Nous espérons que vous maîtrisez désormais mieux les facteurs qui influencent le fait que vos emails atteignent vos boîtes de réception cibles et que vous disposez également d'une liste des mesures à prendre pour améliorer votre programme de messagerie.

Si la liste ci-dessus n'est en aucun cas une liste complète de tout ce que vous pouvez faire pour améliorer la qualité de vos emails (et leur déliverabilité), nous espérons que vous la trouverez utile pour commencer. Lorsque vous concevez votre programme de messagerie, vous devez garder à l'esprit deux points essentiels :

1. Offrez de la valeur.
2. Envoyez vos emails uniquement à ceux qui souhaitent les recevoir.

Si vous respectez ces deux points en suivant ces conseils, votre programme de messagerie a toutes les chances d'être un succès !

Glossaire

- **Boucle de rétroaction :** Système avec lequel un ISP indique à l'expéditeur qu'un destinataire s'est plaint d'un message.
- **Bounce asynchrone :** Retour à l'expéditeur (bounce) envoyé après que le message a été initialement accepté pour livraison par le récepteur.
- **Bounce synchrone :** Retour à l'expéditeur (bounce) communiqué pendant que les serveurs de messagerie de l'expéditeur et du récepteur sont en train de transmettre ou de recevoir activement l'email.
- **Confirmation de l'acceptation :** Système exigeant qu'un abonné potentiel demande à être abonné et clique sur un lien de vérification qui lui est envoyé ultérieurement.
- **Déliverabilité :** Probabilité qu'un message électronique que vous envoyez arrive effectivement à sa destination prévue (généralement, la boîte de réception du destinataire).
- **Destinataire :** Personne ou entité qui reçoit un message par email ; le destinataire est nommé dans le champ À, Cc ou Cci du message.
- **Email de qualité** : Email jugé comme offrant de la valeur par son destinataire.
- **Expéditeur :** Personne ou entité qui envoie un message par email.
- **Filtres de contenus :** Vérifications automatisées du contenu des messages pour rechercher les emails non désirés.
- **Fournisseurs de service Internet (ISP) :** Organisations fournissant un accès à Internet.
- **Message d'adresse mail incorrecte ou inexistante :** Message indiquant un échec de livraison persistant, comme « La boîte aux lettres n'existe pas ».
- **Message d'erreur ou d'échec provisoire :** Message indiquant un échec d'envoi temporaire, comme « La boîte aux lettres n'existe pas ».
- **Plainte :** Message généré lorsqu'un destinataire marque un email comme étant indésirable en cliquant sur le bouton « Marquer comme courrier indésirable » dans son client de messagerie.
- **Programme de messagerie :** Manière dont vous gérez la communication électronique avec vos destinataires par email.
- **Récepteur :** Le ou les systèmes prenant en charge l'infrastructure de messagerie du destinataire (la personne ou le système qui se cache derrière l'adresse email de destination).
- **Répertoire junk :** Également appelé « dossier de courrier indésirable » ou « dossier en vrac ». Dossier dans lequel les messages identifiés par des filtres comme ayant moins de valeur sont collectés de façon à ce qu'ils n'arrivent pas dans la boîte de réception, mais qu'ils restent accessibles pour le destinataire.
- **Réputation :** Confiance instaurée par les expéditeurs en envoyant des emails de haute qualité au fil du temps. Elle est généralement influencée par une combinaison de facteurs.
- **Retour à l'expéditeur :** Message indiquant l'état d'échec de la tentative de livraison.
- **Spamtraps :** Adresses spéciales configurées par des ISP pour surveiller les emails non sollicités.

Ressources supplémentaires

Plus d'informations sur certaines des recommandations de ce livre blanc

- Pour en savoir plus sur la régulation des emails aux États-Unis, visitez le site FTC – http://business.ftc.gov/documents/bus61-can-spam-act-compliance-guide-business
- Pour en savoir plus sur les prestataires de solution SES, consultez la page des ressources Amazon SES – http://aws.amazon.com/ses/resources/
- Pour savoir comment tester vos paramètres d'authentification d'email, consultez le site ESPC – http://www.espcoalition.org/senderid/

Plus d'informations sur Amazon SES

- Présentation – http://aws.amazon.com/ses/
- Documentation pour les développeurs – http://aws.amazon.com/documentation/ses/
- Forum de la communauté – https://forums.aws.amazon.com/forum.jspa?forumID=90
- AWS Support – https://aws.amazon.com/support

Prestataires de solution Amazon SES

- Déliverabilité : Return Path – http://aws.amazon.com/solution-providers/si/return-path
- Rendu d'aperçu et analyse : Litmus – http://aws.amazon.com/solution-providers/si/litmus/
- Service complet et stratégie : Zeta Interactive – http://aws.amazon.com/solution-providers/si/zeta-interactive-1320423244
- Stratégie : Marketing de Synchronicité – http://aws.amazon.com/solution-providers/si/synchronicity-marketing
- Intégration des technologies : Cambridge Technology Enterprises – http://aws.amazon.com/solution- providers/si/cambridge-technology-enterprises

Pages d'administrateur ISP

- AOL – http://postmaster.info.aol.com/
- ATT – http://www.att.com/esupport/postmaster/
- BellSouth – http://www.att.com/esupport/postmaster/
- Charter – http://www.charter.com/customers/support.aspx?supportarticleid=1953
- Comcast – http://postmaster.comcast.net/
- Cox – http://postmaster.cox.net/confluence/display/postmaster/Postmaster+Home
- Facebook – http://postmaster.facebook.com/
- Frontier – http://postmaster.frontier.net/
- Gmail – https://mail.google.com/support/bin/answer.py?answer=81126&topic=12838
- Hotmail – http://postmaster.msn.com/

- RoadRunner – http://postmaster.rr.com/
- United Online – http://unitedonline.net/postmaster/
- USA.NET – http://postmaster.usa.net/
- Yahoo! – http://postmaster.yahoo.com/