Livre Blanc n°1
Novembre 2005

E-mail ou SPAM ?

De quelle manière les entreprises peuvent-elles continuer à utiliser efficacement les pratiques légales de l'e-mail marketing dans un contexte de lutte contre le phénomène de Spam ?

Ce livre blanc a été élaboré dans l'objectif de vous donner les clés pour maximiser les chances de délivrer votre message à votre cible.

Un livre blanc réalisé et publié par eMill — Active+ Software.

eMill

© eMill 2005. Tous droits réservés. Plus d'infos sur http://www.emill.net.

Introduction

Face aux problèmes posés par la hausse du nombre de courriers non sollicités (Spam), les fournisseurs d'accès Internet, les webmails (Hotmail, Yahoo, Gmail, etc.), les éditeurs de logiciels de messagerie et les responsables informatiques des entreprises ont été obligés de protéger les utilisateurs en mettant en place un filtrage des messages reçus. Ce filtrage s'effectue par défaut ou peut parfois être configuré par l'utilisateur.

L'objectif de ces filtres est totalement louable que l'on se place du point de vue du récepteur ou de l'émetteur des messages. En effet, ces procédés permettent de désengorger les messageries, d'améliorer l'image du canal 'e-mail' et donne donc plus de visibilité aux pratiques légales d'e-mail marketing.

Cependant, les techniques des spammeurs s'améliorant, les filtres anti-Spam sont devenus plus agressifs vis-à-vis des messages reçus. Ainsi, de plus en plus d'e-mails « légitimes » se retrouvent détectés comme Spam, c'est ce qu'on appelle des « faux positifs ». De nombreuses études estiment que le taux de « faux positif » est de 2 à 3% mais peut monter jusqu'à 30% si l'émetteur ne fait pas tout pour élaborer un message propre.

Dans cet objectif, il vous faudra veiller à quelques grands principes :

1. Disposer d'une liste de destinataires propre et légitime.
2. Créer un contenu de qualité.
3. Choisir les techniques d'envoi appropriées.
4. Éviter d'avoir une adresse IP « blacklistée ».
5. Gérer efficacement les courriers non délivrés ou retournés (Bounces, NPAI ou DSN).

© eMill 2005. Tous droits réservés. Plus d'infos sur http://www.emill.net.

1 Disposer d'une liste de destinataires propre et légitime.

Que vous souhaitiez utiliser l'e-mail pour communiquer avec vos clients, vos fournisseurs ou vos actionnaires, il est fortement conseillé de construire patiemment une liste à partir de sources de données internes ou de techniques marketing traditionnelles on-line ou off line : jeux-concours, lettres d'information (newsletters), enquêtes, etc.

En utilisant une liste élaborée par vos soins, vous garantissez l'origine des adresses, la façon dont elles ont été rassemblées et bénéficiez d'un a priori positif vis-à-vis des destinataires. Ces atouts vont vous permettre d'optimiser la « délivérabilité » de votre message en étant reconnu par le destinataire et en lui demandant, par exemple, d'ajouter votre nom de domaine à sa liste blanche. Il n'est nul besoin de préciser que cette technique ne peut être que bénéfique à votre image et à l'impact de votre message.

Au contraire, l'efficacité d'une campagne envoyée à une liste louée ou achetée à un prestataire est beaucoup plus aléatoire. En effet, l'origine des adresses et la façon dont elles ont été collectés sont souvent garanties « opt-in » mais l'impact du message est souvent moindre et les chances d'être signalé comme spammeur beaucoup plus fortes.

Enfin, il est vivement déconseillé de céder aux sirènes d'offres alléchantes promettant une liste « opt-in » de 15 millions d'adresses e-mail pour 30 Euros.

© eMill 2005. Tous droits réservés. Plus d'infos sur http://www.emill.net.

2 Créer un contenu de qualité

Avant d'imaginer les techniques les plus improbables pour éviter les filtres anti-Spam, il faut partir d'un constat simple : si vous n'êtes pas à un spammeur, vous avez peu de chances d'être considéré comme tel. Votre priorité doit donc être d'élaborer un message professionnel en suivant quelques règles de base :

- Si vous souhaitez envoyer un message en format HTML, utilisez des éditeurs HTML de qualité (l'éditeur intégré d'eMill ou d'autres comme Dreamwaver ou FrontPage). Des outils comme MS Word ou Publisher créent beaucoup de codes inutiles amenant votre message à être détecté comme du spam.

- Si vous souhaitez envoyer un message en format HTML, il est conseillé de créer une version texte alternative. Ce type de message « multipart » intègre un contenu HTML et un contenu texte qui seront affichés alternativement selon le client mail du destinataire. Pour créer ce type de message dans le logiciel eMill, il vous suffit d'ajouter un contenu texte et un contenu HTML et de cocher l'option « Ce contenu est le corps du message » dans les propriétés de chacun des contenus (clic droit sur le contenu et Propriétés). Notez que l'assistant de création d'un projet d'e-mailing crée automatiquement un contenu HTML et une version texte alternative.

© eMill 2005. Tous droits réservés. Plus d'infos sur http://www.emill.net.

- N'utilisez pas des termes ou des caractères pouvant être assimilés à du Spam car la plupart des filtres sont basés sur leur détection. Pour connaître les caractères à éviter, vous pouvez visiter le site de Microsoft pour Outlook ou celui de Wilson Web.

- Commencez votre message en expliquant comment vous avez collecté l'adresse du destinataire comme par exemple « Vous vous êtes abonnés à notre lettre d'information le Jeudi 9 novembre 2005 ».

- La structure du message envoyé doit respecter les standards MIME. eMill vous garanti cette conformité.

- Pensez à indiquer toutes les informations montrant au destinataire que votre message est légitime : lien de désinscription, adresse complète, lien vers votre politique de confidentialité, etc.

La liste ci-dessus n'est pas exhaustive. Afin de vérifier si votre message répond aux critères des filtres anti-Spam, vous pouvez utiliser des outils comme SpamAssasin. Notez que eMill intègrera dans sa prochaine version, une fonctionnalité permettant de vérifier vos messages en utilisant SpamAssassin.

© eMill 2005. Tous droits réservés. Plus d'infos sur http://www.emill.net.

3 Choisir les techniques d'envoi appropriées

eMill vous propose d'utiliser soit le serveur SMTP intégré soit un ou plusieurs serveurs SMTP externes (votre FAI ou celui de votre entreprise). Selon votre choix vous devrez veiller à certains points :

- **Serveur SMTP de votre fournisseur d'accès** : La plupart des FAI vous permettent d'utiliser leur serveur pour envoyer des campagnes d'e-mailing. Cependant, il est conseillé de les consulter avant de l'utiliser. De plus, il est possible que certains bloquent vos envois à partir d'un certain nombre de messages envoyés par heure. Si vous rencontrez ce problème, l'option « Régulateur » d'eMill permet de limiter le débit d'envoi (option accessible à partir de Projet > Propriétés, onglet Expéditeur).

- **Serveur SMTP de votre entreprise** : Cette solution est souvent la plus efficace car elle vous assure que l'envoi ne sera pas bloqué et que le nom de domaine correspond à l'adresse de l'expéditeur. Le seul problème que vous pouvez rencontrer est l'encombrement du serveur d'envoi pour des campagnes importantes. Pour cela, vous pouvez soit programmer un envoi de nuit soit utiliser l'option « Régulateur » d'eMill qui permet de limiter le débit d'envoi (option accessible à partir de Projet > Propriétés, onglet Expéditeur).

© eMill 2005. Tous droits réservés. Plus d'infos sur http://www.emill.net.

- **Serveur SMTP intégré** : Si vous êtes dans l'incapacité d'utiliser les 2 techniques détaillées ci-dessus, eMill intègre un serveur SMTP dans l'ensemble de ces versions. Si vous choisissez cette solution, il est important d'avoir une adresse IP fixe afin de minimiser le risque d'être détecté comme émetteur de spam.
  De plus, afin d'obtenir des notifications en cas de courriers non délivrés (et ainsi les gérer, voir Partie 5), n'oubliez pas de cocher l'option « Générer des notifications de livraison localement » accessible à partir de Projet > Propriétés, onglet Notifications.
  Notez que l'utilisation du serveur intégré peut vous donner l'impression que l'envoi est plus lent. Ceci est simplement du au fait qu'eMill envoie les messages directement au destinataire final alors que, pour les autres techniques, eMill envoie au serveur SMTP externe qui s'occupe ensuite de la livraison des messages au destinataire final. Dans les faits, l'envoi par un serveur SMTP externe n'est donc pas plus rapide.

4 Éviter d'avoir une adresse IP « blacklistée »

Beaucoup de fantasmes se sont développés autour du risque d'avoir son adresse IP blacklistée, c'est à dire signalée comme émettrice de courriers non sollicités. Il est vrai que le blacklistage peut réduire de 70% le nombre de messages délivrés aux destinataires. Cependant, il faut retenir une chose importante. Pour être blacklisté, il faut avoir été détecté comme étant spammeur.

© eMill 2005. Tous droits réservés. Plus d'infos sur http://www.emill.net.

Or, la plupart du temps, c'est le destinataire du message lui-même et non un système automatique qui va signaler un spammeur. Par conséquent, si vous suivez les conseils édictés plus haut vous ne courrez aucun risque.

Le « blacklistage » est aussi souvent utilisé comme principal argument par les solutions ASP (hébergées) de gestion de campagnes d'e-mailing qui vous garantissent que leurs serveurs d'envoi sont « whitelistés ». Cela signifie qu'ils ont assuré à l'administrateur d'un service mail qu'ils n'envoyaient que des messages légitimes. Cependant, ces entreprises prennent en charge un nombre important de campagnes et ne peuvent pas apporter de garanties sur l'origine des listes de destinataires de tous leurs clients. Le danger vient donc du fait que votre IP soit blacklistée si le serveur de la solution ASP est signalé comme émetteur de spam. Si tel était le cas, vous n'auriez aucun recours pour exprimer votre bonne foi puisque le serveur d'envoi a bel et bien servi à envoyer des courriers non sollicités.

En utilisant, votre propre serveur SMTP, vous endossez la responsabilité de vos envois mais pas ceux d'une personne tierce. Si vous êtes un jour signalé par erreur comme émetteur de Spam, vous aurez la possibilité de contacter l'organisme vous ayant blacklisté pour exprimer votre bonne foi. De plus, vous pouvez authentifier votre adresse IP auprès de votre serveur DNS (Domain Name System) en profitant de l'émergence de protocoles d'identification. Pour avoir plus de détails sur ces systèmes et connaître les procédures d'installation, consultez les protocoles les plus utilisés : Sender ID (Microsoft) et DomainKeys (Yahoo).

Un dernier conseil sur les risques de « blacklistage » est de surveiller de près l'évolution des taux de courriers non délivrés ou bounces. Si vous notez une hausse anormale de ce taux, il vous faut vérifier que l'IP émettrice n'est pas blacklistée. Pour cela, vous pouvez vous rendre sur les sites http://rbls.org ou http://www.spamcop.net.

© eMill 2005. Tous droits réservés. Plus d'infos sur http://www.emill.net.

5 Gérer efficacement les courriers non délivrés.

Un des facteurs privilégiés pour détecter un Spam est de vérifier si son émetteur envoie beaucoup de messages à des adresses email inexistantes. En effet, les spammeurs ont pour habitude d'utiliser des listes d'adresses email constituées, par exemple, de n'importe quel prénom existant suivi de @domain.com. Ce genre d'envoi surcharge complètement les serveurs de réception qui bloquent donc l'émetteur.

Pour éviter cela, il ne faut pas acheter ou louer des listes à des prix dérisoires (voir Partie 2) et gérer efficacement les messages que vous recevrez signalant que les courriers n'ont pas été délivrés. Ces messages sont appelés des bounces, des NPAI (N'Habite Pas A l'Adresse Indiquée), des notifications de livraison ou des DSN (Delivery Status Notification).

Pour gérer les bounces, il vous faut donc utiliser un logiciel comme eMill qui permet de les récupérer puis d'automatiser leur traitement selon leur type. En effet, vous n'allez pas effectuer la même action, si le bounce révèle que l'adresse est inexistante, que la boîte de réception du destinataire est pleine ou que le serveur de réception était occupé. Pour savoir quel type de bounce vous recevez, ces messages contiennent un code appelé « status code » qui contient 3 chiffres séparés par un point. Dans le cas d'un bounce, le premier chiffre peut être un 4 ou un 5. Le '5' représente un échec permanent de livraison (adresse inexistante, nom de domaine inexistant, etc.), vous pourrez donc décider d'effacer ces contacts ou de les notifier de façon particulière dans votre source de données afin de vérifier qu'il n'y a pas d'erreur de frappe ou de confirmer visuellement leur effacement.

© eMill 2005. Tous droits réservés. Plus d'infos sur http://www.emill.net.

Le '4' représente un échec temporaire (boîte pleine, serveur occupé, etc.), vous pourrez donc, par exemple, incrémenter un compteur dans votre source de données et décider d'effacer ces contacts lorsqu'il atteint un certain plafond. Les 2 chiffres suivants le 4 ou le 5 donnent plus de détails sur les raisons de l'échec de l'envoi. Il est difficile et fastidieux de prévoir une action spécifique pour chaque type de bounces mais si, par exemple, vous utiliser les techniques de signature électronique ou de cryptage, vous pourrez identifier facilement les problèmes venant de ce procédé.

La mise en place de ce système peut prendre un peu de temps mais il est efficace, indispensable et pourra être utilisé pour l'ensemble de vos projets.

Pour en savoir davantage sur la gestion des bounces avec eMill, lancez l'aide d'eMill et rendez vous dans Base de connaissances > Gestion des DSNs ou Bounces.

© eMill 2005. Tous droits réservés. Plus d'infos sur http://www.emill.net.