Délivrabilité

Comprendre la lutte contre le spam pour mieux délivrer

10 experts français s'expriment

Table des matières

Édito

De nombreux articles, guides, études, livres blancs traitent de la délivrabilité. Bien souvent, ceux-ci tentent de vous donner la bonne recette pour délivrer vos emails, déploient des listes de bonnes pratiques ou vous aident à poser un diagnostic. Pour autant, il est rare que ces publications essayent d'expliquer pourquoi la délivrabilité est un sujet aussi complexe à appréhender, et surtout pourquoi les opérateurs mais aussi les routeurs déploient autant d'énergie sur le sujet.

La délivrabilité est devenu d'une extrême complexité pour l'ensemble des annonceurs, qu'ils aient de bonnes pratiques ou non. Pour beaucoup d'opérateurs, le webmail est vu comme une porte d'entrée indispensable à leurs portails et donc à leurs revenus publicitaires. Et pour conserver, pour séduire les utilisateurs d'un webmail, l'un des arguments les plus efficaces est la qualité des filtres anti-spam. En parallèle, les attaques de phishing sont venues renforcer la complexité des filtres avec une importance toujours accrue de la notion de réputation.

Aujourd'hui, il ne faut plus simplement respecter les bonnes pratiques. Il faut s'adapter en permanence, surveiller l'ensemble des indicateurs de réputation et surtout anticiper les changements structurels qui sont en cours de déploiement. On pensera par exemple à une catégorisation accrue des emails dans l'inbox de vos destinataires, à la nécessité d'implémenter toutes les technologies permettant de traiter les plaintes et les désinscription en temps réel,…

Dans cette publication, vous trouverez de nombreuses clefs vous permettant de voir l'envers du décors et d'appréhender la complexité de la délivrabilité pour les différents acteurs de l'industrie.

Jérôme Gays, DeliverNow

Retrouvez Jérôme Gays sur le blog de DeliverNow :
www.delivernow.eu/blog

Laurent Garnier, Directeur Expertise Délivrabilité, NP6

Quelles sont les raisons qui poussent les Webmails (comme Hotmail) ou les FAI (comme récemment Orange) à publier le nombre de spamtraps touchés par une adresse IP ? Est-ce que ça ne risque pas d'aider les spammeurs à être plus efficaces ?

Microsoft via SNDS et Orange via Signal Spam indiquent en effet le nombre de spamtraps sollicités par une adresse IP sur une période de 24 heures. Cette information est réservée au titulaire ou à l'utilisateur de l'adresse IP. Elle est accessible pour Microsoft depuis leur site postmaster (postmaster.live.com / snds) et via une adhésion à l'association Signal Spam pour Orange (www.signal-spam.fr).

Les spamtraps sont des comptes abandonnés qui de par ce statut ne sollicitent plus de communications. Ils sont maintenus sciemment par les opérateurs, ce qui leur permet de juger de la qualité d'un envoi et de prendre en compte cette information dans leur processus de filtrage.

Un annonceur qui opère une bonne collecte de la donnée email (double opt-in, consentement éclairé, …) et qui sait l'entretenir (purge des inactifs sur le long terme, mesure de l'appétence, …) ne devrait pas rencontrer beaucoup de spamtraps. À l'instar des boucles de rétroaction, disposer de cette information permet à l'annonceur de juger de l'état de santé de sa base de données et d'agir en conséquence dès que les premiers spamtraps apparaissent. C'est dans cette optique que cette information est mise à disposition par certains opérateurs, et en l'état, elle n'est d'aucun intérêt pour les spammeurs qui sont le plus souvent aux antipodes des bonnes pratiques de collecte et de gestion de base.

Evidemment, l'identité du spamtrap n'est pas divulguée. Et même si cette information pourrait être utile à un annonceur respectueux des bonnes pratiques, Microsoft et Orange ne la communiqueraient pas car elle aurait un pouvoir de nuisance beaucoup trop fort si elle était exploitée par des spammeurs.

Diplômé en informatique, Laurent Garnier intègre NP6, société éditrice du logiciel E-CRM d'email & SMS marketing MailPerformance, en 2000. Il évolue rapidement pour être promu en 2007 Directeur Expertise Délivrabilité. Précurseur, il s'intéresse très tôt à la Délivrabilité et est considéré aujourd'hui comme une référence en la matière. Il participe à des syndicats professionnels comme le SNCD dont il anime l'atelier e-routeurs, le DMA, ou bien à des associations telles que Signal Spam dont NP6 est l'un des membres fondateurs.

Arnaud Clément-Bollée, Senior Deliverability Consultant EMEA, Salesforce Marketing Cloud

De nombreux routeurs comme vous refusent d'envoyer les emails d'acteurs de l'acquisition et ne font que de la fidélisation. Pour quelle raison ? N'est-ce pas normal qu'un annonceur cherche à acquérir de nouveaux contacts ?

Ce n'est pas une question à laquelle il est simple de répondre. En fait, cette question à une réponse éminemment politique. Le but d'un routeur d'email est d'envoyer les emails de ses clients en s'assurant qu'ils sont bien délivrés et qu'ils génèrent de l'engagement. Mais le routeur a aussi pour rôle de les éduquer à respecter les bonnes pratiques. Et régulièrement, ces expéditeurs se retrouvent bloqués par les FAI, ce qui est normal et inhérent à la délivrabilité des emails. En effet, plus on avance dans le temps, plus les bonnes pratiques d'hier deviennent les règles des FAI aujourd'hui.

Lorsque l'on doit résoudre une situation de blocage avec un FAI ou avec un site de blacklist, cela passe souvent par une phase de négociation avec ces acteurs. Durant ces négociations, il est important de montrer patte blanche, c'est à dire d'avoir un discours transparent sur ce qui s'est passé. Or, il peut arriver qu'un FAI refuse de débloquer la situation en mettant en cause le manque d'engagement du routeur dans la mesure où il héberge d'autres acteurs problématiques.

En effet, si ce routeur héberge des acteurs générant plus de plaintes que la moyenne, comment prouver l'engagement de celui-ci ? En effet, le FAI a le devoir de protéger ses abonnées, ses clients se plaignant des emails reçus. Si le FAI ne croit pas en une possible amélioration ou changement des pratiques de l'annonceur, il n'a alors aucune raison de lever le blocage.

Pour comprendre la problématique des acteurs de l'acquisition, il faut partir de la source. J'ai pour habitude de dire que la majorité des problèmes en délivrabilité viennent le plus souvent du recrutement des adresses. En effet, il faut recruter les adresses en concordance, cohérence et transparence avec l'abonné. En respectant ces trois principes, vos abonnés n'auront plus de raison de se plaindre. Chez les acteurs de l'acquisition comme le but est de recruter un maximum d'adresse pour en tirer profit, ces principes ne sont que partiellement respectés voir pas du tout. Cependant, le tableau n'est pas tout noir ou tout blanc et certains s'adaptent très bien. Il faut garder à l'esprit que cela vaut aussi pour les acteurs qui travaillent à la fidélisation et qui peuvent avoir recours aux techniques de l'acquisition en masse.

Ainsi, il est vrai que chez Salesforce Marketing Cloud, nous refusons d'encourager les pratiques des acteurs de l'acquisition en les acceptants à utiliser notre solution. Ceci est d'ailleurs valable pour tous les acteurs, que ce soit acquisition ou fidélisation. De plus, pour nos futurs clients nous faisons une analyse complète des pratiques et de la réputation.

Plus généralement, il est vrai qu'aujourd'hui les routeurs font beaucoup plus attention à la qualité de leurs clients. Mais ceci a toujours été le cas, car un seul client avec de mauvaises pratiques va mettre en péril la totalité du parc.

Je pense sincèrement qu'il est tout à fait normal que certains acteurs comme les FAIs définissent des règles dans le but de contrer les abus ; ce qui impose au marché de s'adapter sous peine de mourir.

Arnaud est, depuis juillet 2014, consultant délivrabilité chez Salesforce Marketing Cloud pour la France, mais aussi pour toute la zone EMEA (Europe, Moyen-Orient et l'Afrique). Avant d'arriver chez Salesforce, Arnaud a travaillé plusieurs années chez eCircle et SmartFocus, mais aussi en tant que Directeur IT et responsable de l'acquisition pour un site ecommerce.

Mathieu Dodergny, Directeur de développement, Marketing Analytique, Experian Marketing Services

On parle souvent de la réputation globale qu'un routeur peut avoir. Est-ce que c'est une réalité, et sur quels critères techniques se base un filtre anti-spam pour détecter le routeur qui se cache derrière un email ?

C'est effectivement une question à laquelle nous sommes régulièrement confrontés, et ce, à différents niveaux.

Le plus important ici est que la réputation globale d'une plateforme de routage email n'est pas réellement technique. C'est une réputation qui se construit d'avantage sur un point de vue humain.

Néanmoins, il est possible pour un filtre anti-spam de détecter un réseau d'envoi d'email et donc un routeur. Techniquement, ce sont les plages d'adresses IP qui forment l'identité d'une plateforme. Dans des cas extrêmes, le ReverseDNS (NDLR : Nom de domaine associé à une ou plusieurs adresses IP) a déjà été utilisé afin de bloquer un réseau entier, mais cela reste quoi qu'il arrive une opération manuelle et pas le fait d'un filtre automatique.

Si on prend le cas d'Experian Marketing Services, par exemple, nous possédons différentes plateformes qui sont utilisées dans plusieurs pays. Dans ce cadre, il est rare que les opérateurs fassent une réelle différence entre ces plateformes, c'est plutôt Experian Marketing Services qui est

vu comme un tout. Pourtant, si on prenait uniquement des critères techniques, chaque plateforme serait bien distincte.

Aujourd'hui, la réputation globale d'une plateforme de routage email est clairement basée sur la qualité de la relation que celle-ci a avec les FAI et l'industrie anti-spam. L'objectif que tout routeur doit avoir est d'être le plus transparent possible avec cet écosystème. Cela se traduit par la volonté d'exposer le plus clairement possible l'identité de l'expéditeur réel, et non du prestataire technique, le routeur, afin de simplifier le travail d'identification des filtres anti-spam. Le meilleur exemple est l'utilisation de noms de domaines de nos clients dans le nom de l'expéditeur.

En résumé, notre travail est d'avoir une belle vitrine, des clients qui respectent les règles afin de pouvoir continuer à être considéré comme médiateur de confiance par les opérateurs, et ainsi continuer à délivrer nos messages le plus efficacement possible et résoudre les soucis de délivrabilité quand ils se produisent.

Pour terminer, aujourd'hui, les grands principes sur lesquels se basent les opérateurs pour donner une réputation à un expéditeur sont globalement les mêmes partout : nombre de spamtraps touchés, taux d'ouverture, taux d'engagement, plaintes spam, … le but d'un routeur est de garder un œil, lui aussi, sur ces critères.

Mathieu Dodergny est arrivé en 2007 chez Experian. Il s'est progressivement spécialisé autour de la notion de délivrabilité. À l'origine de la création de l'équipe délivrabilité en France, il occupe aujourd'hui le poste de Directeur de développement, Marketing Analytique pour les différents bureaux Experian Marketing Services à travers le monde (Amériques, Europe, Asie). Il a à cœur de faire prendre conscience aux professionnels les enjeux primordiaux que représente la délivrabilité, pour parvenir à un marketing efficace, et surtout plus responsable.

Philippe Antuoro, Expert technique, SFR et VP Services et Développements, SignalSpam

Quels sont les enjeux économiques de la lutte anti-spam pour un FAI ? Est-ce que la lutte contre le spam est vue comme un enjeu stratégique par les directions ?

Pour un opérateur français, il y a deux manières de voir l'email. Soit comme un centre de coûts, je dois fournir un service d'email à mes clients, soit comme une opportunité de générer du chiffre d'affaire additionnel. Nous avons donc deux situations différentes, d'une part les opérateurs fournissant un service de base et d'autre part ceux qui tentent de développer un modèle économique autour des services de webmail, via la publicité, avec un chiffre d'affaire directement lié à l'audience.

Dans ce second cas de figure, il faudra au minimum que la valorisation du service rembourse les coûts qui lui sont liés.

Ces revenus publicitaires peuvent être de deux ordres, le vente d'espace via des régies, mais aussi de l'autopromotion. Dans certains cas, on voit même que la déconnexion au webmail redirige vers le portail de l'opérateur et donc lui apporte directement du trafic.

Pour aller plus loin, l'application mobile remplit, dans ce cas, exactement le même but, vendre de l'espace publicitaire et faire de l'autopromotion.

Mais pour rendre un webmail rentable et conserver ses utilisateurs, un élément est primordial, avoir la confiance de ces derniers. Pour y arriver, les opérateurs doivent lutter contre tous les éléments pouvant être irritants pour les utilisateurs et notamment le spam. C'est à dire éviter que le spam n'envahisse la boîte email et surtout, lutter contre toute forme de phishing. Cela passe aussi par la mise en place de stratégies innovantes tel que la désinscription automatique depuis le webmail (mais aussi depuis l'application mobile) ou l'identification automatique des publicités.

Pour en revenir à la question, pour les directions marketing, le webmail est un vrai enjeu parce que l'email service très utilisé représente l'image de marque, un potentiel d'audience et un chiffre d'affaire web / portail. Pour autant, la lutte contre le

spam et l'identification du greymail n'est pas perçue comme stratégique. En effet la lutte contre le spam n'est pas une fin en sois, c'est devenu au fil des ans un thème important à adresser si un FAI veux conserver ses utilisateurs messagerie dans une expérience client ergonomique et agréable.

Par contre, si l'on parle de phishing et de cybercriminalité, là, l'enjeu est vu comme stratégique jusqu'aux directions générales car on s'attaque à la marque en l'usurpant ou en l'utilisant pour voler des utilisateurs. Le rôle que jouent les FAI pour l'économie française ne laisse pas de place à l'improvisation sur ce sujet et les opérateurs ont d'ailleurs des obligations légales en la matière.

Un aspect qui est très souvent ignoré concernant le phishing ou les arnaques est que les attaques peuvent très rapidement se retourner contre les opérateurs par des pertes significatives si rien n'est fait. Un exemple parmi d'autres serait une campagne d'email d'arnaque dont le vecteur initial est l'email et qui tenterait de récupérer un grand nombre de numéro téléphone afin d'envoyer à ceux-ci des SMS d'alertes fictives visant à les inciter à appeler des numéros surtaxés. Dans ce cas, l'opérateur se retrouve parfois obligé de supporter la charge financière de ses clients lésés en les remboursant. On comprend donc aisément qu'il s'agisse d'un sujet stratégique car l'image de marque de l'opérateur est atteinte sur le plan confiance au numérique,mais en plus il faut y ajouter diverses compensations auprès des clients lésés.

Architecte dans le domaine des plates-formes de services Internet, Philippe s'est spécialisé depuis une dizaine d'année sur les services de messagerie Grand Public et entreprise chez les FAIs. Philippe Antuoro a suivi en détail l'évolution des technologies antispam et l'écosystème de l'emailing. Actuellement Expert Technique chez SFR dans les domaines architecture de messagerie Grand Public et lutte contre les abus, Philippe Antuoro intervient aussi dans l'association Signal Spam dans laquelle il a pris en charge le pole Services et Développements.

Thomas Fontvielle, Secrétaire Général, Signal Spam

Une organisation comme SignalSpam regroupe différents types d'acteurs de l'industrie emailing. Quelles sont les conditions que doivent remplir les routeurs pour faire partie de l'association et avoir un accès aux données partagées par SignalSpam ?

Signal Spam est en effet issue d'un partenariat public / privé auquel participent des autorités publiques (Gendarmerie Nationale, l'ANSSI, l'OCLCTIC, la CNIL, …), des organisations professionnelles, ainsi que de l'ensemble de l'industrie e-mailing : fournisseurs d'accès internet (Orange, SFR ou La Poste), expéditeurs d'e-mails, et sociétés de sécurité.

Le rôle de Signal Spam est de collecter des signalements auprès des internautes concernant leur perception du spam, d'effectuer la qualification de ces signalements (message d'origine commerciale, phishing, spambot, etc.), et de les enrichir, notamment grâce aux informations que les FAI renvoient vers l'association, notamment le nombre de plaintes par adresse IP enregistrée chez Signal Spam ou encore le nombre de hits sur des spamtraps.

Les routeurs membres de Signal Spam s'inscrivent dans une démarche positive d'auto-régulation favorisée par les FAI et les autorités. Sans auto-régulation, les risques sont bien connus : blocages des IP, des noms de domaine et éventuellement des campagnes. Sans auto-régulation, les routeurs et expéditeurs risquent aussi de voir arriver un durcissement des dispositions légales et des contrôles pour infraction à la Loi Informatique et Libertés.

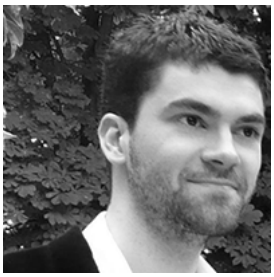
Pour ces raisons, il est important que les acteurs de l'industrie de l'e-mailing reçoivent des informations qui leur permettront de mieux exercer leur métier, dans des conditions toujours plus respectueuses du droit d'opposition et du ressenti des internautes.

Pour autant, les informations confiées par les internautes et les FAI à Signal Spam ne sont accessibles qu'aux membres dont la déclaration de conformité à la charte de déontologie de l'association (rédigée de manière collégiale par ses membres) a été validée.

La charte contient des recommandations basées sur les bonnes pratiques et propose des engagements pour toutes les catégories de membres de Signal Spam. Quelques critères déterminants : une procédure de désabonnement non seulement efficace, mais conforme aux meilleures pratiques, l'implémentation de standards technologiques, l'hygiène globale du parc d'adresses IP, ou encore le contrôle de la qualité des bases et des points de collecte…

À tout moment, l'accès aux données statistiques sur les IP peut être suspendu sur décision du FAI ou de l'association si ces derniers considèrent que les actions du routeur qui en bénéficie ne sont pas à la hauteur de ses engagements ou que les données sont utilisées à d'autres fins que celles prescrites par la charte de déontologie.

Pour découvrir la charte de Signal Spam : www.signal-spam.fr/faq/charte-déontologique



Thomas travaille pour signal Spam depuis Mai 2011, d'abord comme Chargé de mission ensuite comme Secrétaire Général. Il a supervisé l'association au moment où celle-ci développait des outils déterminant dans la régulation de l'e-mail marketing, comme les flux de données agrégées, et dans le domaine de la lutte contre le spam de nature cyber-criminelle. Il est également chef de projet pour Signal Spam au sein du groupement européen «ACDC» (Advanced Cyber-Defense Center), membre du M3AAWG, du London Action Plan, et du CECyF en qualité de représentant de Signal Spam.

Dimitri Perret, Business Developer, Vade-Retro

Vade-Retro est l'un des principaux fournisseur de solutions anti-spam en France, êtes vous parfois victimes de pressions (judiciaires ou autres) de la part d'expéditeurs d'emails mécontents ?

La technologie de Vade-Retro est en effet utilisé par les principaux FAI français, mais elle est aussi utilisée en entreprise et distribuée en Europe et dans le monde à travers un réseau de partenaires.

Pour ce qui est des pressions, oui, nous en subissons. Certains expéditeurs d'email aimeraient forcément obtenir une meilleure délivrabilité pour leurs emails. Et lorsqu'ils détectent que nos technologies sont à l'origine du filtrage de leurs emails, certains n'hésitent pas à nous le faire savoir. Pour autant, nous n'avons jamais réellement subi de plaintes devant la justice ou d'autres formes de pressions plus brutales (NDLR : On se souviendra des attaques DDOS contre Spamhaus).

D'ailleurs, nous avons mis en place une équipe dédiée afin de gérer la relation avec les expéditeurs qui nous demandent des conseils… ou des comptes. Nous les écoutons afin d'avoir une relation constructive avec eux. Néanmoins, la plupart du temps, cela reste l'hébergeur ou le FAI qui a toutes les cartes en main afin de renseigner l'expéditeur d'emails. Ce sont nos clients qui sont responsables du blocage d'un message ou non. C'est donc vers eux qu'ils faut se retourner en cas de blocage constaté. Si besoin, notre client reviendra vers nous afin d'investiguer sur la cause du blocage.

Une autre question qui revient souvent de la part des expéditeurs d'emails est le blocage éventuel de leurs emails par une blacklist interne à Vade-Retro. Il faut savoir q'une telle blacklist n'existe par réellement. C'est plus compliqué que cela. Si nous décidons de bloquer un acteur, c'est qu'il a abusé plusieurs fois, ou pire, qu'il a essayé de contourner notre technologie de filtrage. D'ailleurs, les blocages ne sont que très rarement permanent… Nous privilégions d'ailleurs une approche plus fine que la simple catégorisation « spam » ou « non-spam ». Nous essayons de faire la distinction entre un email inter-personnel, échangé entre deux humains

qui ont une conversation, le graymail, qui est un email commercial pour lequel il y a eu une permission de la part du destinataire et le spam. Cela rajoute une dimension au filtrage, ce n'est plus tout noir ou tout blanc, l'email peut être gris, non dangereux mais non prioritaire.

Vade-Retro essaye de se focaliser sur les bénéfices pour l'utilisateur, nous ne sommes pas contre les routeurs ou les annonceurs. C'est comme dans le sport, les arbitres ne sont pas contre les joueurs, ils sont là pour les réguler et faire en sorte qu'ils appliquent les règles du jeu. Pour tous les acteurs (annonceurs, hébergeur/FAI, utilisateur), c'est la qualité de l'expérience email et la sécurité qui comptent avant tout.

Dimitri est diplômé d'un Master en Marketing à l'Institut des Administrations et des Entreprises de Lille. Globetrotter, passionné de musique et de technologies, il débute sa carrière chez IBM, au sein de l'entité commerciale servant les hébergeurs et éditeurs de logiciels. Il rejoint ensuite Vade Retro Technology en tant que responsable marketing international pour accompagner le développement mondial de la société.

Julien Tartarin, Fondateur, Mailjet

Lorsque l'on a une plate-forme ouverte comme Mailjet, il est inévitable que des spammeurs et autres phishers tentent leur chance. Quels sont les moyens mis en place afin de lutter contre ceux-ci ?

C'est effectivement un défi auquel nous sommes confrontés chaque jour. Mais il faut bien en distinguer les deux facettes. D'une part, nous avons le spam classique, ou spam «Viagra», qui est bien moins problématique que le phishing et qui est aujourd'hui très simple à détecter. Durant la phase de processing des emails sur notre plateforme, nous utilisons nous-même différentes technologies de filtrage afin de détecter ce type d'email et de les bloquer avant la sortie.

Ensuite, avec le phishing, le problème prend une autre ampleur. L'email constitue bien souvent le point de départ d'une attaque de phishing. Cela a pour effet qu'il est très rare que les URLs utilisées soient déjà connues des différentes

listes recensant les attaques. D'autre part, si nous construisons un système de filtrage comparable à ce que l'on fait pour le spam « viagra », nous risquons de générer de nombreux faux positifs et donc de bloquer des expéditeurs tout à fait légitimes. Par exemple, si nous faisions des vérification sur des mots clefs tels que « Paypal », il y a beaucoup de chances que nous filtrions sans raison des emails de confirmation de sites ecommerce.

En pratique, nous faisons surtout de l'analyse comportementale. Cela nous permet de récupérer les schémas classiques utilisés par les phishers qui tentent d'utiliser notre plateforme. Cela nous permet de bloquer la plupart des tentatives d'attaques avant l'envoi du premier email.

Mais dans certains cas, c'est beaucoup plus difficile, et il arrive que certains arrivent à lancer leurs attaques. C'est alors la vitesse de réaction qui est primordiale. La suspension du compte est en général très rapide et nous veillons à ce que tous les liens de tracking contenus dans les emails soient désactivés afin de stopper net l'attaque. À la suite d'une attaque, nous prévenons aussi différentes organisations actives dans la lutte anti-spam / phishing afin que l'information se répande le plus vite possible et qu'elle puisse servir à bloquer d'autres attaques qui utiliseraient la même technique. Nous prévenons aussi systématiquement l'organisme qui est propriétaire de l'adresse email utilisée afin d'émettre une attaque.

Enfin, et c'est en fait le premier rempart, au moment de l'inscription de chaque nouveau client Mailjet, nous vérifions différents paramètres et les soumettons à un prestataire spécialisé afin de détecter d'éventuels fraudeurs. Les scores livrés par ce prestataire sont couplés à d'autres algorithmes de scoring internes afin de décider si un nouveau compte peut oui ou non être validé.

D'un point de vue délivrabilité, le phishing est clairement notre plus grand défi. Les efforts déployés sont très importants dans la mesure où nous faisons face à des techniques très élaborées.

Julien a fondé Mailjet en 2010 avec Wilfried Durand qu'il a rencontré durant ses études à l'université du Maine-La Mans-Laval d'où ils sont sortis en 2005. Julien est le concepteur du cœur de la plateforme Mailjet et continue aujourd'hui à en gérer une grand partie des aspects opérationnels et de délivrabilité. Mailjet compte aujourd'hui plus de 70 employés à travers le monde.

Mathieu Girol, Senior Technical Account Manager, Return Path

À l'heure actuelle, quelle est l'importance de DMARC pour les expéditeurs d'emails ? Est-ce qu'il est urgent de s'y mettre en France ou avons-nous encore un peu de temps ? Quels sont les secteurs qui devraient bouger en premier ?

L'authentification des Emails a maintenant une longue histoire. Certaines technologies comme SenderID ou ADSP sont tombées en désuétude, alors que SPF et DKIM se sont imposées comme des standards majeurs et incontournables. Pourtant malgré leur utilisation massive, ces 2 derniers standards ne parviennent pas séparément à accomplir l'objectif ultime de l'authentification, qui est de permettre aux domaines de réception de vérifier de manière sûre l'identité des expéditeurs d'emails et ainsi de bloquer les tentatives d'usurpation. DMARC vient justement remplir cette fonction.

En plus de protéger l'identité de l'expéditeur, DMARC permet à ce dernier d'avoir à la fois de la visibilité et des détails sur les attaques dont il est victime. Les rapports d'attaques DMARC sont donc une source de données exceptionnelle pour les équipes de sécurité.

Enfin il est important de savoir que si SPF et DKIM sont déjà en place, le passage à DMARC représente un coût technique dérisoire puisqu'il s'agit seulement d'un enregistrement DNS (Domain Name Server).

Tout expéditeur souhaitant protéger son identité se doit donc de passer à DMARC. Les entreprises aux activités

les plus sensibles telles que les Etablissements Bancaires et Financiers ainsi que les institutions (CAF, …) sont les premières victimes des attaques de phishing. Cependant la menace du phishing guette désormais quasiment l'ensemble des entreprises, même celles qui n'utilisent pas le canal Email ! En effet dès que le service offert par l'entreprise nécessite l'authentification (login / mot de passe) des utilisateurs, il existe un intérêt pour les phishers. La raison est simple, de nombreuses personnes utilisent le même mot de passe pour plusieurs services, voler les informations d'authentification d'un service permet in fine d'accéder aux autres.

Enfin l'usurpation d'identité ne se réduit pas qu'au phishing. Return Path détecte quotidiennement des emails frauduleux qui usurpent l'identité de marques connues. Contrairement au phishing, ces emails ne cherchent pas à voler des informations sensibles mais ont pour objectif de commercialiser différents types de produit allant des médicaments aux cigarettes électroniques. Ces emails usurpent l'image d'une marque connue essentiellement pour attirer l'attention de l'utilisateur et ainsi maximiser le taux d'ouverture de l'email et donc l'efficacité de la campagne de spam. Cette usurpation a de fâcheuses conséquences sur la marque ciblée. La première est évidemment la décrédibilisation de son image de marque et donc une perte d'engagement de ses clients. La seconde est la dégradation de la réputation du domaine d'envoi qui a pour conséquences de diminuer l'arrivée en boîte de réception des emails officiels de la marque. L'impact de ces malversations sur le business des entreprises qui dépendent de la communication par email peut être énorme.

Vous l'aurez compris DMARC est donc un mécanisme incontournable pour se protéger contre l'usurpation de domaine, mais attention dans le cadre du phishing il est relativement peu efficace lorsque les cybercriminels utilisent un domaine d'envoi qui n'est pas celui de la marque ciblée. D'où la nécessité d'aborder la problématique du phishing d'une manière plus globale, DMARC étant un outil essentiel mais non suffisant qui doit s'intégrer dans un dispositif plus large.

En conclusion, pour une meilleure efficacité et une meilleure protection, DMARC est le prolongement nécessaire de SPF et DKIM. Son implémentation nécessite une organisation spécifique pour traiter les rapports mais ne nécessite pas de nouvelle technologie. Il n'existe donc aucune raison

d'attendre pour l'utiliser, particulièrement si vous pensez que vos domaines sont ou peuvent être les cibles d'usurpation. Ne dit-on pas d'ailleurs qu'il faut vaut mieux prévenir que guérir ?

Expert en sécurité de l'email, Mathieu Girol a travaillé 4 ans chez Orange en tant que responsable sécurité du service de messagerie. Ancien vice-Chairman du groupe de travail sur l'anti-spam et l'anti-abuse de l'ETIS (www.etis.org), membre du MAAWG (www.m3aawg.org) et du conseil d'administration de Signal Spam (www.signal-spam.fr), il est aujourd'hui responsable technique pour les opérateurs de messagerie chez Return Path.

Jean-Michel Radiskol, Chief Deliverability Officer, Adobe, Neolane

Entre pool d'adresses IP partagées par plusieurs expéditeurs et adresses IP dédiées, quels sont les avantages et inconvénients de ces deux pratiques ? Est-ce qu'un pool partagé n'est pas une bonne manière pour les spammeurs de se fondre dans la masse ?

Le monde du marketing digital est un environnement en effervescence qui nous garde dans une dynamique forte et toujours plus créative, c'est un challenge que j'apprécie.

Avec 200 millions d'emails envoyés chaque jours, la réputation est devenue un point clef de la délivrabilité. Cette réputation peut être assimilée à l'empreinte qu'une entreprise va laisser sur le web. Dans le cas de l'emailing celle-ci sera basée sur l'IP et/ou le domaine.

Afin de se garantir une bonne réputation, il existe en effet deux stratégies distinctes : l'IP dite dédiée et l'IP dite partagée.

Avant de choisir l'une ou l'autre stratégie, il est important de savoir que l'IP dédiée est de manière générale une IP n'ayant pas connu de trafic, vierge de réputation, qui sera entièrement consacrée au trafic email d'une marque, d'un envoyeur. Dans ce cas, il va falloir réaliser un phase de

ramp-up, aussi appelé warm-up, qui consiste à augmenter progressivement le volume d'email sur les nouvelles IP. Cette augmentation progressive peut aller de 2 à 8 semaines en fonction du volume d'email à traiter et de la qualité de la base.

De l'autre côté, l'IP partagée est, comme l'indique son nom, un vecteur commun de trafic d'emails entre plusieurs marques / envoyeurs, ce qui implique qu'une réputation bonne ou mauvaise est déjà établie. Dans tous les cas, en dessous d'un volume de 2 millions d'emails envoyés par mois, environ 750.000 emails en base, on privilégiera l'IP partagée.

Au niveau des avantages et des inconvénients de ces deux stratégies, l'IP dédiée garantira un gestion personnelle de la réputation, permettra l'entrée dans certains programmes de certification ou d'avoir un branding complet de l'infrastructure de routage. De son côté, l'IP partagée à l'avantage d'une plus grande flexibilité au niveau des fréquences et des volumes d'envoi et d'un ramp-up quasi inexistant.

Mais les deux méthodes comportent aussi des inconvénients, l'IP dédiée passe obligatoirement par une période de ramp-up et nécessite des envois réguliers et une consistance dans les volumes. Au niveau des inconvénients de l'IP partagée, on pourra citer qu'aucun programme de certification n'est possible et qu'un seul envoyeur pourra impacter négativement l'ensemble de la réputation.

Pour répondre à la seconde partie de votre question sur l'exploitation par les spammeurs des pools d'IP partagées, les routeurs ont tout intérêt à détecter ces envoyeurs de mauvaise qualité le plus tôt possible. C'est pourquoi, même sur les IP's partagées, il est souvent prévu qu'un nouvel arrivant commence ses envois progressivement afin que nous puissions détecter les mauvaises bases et les mauvaises pratiques.

Dans le monde de l'emailing depuis plus de sept ans et en particulier dans le domaine de la délivrabilité, Jean-Michel Radiskol a connu un certain nombre d'évolutions majeurs (techniques et fonctionnelles) et a participé à l'adaptation des entreprises et de routeurs. À la tête du pole délivrabilité chez Adobe (ex Neolane) depuis presque 5 ans il a pu accompagner de grands comptes comme des petits avec toujours un souci de qualité, d'écoute et de performances.

Sébastien Fischer, Responsable délivrabilité, Cabestan

Est-ce qu'un routeur comme vous filtre le trafic e-mail sortant ? Pourquoi cette pratique ?

En tant que routeur email professionnel, nous avons le devoir de mettre en place différents filtres et règles afin de protéger notre plateforme, mais aussi nos clients. Aujourd'hui, plus personne n'est à l'abri de collecter et d'héberger des adresses emails dites sensibles qui peuvent impacter très fortement et très négativement la livraison des messages.

La conséquence d'une mauvaise qualité de liste peut non seulement avoir un impact sur un client, mais aussi mener au blacklistage d'un subnet complet (ensemble d'adresses IP d'un réseau) ou d'un ou plusieurs noms de domaines. Dans ce scénario, c'est l'ensemble des clients d'un routeur qui peuvent être menacés.

Au delà de la qualité des listes et du traffic, nous devons être en mesure d'assurer la satisfaction des destinataires de l'ensemble des communications électroniques générées par notre plateforme. Afin de mener ces missions à bien, nous utilisons deux types de filtrage.

Le premier se trouve du côté de l'environnement du client. Il consiste à écarter, avant l'envoi, différents types de scénarios. Par exemple, identifier les doublons, vérifier la syntaxe de l'adresse email, rejeter les adresses détectées en erreur lors de précédents envois (les NPAI), écarter les désinscriptions et éviter d'envoyer à nouveau vers des adresses ayant

générées des plaintes (que ce soit via les boucles de rétroactions ou la cellule Abuse de Cabestan). Enfin, il y a bien entendu les règles mises en place par nos clients, que ce soit sur des repoussoirs internes (adresses génériques, domaines jetables, récence de collecte de l'adresse email …) ou sur des règles métiers comme la pression commerciale.

Le second niveau de filtrage se trouve du côté serveur. À nouveau, ce filtrage consiste à écarter des adresses email extrêmement sensibles, comme par exemple une liste d'adresses e-mails de personnes ayant demandé à ne plus recevoir d'e-mails de clients Cabestan (blackliste interne), une liste d'adresses pièges connues que nous enrichissons régulièrement,une liste d'alias(comme les boîtes abuse@ et postmaster@) et de domaines sensibles.

Mais filtrer n'est pas suffisant ! Pour maitriser la réputation de nos clients et celle de notre plateforme, nous déployons beaucoup d'énergie afin d'informer nos clients sur les bonnes pratiques à mettre en place. Ces éléments sont les gages de tenue d'une bonne délivrabilité.

Ancien intégrateur et formateur e-mail, Sébastien Fischer s'est orienté vers l'univers passionnant de la délivrabilité en 2009. Après avoir fait partie des équipes délivrabilité de plusieurs grands routeurs (Emailvision / Smartfocus, Neolane/Adobe), il prend en mars 2013 la responsabilité du pôle délivrabilité de Cabestan. Depuis maintenant 5 ans, il accompagne, alerte, forme et conseille les entreprises aux bonnes pratiques de routage pour maximiser leur chance de délivrer en boite de réception et d'optimiser le ROI de leur campagne.

Retrouvez d'autres articles et interviews à propos de l'actualité e-CRM sur le blog de Badsender: www.badsender.com

Agence Agence eCRM et email marketing

Nous contacter

yesreplay@badsender.com

Conseil

Déploiement

Production

Badsender since 2010