Note technique relative aux dispositifs anti-spam de la messagerie AOL

Ce document rassemble, en une version française, l'essentiel des informations techniques et pratiques disponibles en langue anglaise sur le site http://postmaster.info.aol.com/ agrémentées de quelques précisions ou suggestions complémentaires.

1 CRITERES D'INSCRIPTION EN « LISTE BLANCHE » 2

1.1 CRITERES TECHNIQUES 2
1.2 CRITERES DE REDACTION DES E-MAILS 2
1.3 CRITERES PRATIQUES 3

2 QUELLES ADRESSES IP INSCRIRE SUR LISTE BLANCHE ? 3

2.1 SI VOUS AVEZ VOTRE PROPRE SERVEUR DE MAIL SMTP DEDIE, QUI ROUTE LES MESSAGES DIRECTEMENT SUR INTERNET (VERS AOL) 4
2.2 SI VOS MAILS SONT ROUTES PAR UN OU PLUSIEURS INTERMEDIAIRES AVANT D'ATTEINDRE AOL 5
2.3 SI VOUS NE CONNAISSEZ PAS LE TRAJET EMPRUNTE PAR VOS MAILS POUR ATTEINDRE AOL 6
2.4 SE PROTEGER CONTRE L'USURPATION D'IDENTITE AVEC SENDER POLICY FRAMEWORK (SPF) 8
2.5 QU'EST-CE QUE LA LISTE BLANCHE AMELIOREE (« ENHANCED WHITELIST ») ? 9
2.6 COMMENT INTERPRETER LES CODES D'ERREUR SMTP RETOURNES PAR AOL ? 9

3 INFORMATIONS PRATIQUES 10

3.1 QU'EST-CE QU'UNE BOUCLE DE RETROACTION (« FEEDBACK LOOP ») ? 10
3.2 A QUEL VOLUME DE « RETOURS » S'ATTENDRE VIA LA BOUCLE DE RETROACTION ? 11
3.3 DANS QUELS CAS UN SERVEUR DE MAIL EST-IL PLACE EN CONTROLE DE FLUX DYNAMIQUE PAR AOL ? 12
3.4 LES NOTIFICATIONS (« REPORT CARD ») 12
3.5 LE DOSSIER SPAM 13
3.6 RESUME DES CONSEILS PRATIQUES POUR UN MAILING VERS LES ABONNES AOL 14

4 COMMENT REMPLIR LE FORMULAIRE DE DEMANDE D'INSCRIPTION SUR LISTE BLANCHE ? 16

4.1 IDENTIFIER TOUTES LES ADRESSES IP DE VOTRE ORGANISATION QUI EXPEDIENT DU MAIL DIRECTEMENT VERS AOL. 16
4.2 VERIFIER QUE VOTRE DOMAINE DE MESSAGERIE EST CORRECTEMENT CONFIGURE SUR INTERNET 16
4.3 CHOISIR UNE ADRESSE DE RETROACTION ET VERIFIER QU'ELLE EST JOIGNABLE DE L'EXTERIEUR DE VOTRE ORGANISATION 17
4.4 RENSEIGNER LE FORMULAIRE « DEMANDE D'INSCRIPTION SUR LISTE BLANCHE POUR LA MESSAGERIE AOL » 17
4.5 SOUMETTRE VOTRE DEMANDE 17

5 DEMANDE D'INSCRIPTION SUR LISTE BLANCHE POUR LA MESSAGERIE AOL 18

5.1 CONTACT PRINCIPAL 18
5.2 CONTACT SECONDAIRE (OPTIONNEL) 18
5.3 INFORMATIONS SUR VOTRE ORGANISATION 18
5.4 LISTE DES ADRESSES IP A METTRE SUR LISTE BLANCHE 19
5.5 ADRESSE MAIL POUR LA BOUCLE DE RETROACTION (« FEEDBACK LOOP ») 19

AOL s'attache à fournir à ses abonnés la meilleure qualité de service possible, et nous sommes fiers d'être à l'écoute permanente des besoins de nos clients. La messagerie électronique constitue l'une des fonctionnalités principales de notre service en ligne, et son fonctionnement correct est vital pour la satisfaction de nos abonnés.

AOL n'autorise pas l'utilisation de ses ressources informatiques privées pour distribuer des e-mails non sollicités ou comportant des en-têtes invalides ou falsifiés[1]. A ce titre, AOL, en coopération avec Microsoft, vient d'obtenir le 5 mai 2004 la première condamnation d'un spammeur en France[2].

Les filtres anti-spam d'AOL filtrent jusqu'à 2,6 milliards d'e-mails par jour, soit 80% des e-mails à destination des abonnés AOL – une moyenne de 80 spams par jour et par abonné (source interne AOL). 83% des e-mails circulant sur Internet en mai 2004 seraient du spam (source : Postini Inc.).

Malheureusement, spams et mailings légitimes présentent les mêmes caractéristiques techniques, à savoir des e-mails répétitifs envoyés à de gros volumes d'abonnés AOL en peu de temps. Afin de minimiser les risques qu'un mailing légitime soit intercepté par son système anti-spam, AOL propose aux expéditeurs de gros volumes d'e-mails sollicités un programme de « liste blanche » (« whitelist »).

La liste blanche protège les e-mails soumis à destination d'abonnés AOL depuis certaines adresses IP, en désactivant la plupart des systèmes de filtrage du spam. L'inscription sur liste blanche est soumise au respect de critères techniques et de pratiques dans vos communications avec les abonnés AOL.

1 Critères d'inscription en « liste blanche »

1.1 Critères techniques

- Tout mail soumis doit être conforme aux normes (RFC) en vigueur sur Internet.
- Tout serveur expédiant des mails directement à AOL doit avoir un enregistrement dans le DNS inverse (champ PTR), c'est-à-dire un nom de domaine associé identifiable (cf. RFC 1912 § 2.1).
- Toute machine soumettant des mails à AOL doit être sécurisée afin d'interdire toute utilisation non autorisée ou anonyme – elle ne doit pas être un relais, routeur ou proxy « ouvert ».
- AOL n'accepte pas un mail en provenance directe d'une adresse IP résidentielle – qu'elle soit statique, ou à plus forte raison allouée dynamiquement.
- AOL n'accepte pas un mail comportant des URL encodées de façon superflue (%23%45%67), numériques (dont la partie « host » ne comporte pas de nom de domaine, par exemple http://127.0.0.1/) ou non conformes aux RFC (par exemple http://$_host/).
- Un serveur de mail doit envoyer au minimum 100 mails par mois à AOL afin de rester en « liste blanche ».

1.2 Critères de rédaction des e-mails

- Toute personne transmettant des e-mails depuis les adresses IP mises sur « liste blanche » ne doit pas tenter de masquer, falsifier ou usurper l'identité de l'émetteur ou la source des mails en question, de quelque façon que ce soit.
- Tout envoi de mail en quantité (liste de diffusion, « newsletters »…) doit impérativement mentionner comment et où l'adresse mail de chaque abonné AOL destinataire a été collectée, s'il s'agit d'un envoi unique ou récurrent, et la fréquence éventuelle des envois. Les détails tels que la date, heure (et fuseau horaire) de collecte de l'adresse mail, l'adresse IP d'où la demande d'abonnement a été effectuée et l'URL complète (site web) visitée pour effectuer la demande d'abonnement doivent être disponibles sur demande d'AOL.

[1] La formulation exacte des prescriptions anti-spam du service juridique d'AOL est consultable sur http://postmaster.info.aol.com/guidelines/bulk_email.html.
[2] http://www.aol.fr/presse/spammeur.htm, http://www.juriscom.net/jpt/visu.php?ID=510

- Tout envoi doit contenir un mécanisme simple et évident permettant de se désabonner *en un seul clic*. Un désabonnement par réponse mail (champ « Reply-To : ») peut également être proposé, auquel cas l'adresse spécifiée doit être valide.
- Tout envoi de mail en quantité doit mentionner comment contacter l'organisation émettrice de façon non électronique : nom de l'émetteur, numéro de téléphone et adresse physique. En cas d'impossibilité, un lien valide doit être fourni vers une page web comportant ces informations.
- Tout mail émis vers AOL doit se conformer à la législation en vigueur.

1.3 Critères pratiques

- Tout mailing vers AOL doit être sollicité, c'est-à-dire que l'émetteur doit avoir une relation existante et prouvable avec le destinataire, constituant l'accord du destinataire de recevoir ces mails, et que le destinataire n'a pas demandé à ne plus recevoir de tels mails en provenance de l'émetteur. Sur demande d'AOL, l'émetteur doit être en mesure de fournir l'historique et les détails de ses relations avec le destinataire.
- Toute personne expédiant des mails vers AOL depuis une adresse IP sur « liste blanche » doit désabonner définitivement le plus tôt possible toute adresse mail clôturée, inexistante, ou qui refuse l'émetteur, c'est-à-dire pour laquelle un retour expéditeur (« Delivery Status Notification : Failed », « Mailer-Daemon », « Returned Mail », « Undelivered Mail Returned to Sender », « Failure Notice »…) est généré avec un code d'erreur permanent.
- Une adresse IP sur « liste blanche » qui déclenche trop de plaintes de la part des abonnés AOL, au-delà de 10% de retours expéditeurs, ou n'accepte pas au moins 90% des retours expéditeurs qui lui sont renvoyés est susceptible d'être radiée de la « liste blanche » sans préavis. Cette radiation peut être étendue à toutes les adresses IP de l'organisation source de ces mails si ces violations sont récurrentes ou généralisées.
- Le respect de ces critères ou la mise sur « liste blanche » n'implique aucune relation, affiliation ou obligation contractuelle de quelque nature que ce soit de la part d'AOL envers les émetteurs de mail.
- Des audits réguliers des volumes de mail, plaintes et nombre de retours expéditeurs générés peuvent déclencher la radiation des adresses IP d'une organisation de la « liste blanche » sans préavis.
- La délivrance de mails peut être temporairement suspendue en cas d'incident technique majeur.

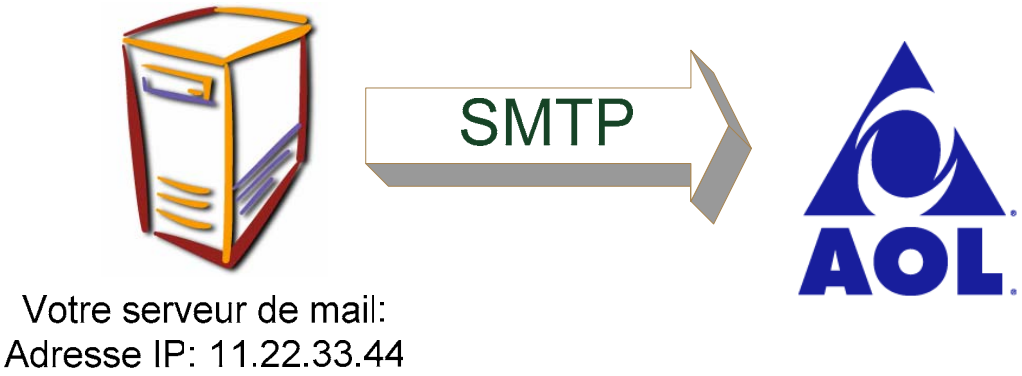
2 Quelles adresses IP inscrire sur liste blanche ?

Seules les adresses IP des serveurs SMTP qui soumettent *directement* des mails à AOL sont à inscrire sur la liste blanche. Tout dépend donc du « chemin réseau » qu'empruntent les mails que vous envoyez à destination d'AOL.

Note : ce sont les adresses IP des serveurs SMTP qui routent les mails « sortant » de votre domaine vers AOL qui nous intéressent, et non celles des serveurs qui acceptent les mails « en entrée » de votre domaine (qui réceptionnent les mails en provenance d'AOL par exemple), ces derniers étant facilement localisables via les enregistrements MX du DNS relatifs au domaine de messagerie concerné. Les « MX » peuvent cependant fournir une indication sur la plage d'adresses IP utilisée, les serveurs d'entrée et de sortie d'un domaine de messagerie étant souvent localisés au sein de la même plage /24.

2.1 Si vous avez votre propre serveur de mail SMTP dédié, qui route les messages directement sur Internet (vers AOL)

C'est le cas le plus simple et le plus favorable – vos messages parviendront directement de votre serveur à AOL, sans intermédiaire, et seront donc facilement identifiables au niveau réseau – ainsi, il sera possible de vous mettre individuellement sur liste blanche, et de valider la conformité de vos envois et la satisfaction des abonnés AOL suite à la réception de vos messages.



Dans ce cas, l'adresse IP à fournir sur le formulaire de demande de mise sur liste blanche est celle de votre serveur de mail : 11.22.33.44 dans cet exemple.

Vous êtes probablement dans ce cas si votre serveur de mail SMTP se trouve chez un hébergeur professionnel, dans un centre réseau en colocation par exemple.

Attention : AOL n'accepte pas un mail en provenance directe d'une adresse IP résidentielle – qu'elle soit statique, ou à plus forte raison attribuée dynamiquement. Si vous souscrivez une offre d'abonnement « haut débit » destinée aux particuliers (typiquement câble ou ADSL) auprès d'un Fournisseur d'Accès à Internet (FAI), et même si vous installez votre propre serveur de mail derrière un routeur câble ou ADSL, votre FAI vous attribuera probablement une adresse IP au sein d'une plage résidentielle, et il vous sera impossible d'expédier *directement* du courrier à destination d'AOL. Vous devrez obligatoirement router vos mails à destination d'AOL via le serveur de mail « officiel » fourni par votre FAI, avec les inconvénients associés – lire ci-dessous.

Deux conditions *nécessaires* pour vous assurer que l'adresse IP que votre FAI vous attribue n'est pas une adresse résidentielle sont :

1. obtenir une adresse IP statique, hors des plages que votre FAI a déclarées à AOL comme résidentielles, donc à bloquer
2. faire pointer le champ PTR (DNS inverse) de cette adresse IP vers votre nom de domaine, au lieu de celui de votre FAI

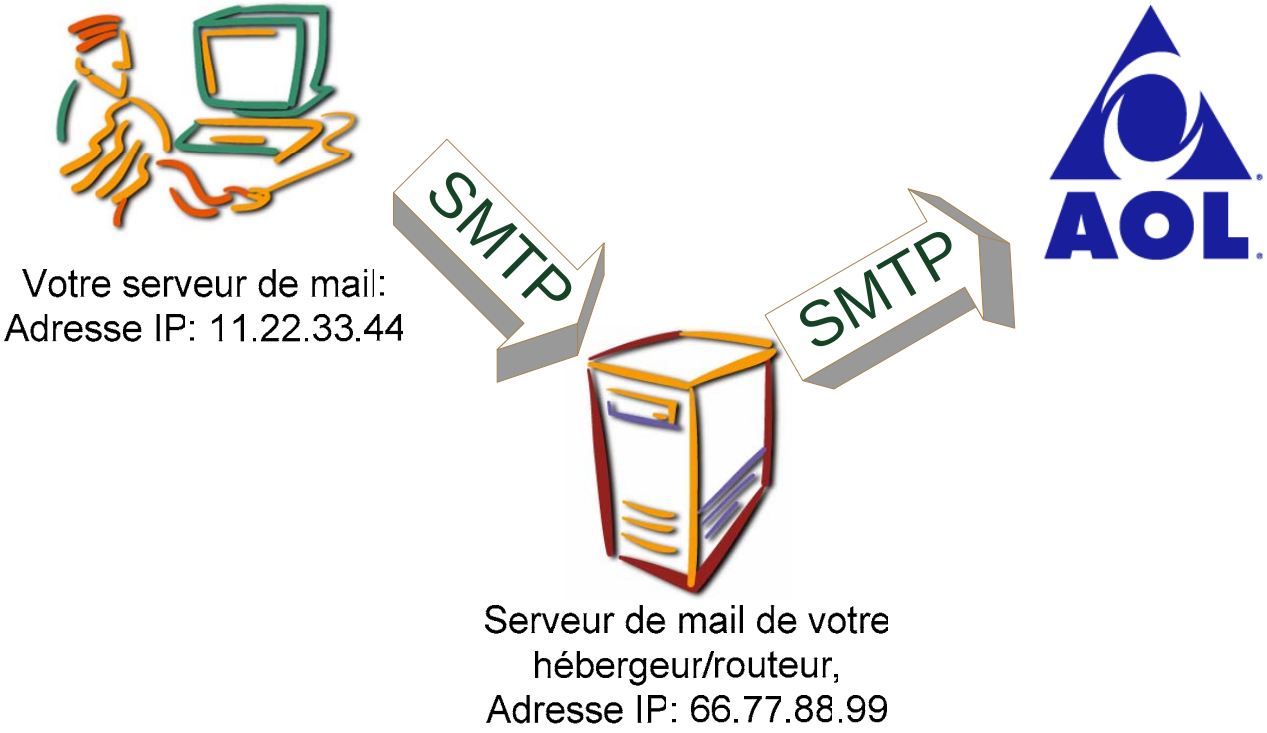
Cela permet d'imputer correctement les plaintes pour spam émises par les abonnés AOL sur votre nom de domaine au lieu de celui de votre FAI. Voici des exemples de champs PTR qui sont associés à des adresses IP considérées comme résidentielles, contrairement à un DNS inverse « professionnel » tel que mail.votresociete.com :

- AC96CBEC.ipt.aol.com
- l01v-58-230.d1.club-internet.fr
- m34.net81-66-86.noos.fr

- ip-101.net-80-236-24.asnieres.rev.numericable.fr
- alesia-4-82-66-58-27.fbx.proxad.net, lns-p19-5-82-65-31-153.adsl.proxad.net
- d213-101-205-201.cust.tele2.fr
- dyn-83-154-152-33.ppp.tiscali.fr
- atuileries-103-1-4-14.w80-11.abo.wanadoo.fr

Cas particulier : en cas de traduction d'adresses IP (NAPT, Network Address & Port Translation), il vous faut fournir les adresses *après traduction*, telles qu'elles seront perçues par les serveurs AOL – ces adresses étant destinées à renseigner une liste de contrôle d'accès (ACL) chez AOL.

2.2 Si vos mails sont routés par un ou plusieurs intermédiaires avant d'atteindre AOL



Dans ce cas, c'est l'adresse IP de la *dernière* machine par laquelle vos mails transitent, immédiatement avant de parvenir chez AOL, qu'il faudra fournir sur la demande de mise en liste blanche, à savoir 66.77.88.99 dans cet exemple. Inscrire la machine 11.22.33.44 sur liste blanche chez AOL n'aurait *aucun* effet puisque les mails seront reçus par AOL en provenance d'une adresse IP différente.

Le formulaire de demande de mise en liste blanche est donc à remplir, dans son intégralité, par l'administrateur système de la machine 66.77.88.99 – selon le cas, cela peut donc être votre hébergeur, votre prestataire, votre Fournisseur d'Accès à Internet, etc.

Cette architecture technique est à éviter pour les raisons suivantes :

- Si la machine de votre hébergeur (66.77.88.99) ne vous est pas dédiée mais est mutualisée et route les mails de plusieurs clients, il sera impossible de distinguer vos envois de mail de ceux des autres expéditeurs – en particulier, si l'un des autres clients hébergés sur le même serveur de mail que vous est un « spammeur », le serveur de mail entier (66.77.88.99) risque d'être placé en contrôle de flux dynamique par AOL, et vos mails ne seront pas délivrés.

- En environnement mutualisé chez un hébergeur, les plaintes des abonnés AOL, via la boucle de rétroaction (lire ci-dessous) seront retournées à l'administrateur du serveur de mail 66.77.88.99, donc il vous sera impossible d'avoir un accès direct à ces plaintes : il vous faudra négocier avec votre hébergeur ou prestataire afin qu'il vous fasse suivre celles qui vous concernent.

De même, effectuer vos envois via les serveurs de mail « grand public » d'un Fournisseur d'Accès à Internet pour particuliers est fortement déconseillé. En effet, depuis octobre 2003, le virus Gaobot[3] et ses 600 variantes se répandent et infectent les machines des abonnés Internet des FAI qui n'ont pas d'anti-virus ou de filtrage des ports MS-RPC. Ils prennent le contrôle de leurs ordinateurs, qu'ils transforment en « distributeurs de spam » émettant chacun quelques millions de spams par jour.

L'antivirus déployé sur les serveurs de mail AOL a intercepté plus d'un milliard de virus au cours des 12 derniers mois, soit plus de 30 virus par abonné et par an. De tels virus « spammeurs » émettent quelques centaines de mails vérolés pour se répliquer, et des millions de spams depuis l'adresse IP de chaque abonné infecté.

Les FAI non protégés contre ces attaques internes, ou qui appliquent des politiques laxistes de gestion des plaintes pour spam émis par leurs abonnés, se retrouvent alors avec des serveurs de mail saturés, dont plus de 99% des mails sortant sont du spam certains jours. Certains FAI imposent des quotas en émission sur leurs abonnés résidentiels afin de limiter ce type d'incidents. Lorsqu'ils n'ont pas de tels quotas en place et ne maîtrisent pas la quantité de spam qui sort quotidiennement de leurs serveurs, AOL leur en impose en réception afin de pouvoir continuer à accepter leurs mails malgré le déluge de spam associé. Toutes ces mesures techniques d'endiguement du spam peuvent paralyser vos envois en masse.

Ainsi, passer par les serveurs de mail d'un FAI « grand public » pour effectuer des mailings en masse a fort peu de chances de réussir : vos mails seraient noyés dans les 99% de spam qui sortent de tels serveurs mal configurés et non protégés.

En conclusion :

Pour effectuer des envois importants en volume, de manière régulière et récurrente vers AOL dans les meilleures conditions possibles en minimisant les risques d'incident, il est recommandé d'avoir son propre serveur de mail SMTP, en colocation chez un hébergeur professionnel. Ainsi, ce serveur indépendant ne sera pas soumis aux restrictions imposées sur les serveurs de mail de FAI « grand public ».

Un mailing émis à travers les serveurs de mail d'un FAI « grand public » a fort peu de chances d'aboutir : dans le meilleur des cas, seule une fraction de vos mails sera délivrée, et ce très probablement dans le dossier spam des destinataires.

Si votre courrier est routé via le serveur de mail mutualisé d'un prestataire, assurez-vous que ce dernier lutte efficacement contre ses propres clients « spammeurs ».

2.3 Si vous ne connaissez pas le trajet emprunté par vos mails pour atteindre AOL

Il vous suffit d'envoyer un mail, via le même processus et le même serveur que vous comptez utiliser pour vos mailings vers les abonnés AOL, à destination d'une adresse mail extérieure à votre organisation,

[3] http://securityresponse.symantec.com/avcenter/venc/data/w32.hllw.gaobot.gen.html

par exemple un compte webmail gratuit tel que Yahoo!Mail, voila.fr ou LaPoste.net. Les en-têtes du mail reçu vous révèleront le trajet emprunté par votre mail. Voici un exemple d'analyse :

```
Return-Path: <reservations@pascher.com>
Received: from  rly-xn02.mx.aol.com (rly-xn02.mail.aol.com [172.20.83.135])
  by air-xn02.mail.aol.com (v98.19) with ESMTP
  id MAILINXN23-6344094415218e; Sat, 01 May 2004 20:31:38 -0400
Received: from  mail1.hosting.net (mail1.hosting.net [213.180.1.68])
  by rly-xn02.mx.aol.com (v98.5) with ESMTP
  id MAILRELAYINXN28-6344094415218e; Sat, 01 May 2004 20:31:14 -0400
Received: from www.pascher.com ([213.180.109.51] helo=1089-trk-web02)
  by mail1.hosting.net with esmtp (Exim 4.32)
  id 1BK4sz-0001Az-O3
  for ClaireLucas@aol.com; Sun, 02 May 2004 02:31:13 +0200
From: "PasCher.com" <reservations@pascher.com>
To: ClaireLucas@aol.com
Subject: VOS RESERVATIONS SONT ARRIVEES !
Date: Sun, 02 May 2004 02:16:22 +0200
```

Ce sont les lignes « `Received:` » qui balisent la trajectoire d'un mail, chaque serveur SMTP intermédiaire en ajoutant une au-dessus des précédentes. Pour remonter le trajet d'un mail, il suffit donc de les interpréter une par une, de haut en bas.

```
Received: from  rly-xn02.mx.aol.com (rly-xn02.mail.aol.com [172.20.83.135])
  by air-xn02.mail.aol.com (v98.19) with ESMTP
  id MAILINXN23-6344094415218e; Sat, 01 May 2004 20:31:38 -0400
```

Cette ligne a été rédigée par **air-xn02.mail.aol.com**, qui indique avoir reçu ce mail en provenance de **rly-xn02.mail.aol.com [172.20.83.135]**. Ce sont tous deux des serveurs de mail internes à AOL. Il faut donc rechercher au sein des lignes « `Received:` » suivantes d'où ce mail a été expédié vers AOL.

```
Received: from  mail1.hosting.net (mail1.hosting.net [213.180.1.68])
  by rly-xn02.mx.aol.com (v98.5) with ESMTP
  id MAILRELAYINXN28-6344094415218e; Sat, 01 May 2004 20:31:14 -0400
```

Cette ligne a été rédigée par **rly-xn02.mx.aol.com** – le relais SMTP qui transmet le mail à air-xn02.mail.aol.com ensuite. Le mail est en provenance de **mail1.hosting.net [213.180.1.68]**.

C'est bien l'adresse IP recherchée ici : **213.180.1.68**, à savoir la dernière étape immédiatement avant l'arrivée du mail sur les serveurs du destinataire – AOL, Yahoo! voila.fr, laposte.net selon le cas – et c'est cette adresse qu'il faudra inscrire sur liste blanche chez AOL.

Accessoirement, en continuant l'analyse, on découvre sur la ligne suivante que mail1.hosting.net a probablement reçu ce mail en provenance de 213.180.109.51 :

```
Received: from www.pascher.com ([213.180.109.51] helo=1089-trk-web02)
  by mail1.hosting.net with esmtp (Exim 4.32)
  id 1BK4sz-0001Az-O3
  for ClaireLucas@aol.com; Sun, 02 May 2004 02:31:13 +0200
```

Cette ligne n'est pas considérée par nos systèmes anti-spam – en effet, elle a été rédigée par une machine hors administration AOL, et a donc très bien pu être falsifiée.

Dans cet exemple, le formulaire de demande de mise sur « liste blanche » pour l'adresse 213.180.1.68 est à remplir par l'hébergeur **hosting.net** – et non pas par l'émetteur du mailing, pascher.com.

Inversement, AOL retournera toute plainte reçue concernant ces mails à l'hébergeur, via son adresse abuse@hosting.net, à charge pour lui de les répartir entre ses différents clients. AOL ne pourra pas retourner les plaintes de ses abonnés directement à l'émetteur, pascher.com, car il route ses mailings via un serveur SMTP mutualisé entre plusieurs sociétés.

2.4 Se protéger contre l'usurpation d'identité avec Sender Policy Framework (SPF)

La majorité des spams circulant sur Internet contient des en-têtes falsifiés. SPF est un standard émergent pour réduire concrètement le nombre de retours expéditeurs reçus sur des mails que vous n'avez jamais envoyés. SPF permet de se protéger en partie contre l'usurpation d'identité, appelée également « spoofing », et donc de bloquer certains spams et virus avant même la transmission du corps d'un message. SPF protège l'adresse de retour expéditeur d'un mail : « Return-Path : » ou « RFC 2821 Envelope Sender ».

AOL travaille avec l'Internet Engineering Task Force (IETF) et les principaux acteurs de l'industrie afin de standardiser et de généraliser des technologies telles que SPF, Caller-ID et DomainKeys sur Internet.

AOL commence à utiliser SPF pour maintenir la liste blanche elle-même, et à vérifier les enregistrements SPF publiés par les domaines de messagerie tiers. Sans enregistrement SPF à jour publié dans le DNS de votre domaine de messagerie, votre enregistrement sur liste blanche risque donc d'expirer.

Publier un enregistrement DNS SPF est extrêmement simple techniquement, et démontre votre motivation à lutter contre l'usurpation d'identité : il suffit de rajouter une ligne – un champ TXT – dans l'entrée DNS correspondant à votre nom de domaine. Alors que les champs « MX » indiquent les serveurs de mail en entrée de votre domaine de messagerie, les champs SPF indiquent quels sont les seuls serveurs autorisés à router les mails en sortie de votre domaine.

Un guide pour le déploiement de SPF est disponible sur http://spf.pobox.com/forsysadmins.html, ainsi qu'un assistant pour la rédaction des enregistrements : http://spf.pobox.com/wizard.html.

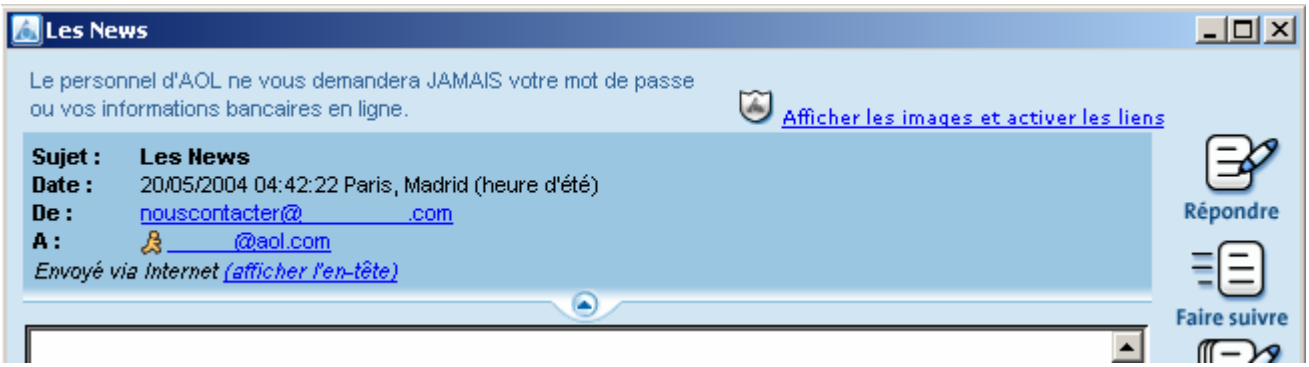
Si ultérieurement vous souhaitez exploiter SPF pour bloquer les mails porteurs d'en-têtes falsifiés sur votre propre serveur de mail, des modules de vérification SPF sont disponibles sur http://spf.pobox.com/downloads.html pour les logiciels serveurs SMTP les plus courants : Sendmail, Postfix, Exim, Qmail…

Le site officiel consacré à SPF est http://spf.pobox.com/ et recense déjà 15.000 domaines ayant adopté cette technologie, dont AOL.com, DynDNS.org, Google.com, GNU.org, OReilly.com, Oxford.ac.uk, Perl.org, PhilZimmermann.com, SAP.com, Spamhaus.org, Symantec.com, W3.org…

Fin mai 2004, l'enregistrement SPF pour le domaine de messagerie aol.com est : "v=spf1 ip4:152.163.225.0/24 ip4:205.188.139.0/24 ip4:205.188.144.0/24 ip4:205.188.156.0/23 ip4:205.188.159.0/24 ip4:64.12.136.0/23 ip4:64.12.138.0/24 ptr:mx.aol.com ?all".

2.5 Qu'est-ce que la liste blanche améliorée (« Enhanced WhiteList ») ?

Par souci de sécurité, les versions les plus récentes du logiciel AOL désactivent les liens et l'affichage des images incrustées dans un mail en provenance d'un expéditeur inconnu de l'abonné AOL destinataire. Ce dernier peut cliquer sur « **Afficher les images et activer les liens** » pour les rétablir.



La « liste blanche améliorée » supprime cette restriction pour les expéditeurs de mail en masse

1. qui figurent déjà sur la liste blanche
2. et dont le taux de plaintes enregistrées par AOL est stable dans le temps, et faible

Le passage d'une adresse IP en liste blanche améliorée est automatique au bout de 30 jours consécutifs sans dépassement du seuil de plaintes autorisé. Il n'y a pas de demande spécifique à faire auprès d'AOL, ni d'intervention manuelle : l'ensemble du processus est entièrement automatisé.

L'évaluation des critères pour cette liste blanche améliorée se fait adresse IP par adresse IP, et non pour un domaine entier. En cas de dépassement du seuil de plaintes, une adresse IP est retirée automatiquement de la liste, et y retourne au bout de 30 jours consécutifs sans dépassement de seuil.

Ceci constitue une raison supplémentaire de ne pas envoyer vos mails via un FAI « grand public » mais bien de sous-traiter à un prestataire, hébergeur, routeur de mail ou gestionnaire de listes de diffusion professionnel compétent, ou d'avoir votre propre serveur de mail dédié.

2.6 Comment interpréter les codes d'erreur SMTP retournés par AOL ?

Un code d'erreur permanent, typiquement 550 à 554 est retourné lorsqu'un mail est refusé par AOL. Ce code ne signifie rien en lui-même – sauf que le mail a été définitivement refusé. La motivation exacte du refus est explicitée via le commentaire en langue anglaise qui accompagne ce code d'erreur :

Exemple : *550 "username" Is Not Accepting Mail From This Sender*

Cette erreur indique que l'abonné AOL destinataire a configuré, volontairement ou involontairement, sa boîte aux lettres afin de restreindre les expéditeurs ou les domaines de messagerie desquels il accepte du mail en provenance de l'Internet. Il lui faudra modifier ses préférences, via le mot-clé AOL « Contrôle du spam », afin de pouvoir recevoir vos mails. AOL respecte la confidentialité et la vie privée de ses abonnés, et les vaguemestres (Postmasters) AOL ne peuvent ni modifier les réglages de l'abonné, ni faire suivre vos mails.

Un exemple de boîte aux lettres configurée expressément de façon restrictive

Une liste des différents messages d'erreur et de leurs explications complètes est disponible sur http://postmaster.info.aol.com/errors/, ainsi qu'un assistant pour leur interprétation : http://postmaster.info.aol.com/selfhelp/

3 Informations pratiques

3.1 Qu'est-ce qu'une boucle de rétroaction (« Feedback Loop ») ?

L'existence d'une boucle de rétroaction est indispensable à la mise sur « liste blanche » d'adresses IP.

Une boucle de rétroaction est une adresse de type « abuse@votredomaine.fr », cf. RFC 2142 § 1, 2 et 4, http://www.rfc-ignorant.org/rfcs/rfc2142.php.

Le logiciel AOL dispose d'un bouton « **Signaler un spam** » (AOL 8), ou « **Spam** » (AOL 9), qui permet aux abonnés de transmettre tout mail indésirable ou non sollicité, afin qu'il soit enregistré comme spam et analysé. Si une boucle de rétroaction est configurée sur l'adresse IP source, ce mail sera renvoyé à l'adresse de rétroaction « abuse@... » enregistrée.

AOL masque les destinataires (champs « To : » et « Cc : ») du mail d'origine avant de vous retourner ces mails. Cependant, le corps du message lui-même n'est pas modifié. L'ensemble vous est alors renvoyé, sous forme d'attachement, par un mail en provenance de l'adresse scomp@aol.net, ayant pour sujet « Client TOS Notification », à destination de l'adresse « abuse@votredomaine.fr » que vous avez renseignée.

Chaque mail scomp@aol.net résulte de l'action manuelle de l'un de nos abonnés sur le bouton « **Spam** ». Il n'y a aucune automatisation. Si un processus automatisé avait décidé de rejeter votre mail – tel que les filtres anti-spam, une adresse destinataire invalide, clôturée, inexistante ou une boîte aux lettres configurée, volontairement ou involontairement, pour refuser ce mail – vous auriez alors reçu une erreur SMTP permanente (typiquement 550 à 554), soit en ligne lors de la transaction SMTP, soit sous forme de retour expéditeur : « Returned Mail : User Unknown » de Mailer-Daemon@aol.com.

Tout retour de mail via la boucle de rétroaction « SComp » (Spam Complaints) indique donc :

- que votre mail a bien été délivré dans la boîte aux lettres de l'abonné, et
- que l'abonné AOL a manuellement cliqué sur le bouton « Spam » pour signifier qu'il considère ce mail comme indésirable.

Un abonné peut cliquer « par erreur » sur le bouton « Spam », mais d'après notre expérience ces « erreurs » sont rares. Par ailleurs, le système anti-spam côté serveur AOL ne prend pas de décisions de contrôle de flux sur des clics individuels mais sur des centaines de rapports de spam d'abonnés différents afin de diluer statistiquement l'influence de telles erreurs.

Note : le champ expéditeur apparent (« From ») des mails signalés comme indésirables par nos abonnés est totalement ignoré, car il est falsifiable techniquement. Seule l'adresse IP d'où le mail est parvenu, au niveau réseau, ne peut être falsifiée, et c'est donc là-dessus que tous les filtres, mécanismes anti-spam et de traitement des plaintes des abonnés AOL sont basés.

L'intérêt de la boucle de rétroaction pour l'administrateur du serveur de mail émetteur est donc qu'elle lui permet de piloter quasiment en temps réel le nombre de clics sur le bouton « Spam » de la part des abonnés AOL destinataires, et donc d'avoir un retour quasi-immédiat sur la désirabilité des mails envoyés. Egalement, elle permet à l'administrateur de surveiller tout usage non conforme ou non autorisé de son serveur de mail.

AOL enregistre en général 35% des plaintes pour spam dans les 24 heures suivant l'envoi d'un mailing, autant le lendemain, et 10% le troisième jour, au fur et à mesure que les abonnés consultent leur boîte aux lettres – 80% des plaintes sont donc généralement émises dans les 72 heures suivant l'envoi.

La plupart des professionnels qui routent des mailings vers AOL tirent parti de cette boucle de rétroaction afin de désabonner automatiquement de leurs listes tout abonné AOL qui clique sur le bouton « Spam ». Globalement cette pratique est mutuellement bénéficiaire :

- le diffuseur de newsletters est ainsi capable d'épurer sa liste d'abonnés AOL en temps réel, et ainsi de s'assurer que tous ses mails sont bien sollicités, ce qui augmente d'autant la valeur de sa base d'abonnés
- AOL enregistre en quelques jours une baisse du nombre de clics sur le bouton « Spam », ce qui signifie que la satisfaction des abonnés augmente et que tous les mails reçus sont bien sollicités

3.2 A quel volume de « retours » s'attendre via la boucle de rétroaction ?

Vous pouvez vous attendre à un nombre de mails retournés via la boucle de rétroaction de l'ordre de 1% environ du nombre de destinataires AOL auxquels vous écrivez.

Exemple : vous envoyez quelques newsletters pour un total de 300000 destinataires (non uniques) AOL additionnés. Vous pouvez prévoir de 500 à 5000 mails en retour de scomp@aol.net vers l'adresse de

rétroaction que vous avez renseignée. La boîte aux lettres recevant les retours via la boucle de rétroaction doit donc être dimensionnée en conséquence : quotas, espace disque…

La création d'une boîte aux lettres dédiée à AOL est fortement conseillée, par exemple « abuse-aol@votredomaine.fr », afin de ne pas noyer l'adresse abuse@votredomaine.fr qui existe probablement déjà, selon les recommandations de la RFC 2142 § 1, 2 et 4, cf. http://www.rfc-ignorant.org/rfcs/rfc2142.php. Une autre solution consiste à filtrer tout mail en provenance de scomp@aol.net à destination de l'adresse abuse@votredomaine.fr afin de les aiguiller vers un processus de traitement séparé et automatisé de radiation de vos listes.

Vérifiez que l'adresse de rétroaction que vous fournissez est valide et accepte les mails en provenance de l'Internet avant de retourner le formulaire complété, par exemple en y expédiant un mail depuis un webmail externe à votre société (Yahoo!Mail, voila.fr, laposte.net…). En effet, la procédure envoie un mail de validation à cette adresse : il vous faudra accéder à ce mail afin de valider votre demande de mise sur liste blanche.

3.3 Dans quels cas un serveur de mail est-il placé en contrôle de flux dynamique par AOL ?

Le ratio $\frac{nombre\,de\,clics\,sur\,le\,bouton\,"Spam"}{nombre\,de\,destinataires\,AOL\,délivrés}$ permet de mesurer quantitativement la « désirabilité » de vos mails par les abonnés AOL. Il permet de transcender les problématiques « opt-in », « double opt-in » versus « opt-out » de constitution de vos listes d'abonnés : si vos mails sont indésirables, votre ratio sera très rapidement « hors norme », quelle que soit la méthode utilisée, y compris légitime.

Tout serveur SMTP en dépassement de seuil est automatiquement (en l'espace de quelques secondes) placé en contrôle de flux : le système de messagerie d'AOL refusera temporairement toute nouvelle admission de mail, pour une durée de l'ordre de 24h environ. Ce contrôle de flux dynamique a pour objectif de protéger le système de messagerie AOL contre les injections massives de spam qui le visent périodiquement. Il n'y a aucun moyen simple de déverrouiller un serveur SMTP placé en contrôle de flux dynamique : il suffit d'attendre 24h environ, et les restrictions en émission disparaîtront d'elles-mêmes, à charge pour le serveur distant de ne pas dépasser le seuil de plaintes à nouveau. Si tel est le cas, il sera à nouveau placé sous contrôle de flux dynamique en quelques secondes.

3.4 Les notifications (« Report Card »)

Si l'un de vos serveurs de mail SMTP se retrouve placé par AOL en contrôle de flux dynamique pour dépassement du seuil de plaintes auprès de nos abonnés, une notification (« Report Card ») sera automatiquement expédiée, une fois par jour, à l'attention de l'administrateur du domaine de messagerie distant, consolidant les chiffres du nombres de plaintes recensées à travers tout le domaine DNS inverse concerné.

Une notification par jour est envoyée au maximum par domaine concerné, ce dernier étant obtenu par le champ PTR (DNS inversé) sur l'adresse IP du serveur de mail incriminé. Il est donc extrêmement important que les champs PTR sur vos adresses IP pointent vers le domaine qui souhaite être notifié, et non vers son hébergeur ou son FAI amont.

Exemple : smtp.pascher.com = 12.34.56.78 expédie *directement* ses mails vers AOL, mais le champ PTR (DNS inverse) associé à 12.34.56.78 pointe vers host334.hosting.net.
Dans ce cas, la notification sera expédiée à l'administrateur du domaine hosting.net, et non à celui de pascher.com, et les plaintes seront consolidées avec toutes les autres du domaine hosting.net – il sera impossible d'avoir un rapport individuel concernant pascher.com.

Si pascher.com souhaite obtenir un rapport individuel du nombre de plaintes générées, il devra demander à son hébergeur professionnel de modifier le champ PTR pour le faire pointer sur le domaine pascher.com.

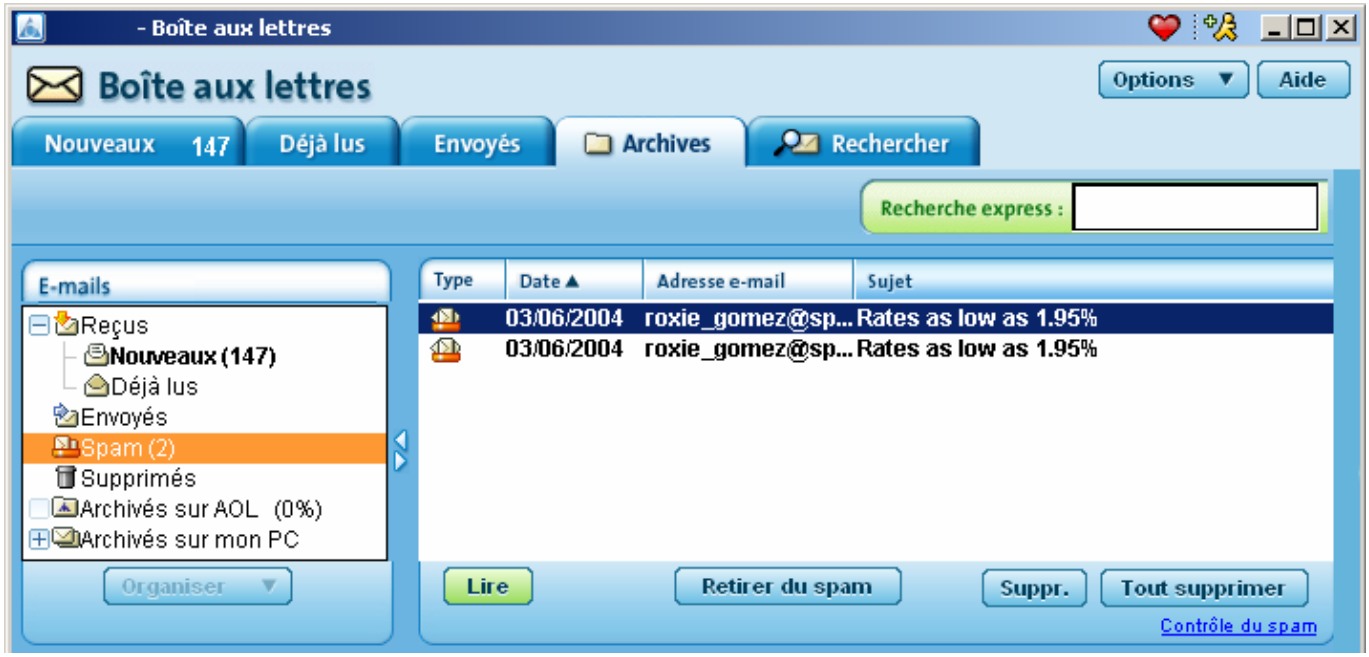
Les notifications sont envoyées par mail chaque jour, pour chaque domaine (DNS inverse) concerné, aux adresses postmaster@domaine et abuse@domaine. Ces adresses ne sont pas configurables par AOL actuellement.

Si vous recevez régulièrement de telles notifications, il vous faudra réexaminer vos procédures d'acquisition et de gestion de vos listes de diffusion : vous risquez en effet d'être placé en contrôle de flux régulièrement, et cela perturbera la diffusion de vos communications à l'attention des abonnés AOL.

Il n'y a pas d'avertissement anticipé lors de la mise en contrôle de flux de vos serveurs – vous vous en apercevrez en consultant les fichiers logs de votre serveur de mail, par la présence d'erreurs « 554 RLY:B1 ».

3.5 Le dossier spam

AOL 9.0 est doté de nouveaux filtres anti-spam très performants, dont un filtre intelligent et spécifique à chaque abonné AOL, qui améliore le filtrage de jour en jour par apprentissage en fonction des actions que chaque abonné mène sur ses mails, spécifiquement les clics sur les boutons « Spam » et « Retirer du spam ». La précision de ce filtrage s'affine au cours du temps, et ainsi, en quelques jours, le filtre s'adapte aux préférences individuelles de chaque abonné AOL. Il déplace les mails qu'il considère comme probablement indésirables hors de la boîte de réception principale de l'abonné vers un nouveau dossier de l'onglet Archives : le « dossier spam ».



La mise sur liste blanche n'a pas d'effet sur la répartition des nouveaux mails entre la boîte de réception (« Inbox ») et le « dossier spam » d'un abonné AOL.

Lorsque AOL délivre un mail dans la boîte aux lettres d'un de ses abonnés, le filtrage adaptatif statistique individualisé de chaque abonné décide si ce mail doit être stocké dans la boîte de réception ou le dossier spam. Ce filtre ne dépend que des préférences et de l'apprentissage que chaque abonné a donné à son filtre via les clics sur les boutons « Spam » et « Retirer du Spam ». AOL ne peut pas modifier les caractéristiques du filtre d'un abonné individuel.

Afin de minimiser les chances que vos mailings légitimes soient dirigés vers le dossier spam, nous vous conseillons d'utiliser toujours la même adresse émetteur dans vos mails à destination des abonnés AOL, et de leur suggérer d'enregistrer cette adresse émetteur comme contact dans leur carnet d'adresses. Cette précaution garantit que vos mails ultérieurs expédiés depuis cette adresse ne peuvent alors plus être routés vers le dossier spam.

Egalement, si un abonné AOL ne reçoit pas les mails que vous lui envoyez, conseillez lui d'aller consulter son dossier spam (mot-clé AOL : DossierSpam) : peut-être y retrouvera-t-il les mails que vous lui avez expédiés au cours des 5 derniers jours. Il suffira alors à cet abonné AOL de sélectionner votre mail et de cliquer sur le bouton « Retirer du spam » pour récupérer le message. Cette action rajoute automatiquement l'adresse de l'émetteur dans son carnet d'adresses, prévenant ainsi toute erreur de classification future.

3.6 Résumé des conseils pratiques pour un mailing vers les abonnés AOL

Avoir son propre serveur de mail qui route directement les mails vers AOL, ou sous-traiter à un prestataire professionnel « sérieux » qui lutte efficacement contre le spam, y compris parmi ses propres clients. Eviter les serveurs de mail mutualisés, et à plus forte raison les FAI « grand public ».

Avoir deux serveurs de mail différents – deux adresses IP distinctes – pour expédier directement à AOL les mails non récurrents d'un côté (confirmation de commandes, etc.) et les newsletters récurrentes de l'autre. Ainsi, si ce dernier serveur se retrouve en contrôle de flux dynamique, vos confirmations de commandes ne seront pas impactées. Pour les mêmes raisons, il est conseillé d'acheminer le mail des employés de votre société via une adresse IP différente que celle servant pour les envois en masse.

Désabonner immédiatement et définitivement les adresses mail AOL invalides, clôturées, inexistantes, ou configurées pour refuser vos mails.

Utiliser à bon escient la « boucle de rétroaction » afin de désabonner le plus rapidement possible et définitivement les abonnés qui cliquent sur le bouton « Spam » et ainsi font « monter » votre « score » spam, ce qui risque à terme de vous placer en franchissement de seuil et en contrôle de flux dynamique. Idéalement les abonnés utiliseraient le lien placé à l'intérieur de chacun de vos mails pour se désabonner, cependant dans les spams « purs et durs », ces liens ne fonctionnent pas ou ne servent qu'à confirmer l'existence de la boîte aux lettres correspondante, ce qui démultiplie le spam ultérieurement – il n'est donc pas surprenant que certains internautes n'utilisent plus ces liens par méfiance.

Conserver le même expéditeur dans vos communications avec les abonnés AOL, et leur suggérer de le rajouter dans leur carnet d'adresses personnel afin que vos mails légitimes ne puissent être routés vers le dossier « spam ».

Mentionner dans vos communications un expéditeur et un sujet explicites, qui ne puissent pas prêter au doute ou à la confusion avec les sujets habituels du spam. Le logiciel AOL n'affiche pas le commentaire mais bien l'adresse messagerie de l'expéditeur du mail, ou à défaut « UnknownSender@UnknownDomain ». Un mail comportant comme en-tête :

> From: Lettre d'information de PasCher.com <nobody@h335.hosting.net>
> Subject: Confirmation

sera affiché dans le logiciel AOL comme en provenance de nobody@h335.hosting.net – le commentaire n'est pas affiché – et avec le sujet « Confirmation » – voila qui est assez énigmatique, et peut-être assimilé à du spam.

Un tel mail ne sera donc pas immédiatement reconnaissable par l'abonné, car ni l'adresse expéditeur affichée ni le sujet du mail ne référencent votre marque. Il est fort probable que nombre d'abonnés AOL vont alors cliquer sur le bouton « Spam » sans même avoir ouvert le message et vérifié son contenu.

Eviter la constitution « à la sauvette » de listes de diffusion via un champ à remplir sur une page web, du type « Tapez votre adresse mail puis cliquez sur OK pour vous abonner ». Nous suggérons fortement, dans ce cas, d'envoyer une demande de validation préalable à l'adresse mentionnée afin de vérifier que l'abonnement à la lettre d'information est sollicité :

> Quelqu'un (potentiellement vous) a inscrit cette adresse mail sur notre liste de diffusion bons-plans@pascher.com. Nous souhaitons nous assurer que vous êtes l'auteur de cette demande, et que cet abonnement est bien sollicité.
> Pour valider votre inscription, veuillez répondre à ce message, ou cliquer sur ce lien … sous 48 heures. Dans le cas contraire, merci d'effacer ce message et ne pas en tenir compte – nous nous excusons de la gêne occasionnée.
>
> Traçabilité : cette demande d'abonnement a été effectuée via l'URL … depuis l'adresse IP 12.34.56.78 le 3 mai 2004 à 17h32 (heure de Paris).

Cette procédure en deux étapes est certes plus contraignante, mais elle permet de s'assurer sans erreur possible que l'adresse mail fournie est correcte et que l'abonnement est bien sollicité. Elle instaure une relation de confiance, de transparence et de sécurité entre l'abonné et vous, et garantit un taux de plaintes extrêmement faible ultérieurement.

Un audit récent d'un de nos partenaires a révélé qu'il expédiait 30.000 newsletters hebdomadaires à des adresses mail @aol.fr. Or, il n'y a aucune adresse mail valide sous ce domaine ! Tous nos abonnés ont une adresse mail de la forme pseudo@aol.com, dont la partie locale (gauche) est composée de 3 à 16

caractères, lettres ou chiffres exclusivement.

Egalement, certains abonnés se trompent lorsqu'ils saisissent leur adresse mail. Si vous ne validez pas que l'adresse mail saisie est la bonne, la personne qui recevra vos newsletters va les considérer comme autant de courriers indésirables, et elle cliquera sur le bouton « Spam » car elle n'a jamais demandé à recevoir vos mails.

Soyez « transparent » dans la gestion des abonnements/désabonnements de vos liste de diffusion : prévenez l'abonné concerné à chaque fois, et permettez lui d'avoir un moyen simple de connaître la liste complète de toutes les newsletters sur lesquelles il est inscrit à un instant donné. Dans le cas contraire, il va bloquer tous vos envois via l'interface de contrôle du spam disponible dans le logiciel AOL s'il ne trouve pas un moyen simple et rapide de se désabonner…

4 Comment remplir le formulaire de demande d'inscription sur liste blanche ?

4.1 Identifier toutes les adresses IP de votre organisation qui expédient du mail directement vers AOL.

Ces machines doivent être sous votre administration directe. Si vos mailings transitent par un prestataire, c'est probablement lui qui devra remplir ce formulaire.

Pour chacune de ces adresses IP, vérifiez qu'elles disposent d'un champ PTR (DNS inverse) visible à l'extérieur de votre organisation. Il ne sert à rien de le vérifier en interne – souvent les zones DNS inverses sont mal configurées (absence de délégation par exemple) et ne sont pas propagées à l'extérieur. Mieux vaut donc utiliser un outil externe à votre organisation pour effectuer cette vérification, par exemple :

- l'outil de vérification du DNS inverse d'AOL : http://postmaster.info.aol.com/tools/rdns.html
- ou tout outil tiers, tel que http://remote.12dt.com/

Saisissez chacune de vos adresses IP et vérifiez l'existence d'un DNS inverse (champ PTR). Dans le cas contraire, ces adresses IP seront rejetées automatiquement par le formulaire de demande de mise sur liste blanche, car AOL n'accepte pas un mail en provenance *directe* d'une adresse IP qui n'a pas de champ PTR associé via le DNS inverse.

Note : le champ PTR doit pointer vers un nom de machine et de domaine existant – ayant lui-même un enregistrement DNS de type A pointant vers une adresse IP – et non vers une autre adresse IP, ou le domaine réservé in-addr.arpa.

4.2 Vérifier que votre domaine de messagerie est correctement configuré sur Internet

Nous vous suggérons l'utilisation de l'outil http://www.dnsreport.com/

Saisissez votre nom de domaine de messagerie, par exemple « pascher.com » et cliquez sur le bouton « DNS report ».

Toute case rouge « FAIL », en particulier dans les sections MAIL et MX, indique un problème grave qu'il faudra probablement corriger avant que vous ne puissiez envoyer du mail à AOL.

Exemple à l'heure où ces lignes sont écrites :
http://www.dnsreport.com/tools/dnsreport.ch?domain=pascher.com

> MX : FAIL : Missing reverse DNS entries for MX records
> ERROR: None of your mail server(s) seem to have reverse DNS (PTR) entries (I didn't get any responses for them). RFC1912 2.1 says you should have a reverse DNS for all your mail servers. It is strongly urged that you have them, as many mailservers will not accept mail from mailservers with no reverse DNS entry.

Vous pouvez également consulter l'outil de vérification voisin, intitulé « Mail Test ».

4.3 Choisir une adresse de rétroaction et vérifier qu'elle est joignable de l'extérieur de votre organisation

Une fois la boîte aux lettres « abuse-aol@pascher.com » créée, envoyez-y un mail depuis le webmail Yahoo!Mail, voila.fr ou laposte.net… et vérifiez que vous recevez bien ce mail à destination.

4.4 Renseigner le formulaire « Demande d'inscription sur liste blanche pour la messagerie AOL »

(cf. § 5 page 18 ci-après)

4.5 Soumettre votre demande

Il ne vous reste plus qu'à saisir ces informations sur le formulaire suivant : http://postmaster.info.aol.com/tools/whitelist_guides.html, après avoir accepté les conditions d'inscription sur liste blanche d'AOL. La plupart de ces critères sont traduits au § 1 page 2.

Un mail de validation de votre demande sera adressé à l'adresse de rétroaction que vous avez mentionnée. Il vous faudra pouvoir y accéder afin de valider la requête, afin qu'elle soit ensuite traitée par l'équipe des vaguemestres (Postmaster) AOL.

Note : il est également possible de demander la mise en place d'une boucle de rétroaction sur une plage d'adresses IP sans qu'elles soient mises en liste blanche – pour cela, remplissez le formulaire http://postmaster.info.aol.com/tools/fbl.html, *uniquement si vous ne souhaitez pas mettre ces adresses IP sur liste blanche.*

N'hésitez pas à contacter votre interlocuteur habituel chez AOL en cas de difficulté ou pour toute précision complémentaire, ou à défaut le service clientèle AOL au 0 892 02 03 04 (€ 0,34/min depuis un téléphone fixe), cf. http://www.aol.fr/societe_aol/contact.htm.

5 Demande d'inscription sur liste blanche pour la messagerie AOL

Note : les numéros de téléphone doivent être mentionnés avec le code indicatif du pays selon la notation internationale, par exemple : +33 1 23 45 67 89.

5.1 Contact principal

Prénom, Nom : _____
Numéro de Téléphone : +_____
Adresse mail : _____

Cette adresse mail recevra un mail de confirmation lorsque votre demande de mise sur liste blanche aura été traitée.

❑ Cocher si vous souhaitez recevoir sur cette adresse mail les « AOL Postmaster Alerts », en langue anglaise, vous informant des évolutions de notre politique de messagerie.

5.2 Contact secondaire (optionnel)

Prénom, Nom : _____
Numéro de Téléphone : +_____
Adresse mail : _____

❑ Cocher si vous souhaitez recevoir sur cette adresse mail une copie du mail de confirmation lorsque votre demande de mise sur liste blanche aura été traitée.

❑ Cocher si vous souhaitez recevoir sur cette adresse mail les « AOL Postmaster Alerts », en langue anglaise, vous informant des évolutions de notre politique de messagerie.

5.3 Informations sur votre organisation

Nom de la société : _____
Adresse physique : _____
Numéro de Téléphone : +_____
Nom de domaine Internet utilisé : _____
Adresse mail (optionnel) : _____

❑ Cocher si vous souhaitez recevoir sur cette adresse mail une copie du mail de confirmation lorsque votre demande de mise sur liste blanche aura été traitée.

❑ Cocher si vous souhaitez recevoir sur cette adresse mail les « AOL Postmaster Alerts », en langue anglaise, vous informant des évolutions de notre politique de messagerie.

5.4 Liste des adresses IP à mettre sur liste blanche

Vous pouvez lister les adresses IPv4 individuellement, ou indiquer une plage, telle que 12.34.56.[112-119] ou 12.34.56.* (cf. § 2 page 3)

_____ _____

_____ _____

_____ _____

_____ _____

❑ L'existence d'un champ PTR (DNS inverse) visible de l'Internet sur chacune de ces adresses IP a été vérifiée via les pages web http://remote.12dt.com/ ou http://postmaster.info.aol.com/tools/rdns.html (cf. § 4.1 page 16)

5.5 Adresse mail pour la boucle de rétroaction (« Feedback Loop »)

_____

Tout mail en provenance des adresses IP mentionnées ci-dessus, et signalé comme un spam par un abonné AOL sera retourné vers cette adresse mail. (cf. § 3.1 page 10)

Si vous souhaitez associer des adresses de rétroaction différentes sur chacune des adresses IP mentionnées, remplissez autant de fois ce formulaire que vous avez d'adresses mail de rétroaction différentes.

Une adresse IP ne peut être associée qu'à une seule adresse mail de rétroaction.

❑ L'existence et le fonctionnement normal de cette boîte aux lettres ont été vérifiés en y envoyant un mail de l'extérieur, qui y a été délivré correctement

❑ La bonne configuration du DNS pour le domaine de messagerie concerné a été vérifiée via l'outil http://www.dnsreport.com/ (cf. § 4.2 page 16)

❑ Vous avez lu, compris et approuvé les conditions d'inscription sur liste blanche d'AOL (§ 1 page 2)

Reportez vous au § 4.5 page 17 pour soumettre votre demande à AOL.

N'hésitez pas à contacter votre interlocuteur habituel chez AOL en cas de difficulté ou pour toute précision complémentaire, ou à défaut le service clientèle AOL au 0 892 02 03 04 (€ 0,34/min depuis un téléphone fixe), cf. http://www.aol.fr/societe_aol/contact.htm.