

**Groupe de travail sur le pourriel**

**Pratiques exemplaires recommandées  
pour les fournisseurs de services Internet  
et autres exploitants de réseaux**

**Sous-groupe sur la gestion des technologies et des réseaux**

**mai 2005**

## Table des matières

Préface .....	iii
Contexte .....	1
Groupe de travail sur le pourriel .....	1
Envergure du travail .....	2
Intention .....	2
Pratiques exemplaires recommandées et leurs fondements.....	3
Conclusion .....	8

## Préface

La publication, en mai 2004, du *Plan d'action anti-pourriel pour le Canada* et la mise sur pied du Groupe de travail canadien sur le pourriel ont enclenché un effort de concertation à l'échelle nationale, dans le but de résoudre un problème sérieux grandissant. Compte tenu de l'apport des solutions techniques à la résolution de ce problème, le Groupe de travail a mis sur pied le Sous-groupe sur la gestion des technologies et des réseaux, entre autres sous-groupes.

La création de ce sous-groupe représente le tout premier effort de collaboration et de concertation entre un grand nombre d'organisations, notamment la plupart des plus grands et plus petits fournisseurs de service Internet (FSI) de large bande et d'accès commuté, d'autres exploitants de réseaux, des grandes entreprises qui utilisent Internet, des concepteurs de logiciels, des intervenants anti-pourriel ainsi que le gouvernement. Le regroupement de ces organisations, ainsi que les discussions libres et franches qui se sont déroulées, sont en soi une réalisation remarquable.

Le Sous-groupe a élaboré une série de pratiques exemplaires techniques qu'il recommande dans le but de réduire le pourriel au Canada. Son mandat consiste à poursuivre les efforts et les progrès en cours depuis déjà quelques temps au Canada et à l'échelle internationale. Le Sous-groupe a toutefois fait avancer ce travail au point d'établir le tout premier vrai consensus national sur des mesures techniques à prendre pour lutter contre le pourriel. Ces pratiques exemplaires représentent pour le Canada un modèle à partager à l'échelle internationale dans la lutte mondiale contre le pourriel.

Bien que ces pratiques exemplaires soient de nature volontaire, le Sous-groupe est heureux de constater que bon nombre de FSI et d'exploitants de réseaux canadiens ont déjà commencé à mettre en pratique une partie ou la totalité de ces recommandations, au mieux des intérêts de leurs clients et de leurs réseaux. En outre, ces FSI exigent de plus en plus souvent que les autres FSI et exploitants de réseau mettent en œuvre ces pratiques exemplaires avant d'accepter d'acheminer les courriels. À ce titre, les pratiques exemplaires inciteront fortement les intervenants canadiens du secteur Internet à harmoniser leurs pratiques techniques anti-pourriel, dans un contexte technologique en perpétuelle évolution.

## **Contexte**

Internet n'est plus ce qu'il était il y a 10 ans, à savoir un phénomène propre aux consommateurs et aux entreprises. En 1995, on n'entendait pratiquement pas parler de courrier commercial non sollicité. Jusque là, les utilisateurs d'Internet, en majorité des utilisateurs techniques, respectaient ce médium qu'ils considéraient comme un outil facilitant la productivité et la communication. Peu d'utilisateurs abusaient des réseaux, et les politiques d'utilisation acceptable étaient en grande partie respectées.

Mais, 10 ans plus tard, nous sommes aux prises avec des problèmes de désinformation et de renseignements inexacts, sans compter le gaspillage de bits et d'octets. Environ 66 p. 100 des messages électroniques sont considérés comme du pourriel. La capacité des réseaux physiques et du personnel qui y travaille est mise à l'épreuve chaque jour dans la bataille apparemment interminable pour maintenir l'intégrité du service.

L'année dernière, un grand nombre de mesures anti-pourriel ont été prises sur de nombreux fronts. Et cela ne s'est pas limité aux FSI ni au secteur de la gestion de réseaux. Les associations de fournisseurs Internet de presque tous les pays s'attaquent au problème. En plus d'assumer leurs rôles traditionnels, des organisations comme l'Organisation des Nations Unies et l'Organisation de coopération et de développement économiques ont constitué des comités de lutte contre le pourriel.

Plus près de nous, les secteurs d'activités Internet des États-Unis et du Canada ont eu de nombreux entretiens sur la façon de combattre le pourriel. Aux États-Unis, l'Anti-Spam Technical Alliance (ASTA), organisation à laquelle appartiennent plusieurs importants fournisseurs de service Internet canadiens, a élaboré et publié une liste de pratiques exemplaires qu'elle recommande comme méthodes de gestion de réseaux susceptibles de servir la lutte anti-pourriel.

## **Groupe de travail sur le pourriel**

Au Canada, la ministre de l'Industrie a annoncé, le 11 mai 2004, la création du Groupe de travail sur le pourriel chargé de superviser la mise en place d'un vaste plan d'action visant à réduire le volume de courrier électronique commercial non sollicité.

Présidé par Industrie Canada, le Groupe de travail a adopté une approche consultative ouverte réunissant des experts et des intervenants clés qui représentent les FSI canadiens et autres exploitants de réseau, les entreprises qui utilisent le courrier électronique à des fins commerciales légitimes, des groupes de consommateurs et des membres du milieu juridique.

Pour exécuter sa tâche, le Groupe de travail canadien sur le pourriel a constitué des sous-groupes, dont le Sous-groupe sur la gestion des technologies et des réseaux. Celui-ci est composé des représentants de la plupart des FSI de large bande et d'accès commuté ainsi que d'autres exploitants de réseaux (qui comprennent, selon le Sous-groupe, les grands utilisateurs d'Internet

comme les universités et les ministères gouvernementaux), des concepteurs de logiciels et des intervenants anti-pourriel.

Le Sous-groupe a examiné le travail effectué par les FSI officiels et non officiels ainsi que par les groupes d'exploitants de réseaux, et a dressé une liste de pratiques exemplaires. Les FSI et les autres exploitants de réseaux pourront appliquer ces pratiques pour freiner l'utilisation abusive de leurs réseaux, tant à l'interne par leurs clients qu'à l'externe par les polluposteurs qui inondent les clients de courriels.

## **Envergure du travail**

En août 2004, le Sous-groupe sur la gestion des technologies et des réseaux a entrepris l'élaboration d'un certain nombre de pratiques exemplaires techniques qui contribueraient à réduire le volume de pourriel. Son mandat s'inscrit dans la foulée des efforts et des progrès accomplis depuis quelque temps au Canada et à l'échelle internationale, dont les travaux de l'ASTA et du Messaging Anti-Abuse Working Group, ainsi que ceux de plusieurs associations du secteur d'activités. Un certain nombre de FSI, d'autres exploitants de réseaux et des groupes techniques collaborent depuis de nombreux mois afin de partager leurs pratiques exemplaires pour réduire le pourriel.

Le Sous-groupe n'a pas essayé de refaire le travail déjà accompli, préférant réunir les divers groupes du secteur d'activités pour mettre en commun les résultats du travail en cours et encourager l'adoption des pratiques exemplaires par les FSI, les autres exploitants de réseaux et les grandes entreprises qui utilisent Internet.

Le Sous-groupe tient à souligner que l'adoption répandue de ces pratiques ne constituera pas à elle seule une solution exhaustive au problème du pourriel.

Toutefois, les recommandations font partie d'une stratégie multidirectionnelle plus vaste visant à le régler.

## **Intention**

Les pratiques exemplaires en matière de lutte anti-pourriel recommandées au secteur par le Sous-groupe sont volontaires. L'échéancier de leur mise en œuvre peut varier selon la configuration technique particulière du réseau du fournisseur de service ou de l'exploitant ainsi que des besoins et de la situation de celui-ci. Dans certains cas, des solutions de rechange peuvent permettre d'atteindre les mêmes objectifs que ceux des recommandations. Le choix des solutions reste à la discrétion du fournisseur de service ou de l'exploitant de réseau.

Le Sous-groupe appuie tous les efforts déployés pour combattre le pourriel. La souplesse inhérente à la mise en œuvre de ces pratiques exemplaires est l'élément essentiel à une adoption généralisée et efficace par les fournisseurs de service de toutes tailles. Vu la nature technique de ces recommandations et l'évolution rapide de la technologie, le Sous-groupe est persuadé qu'il faut éviter de codifier ces pratiques exemplaires sous forme d'exigences obligatoires.

## Pratiques exemplaires recommandées et leurs fondements

Pratiques exemplaires recommandées pour les fournisseurs canadiens de service Internet et les autres exploitants de réseaux pour lutter contre le pourriel ainsi que les fondements pour chacune des recommandations.

- 1. Tous les registraires et hôtes canadiens de noms de domaine devraient publier des renseignements sur Sender Policy Framework (SPF) dans les fichiers de leur zone respective de serveur de nom de domaine le plus tôt possible.**

Le but de l'authentification de l'expéditeur de courriel est de réduire la mystification du nom de domaine dans le courriel, réduisant par le fait même la fréquence des tentatives de pourriel et d'hameçonnage.

Le groupe Internet Engineering Task Force (IETF) continue d'évaluer les méthodes d'authentification de l'expéditeur de courriel. À l'heure actuelle, la proposition relative au SPF classique (SPFv1) est le modèle de conception d'authentification de l'expéditeur de courriel le plus techniquement avancé et le plus largement déployé.

Cette recommandation n'empêche pas l'utilisation d'autres propositions qui authentifieront des courriels (par exemple Sender-ID, Domain Keys, SPF, courrier Internet identifié, etc.). Le secteur industriel continuera d'élaborer des normes à cet égard.

- 2. Les FSI et autres exploitants de réseaux devraient limiter, par défaut, l'utilisation du port 25 par les utilisateurs finaux. Au besoin, la capacité d'envoyer ou de recevoir du courriel au moyen du port 25 devrait être limitée aux ordinateurs hôtes du réseau du fournisseur. L'utilisation du port 25 par les utilisateurs finaux devrait être permise au besoin ou être conforme à l'entente entre le fournisseur et l'utilisateur final et aux modalités de service.**

Selon la majorité des FSI et autres exploitants de réseaux, il n'y a aucune raison pratique pour que des utilisateurs clients aient des serveurs de courrier utilisant des intervalles d'adresses Protocole Internet (IP) commutées/dynamiques.

Il y a plusieurs façons d'éliminer ce problème. Les FSI et autres exploitants de réseaux peuvent se servir de leur propre outil de gestion de réseau pour bloquer la sortie de messages par le port 25.

D'après leur expérience, les membres de ce sous-groupe savent que le blocage du port 25 n'affecte qu'un très petit nombre d'utilisateurs et que ces derniers peuvent normalement s'accommoder de façons différentes.

Les avantages de ce blocage peuvent être énormes. Ainsi, des FSI ont constaté une diminution de 95 p. 100 des émissions de virus, de 98 p. 100 des rapports d'abus et une réduction des infections

internes de virus et des appareils infectés servant à envoyer des pourriels, ajoutant à cela la réduction des coûts reliés à la gestion des abus de réseau.

**3. Les FSI et autres exploitants de réseaux devraient bloquer les pièces jointes aux courriels dont les extensions sont connues pour transporter des virus ou filtrer les pièces jointes en fonction des propriétés du contenu.**

Un grand nombre de virus et de vers sont acheminés par les pièces jointes. Le blocage des courriels contenant des pièces jointes problématiques aurait peu de répercussions sur les utilisateurs. Les extensions de fichiers les plus susceptibles de porter des virus sont : .pif, .scr, .exe et .vbs.

Bon nombre de FSI et autres exploitants de réseaux devraient filtrer les pièces jointes en fonction des propriétés (c'est-à-dire des infections) par opposition aux noms d'extension. C'est une question de disponibilité des ressources. Étant donné que certains utilisateurs commerciaux et techniques pourraient avoir des motifs valables d'envoyer des fichiers comportant des extensions .exe ou .vbs, il se peut que le filtrage du contenu soit plus efficace que celui des noms d'extension.

**4. Les FSI et autres exploitants de réseaux devraient surveiller étroitement le volume de courriels entrants et sortants afin de repérer les activités inhabituelles dans le réseau et leur source, et prendre des mesures en conséquence.**

La surveillance et la limitation éventuelle de la quantité de courriels qu'un utilisateur donné pourrait envoyer décourageraient les polluposteurs d'utiliser les réseaux des fournisseurs comme point d'envoi. Ces mesures serviraient également de premier indice d'infection de l'appareil d'un utilisateur.

À l'heure actuelle, certains fournisseurs limitent la quantité de courriels expédiés de façon restreinte. Les techniques varient en fonction du serveur de courriel utilisé.

**5. Les FSI et autres exploitants de réseaux devraient établir et maintenir de façon continue des processus efficaces et rapides pour la gestion et l'élimination des éléments de réseau infectés constituant une source de pourriel.**

Au moyen de virus, de programmes-vers et de logiciels pernicious, les pirates informatiques et polluposteurs ont délibérément installé des millions de relais ouverts de type « porte arrière » et de passerelles de procuration sur les ordinateurs personnels d'utilisateurs peu méfiants. Les polluposteurs utilisent ce réseau d'appareils infectés pour générer des milliards de courriels non sollicités. En plus, les pirates ont utilisé ce réseau d'appareils informatiques à des fins d'exécution de Refus de service distribué sur les sites Web, d'inscription de comptes frauduleux et de préparation à des activités anonymes futures de piratage informatique.

Diverses méthodes peuvent être utilisées pour traiter les appareils infectés, notamment la suspension de comptes-clients, l'isolement ou la mise en quarantaine de ces appareils à l'extérieur du réseau.

**6. Les FSI et autres exploitants de réseaux devraient établir des processus interentreprises pertinents afin de réagir aux rapports d'incidents des autres exploitants de réseaux.**

Le Sous-groupe sur la gestion des technologies et des réseaux dresse présentement une liste de personnes-ressources des FSI et autres exploitants. Il serait utile de pouvoir s'attendre à une réponse commune lorsqu'on signale un incident d'abus de réseau important à un autre opérateur de réseau. Le processus de recours hiérarchique au sein des entreprises demeurerait un processus privé, mais une heure de reprise prévue commune devrait figurer dans les communications initiales interentreprises.

**7. Les FSI et autres exploitants de réseaux ainsi que les fournisseurs de service de courrier électronique devraient communiquer leurs politiques et procédures en matière de sécurité à leurs abonnés.**

Ce point vise à faire en sorte que les abonnés soient bien au courant des politiques et procédures de sécurité de leur FSI, des autres exploitants de réseaux et des entreprises fournissant des services de courriel. Ce point aura une importance particulière pour les recommandations 2, 3 et 5.

Un autre sous-groupe du Groupe de travail, le Sous-groupe sur l'éducation et la sensibilisation du public, a élaboré une campagne multilatérale d'information et de sensibilisation du public afin de faire connaître, particulièrement aux utilisateurs finaux canadiens, les méthodes à prendre pour limiter la quantité de courriels commerciaux non sollicités reçus.

**8. Les FSI et autres exploitants de réseaux devraient adopter la validation du courriel sur tous leurs serveurs Simple Mail Transfer Protocol (SMTP) (c'est-à-dire entrée, sortie, relais).**

La validation du courriel ferait en sorte que seuls les clients « authentifiés » seraient autorisés à envoyer du courrier sur le serveur. Par exemple, l'authentification SMTP est une amélioration qui permet aux serveurs SMTP de vérifier l'identité des clients du système de courriel. Le protocole demande le nom d'utilisateur et le mot de passe de l'expéditeur du message et les valide en les comparant aux données des clients préinscrits. Cette procédure peut être utilisée pour réduire les pourriels, car ceux-ci ne proviennent généralement pas d'utilisateurs inscrits sur la liste d'autorisation SMTP.

**9. Les avis de non-remise (NDN) ne devraient être envoyés que dans les cas de messages électroniques légitimes.**

Les gestionnaires d'Agents de transfert des messages (ATM) et les fabricants de filtres anti-pourriel ont maintenant accepté cette pratique. Quand un message est envoyé à un compte d'utilisateur non existant, l'ATM répond que l'utilisateur n'existe pas. Cela peut causer des problèmes lorsqu'un polluposteur contrefait un grand nombre d'adresses d'un domaine, car le serveur émet une réponse de non-remise pour chaque adresse non existante. Le logiciel ATM

devrait être configuré de manière à ne pas envoyer de messages de non-remise dans les cas d'adresses contrefaites.

La cessation généralisée des NDN pourrait causer des problèmes aux utilisateurs qui ont mal tapé l'adresse et présument que le message est parvenu au destinataire.

- 10. Les FSI et autres exploitants de réseaux devraient veiller à ce que tous les noms de domaine, les fichiers de systèmes de noms de domaine (DNS) et les fichiers d'enregistrement d'adresse IP applicables (WHOIS/SWIP/RWHOIS) soient maintenus à jour à l'aide de renseignements corrects, complets et courants. Ces renseignements devraient comprendre les points de contact responsables de résoudre les questions d'abus et inclure, sans toutefois s'y limiter, les adresses postales, les numéros de téléphone et les adresses électroniques.**

L'identification de points de contact pour les FSI et les exploitants de réseaux est essentielle à la gestion des abus des systèmes de communication électronique. Tous les messages électroniques comprennent des renseignements tels que les noms Internet DNS, les adresses IP et autres données concernant la source, la transmission et la destination du message. Les FSI et autres exploitants de réseaux responsables des sources des messages électroniques devraient être facilement et exactement identifiables. Les noms de domaine qualifiés (par exemple nomInternet.nomdedomaine.ca), les noms de domaine et les adresses IP devraient être enregistrés et maintenus à l'aide de renseignements permettant cette identification.

Les exploitants de réseaux devraient également veiller à ce que les fichiers de nom de domaine, les fichiers DNS avant et inversés et les fichiers de la base de données WHOIS, du projet partagé WHOIS (c'est-à-dire SWIP) ou de référence (c'est-à-dire RWHOIS) soient adéquatement maintenus à l'aide de données exactes, complètes et courantes. Par exemple, les fichiers WHOIS de l'American Registry for Internet Numbers devraient inclure OrgAbuseHandle, y compris les coordonnées des responsables de la gestion des abus provenant de ce réseau. Les FSI et les exploitants de réseaux sont responsables du maintien de données d'enregistrement, de fichiers DNS et autres renseignements signalétiques conformes aux documents Request for Comments (RFC) pertinents, notamment le RFC 2142 — Mailbox Names for Common Services, Roles and Functions.

- 11. Les FSI et autres exploitants de réseaux devraient veiller à ce que leurs adresses routables et visibles sur Internet aient des fichiers DNS avant et inversés appropriés et mis à jour ainsi que des entrées WHOIS et SWIP. Tous les exploitants de réseau local d'entreprise (RLE) devraient se conformer au document Request for Comments (RFC) 1918 — « Address Allocation for Private Internets ». Les RLE, plus particulièrement, ne devraient pas utiliser l'espace IP enregistré globalement à quelqu'un d'autre ou l'espace IP non enregistré à quelqu'un, à titre d'espace IP privé.**

Le pourriel et le maliciel comportent souvent un en-tête de message contrefait. Il importe donc de veiller à ce que toutes les adresses routables et visibles sur Internet aient des fichiers DNS avant et inversés appropriés et mis à jour ainsi que des entrées WHOIS et SWIP, afin de pouvoir repérer les sources des messages électroniques et autres modes de communication en ligne.

L'identification de la source permet d'avertir les FSI ou les autres exploitants de réseaux responsables afin qu'ils puissent prendre des mesures appropriées pour éliminer le pourriel ou les autres problèmes associés au protocole. Les adresses IP enregistrées auprès d'un autre organisme ne devraient pas être utilisées au sein des réseaux privés, car elles entravent considérablement l'identification des FSI et autres exploitants de réseaux responsables d'un message électronique. Les destinataires peuvent utiliser les noms Internet DNS à des fins de politique d'accès, mais les noms doivent être soigneusement choisis, afin d'éviter que des filtres trop vastes ne bloquent les messages électroniques légitimes. Prière de consulter la recommandation 10 concernant le maintien des fichiers à l'aide de renseignements exacts, complets et courants.

Pour faciliter l'identification des sources de messages électroniques, on suggère également que les serveurs aient des noms Internet DNS qui différencient clairement ces serveurs des adresses des postes de travail des consommateurs ou des entreprises. Les noms Internet des fichiers DNS avant (traduction de l'adresse IP en nom Internet) et inversés (traduction du nom Internet en adresse IP) devraient correspondre. Les clients des FSI autorisés à exploiter des serveurs de courriel ou autres serveurs profiteront de cela, car ils pourront exploiter des systèmes DNS avant et inversés au sein de leur domaine, distinguant ainsi les hôtes des hôtes résidentiels ou des hôtes interdits. Les destinataires de messages électroniques peuvent ainsi établir des systèmes qui différencient les serveurs de courriel légitimes des hôtes susceptibles d'être des sources de pourriel.

Les adresses IP résidentielles, dynamiques ou interdites devraient également prévoir une convention d'adressage par domaines avant et inversé claire et uniforme. Par exemple, les politiques de contrôle d'accès des destinataires qui distinguent les sources de courriel fiables des sources non fiables sont plus faciles à établir lorsque les conventions d'adressage incluent le propriétaire du domaine, la classe de service, l'affectation statique ou dynamique et d'autres identificateurs, notamment une identification axée sur une fourchette d'adresses IP. Ces conventions peuvent également empêcher que les clients des FSI autorisés à exploiter des serveurs de courriel soient bloqués parce qu'il est impossible de les distinguer des sources de messages électroniques illégitimes. Les conventions d'adressage comportant un schéma « de plus fort poids à droite » simplifient les filtres et font en sorte que les politiques de contrôle d'accès n'affectent pas les sources de messages électroniques légitimes. Par exemple, une telle convention d'adressage pour l'adresse IP résidentielle, dynamique « 1.2.3.4 » au FSI Example.ca serait « 4-3-2-1.dyn.res.example.ca. ». Un exemple de convention d'adressage pour l'adresse IP commerciale, statique « 1.2.3.4 » au FSI Example.ca serait « 4-3-2-1.static.bus.example.ca. ». Un exemple de convention d'adressage pour un serveur de courriel utilisé par Smallbizcustomer.ca serait « mail.smallbizcustomer.ca. ».

**12. Les FSI et autres exploitants de réseaux devraient interdire l'envoi de courriels renfermant des en-têtes frauduleux ou contrefaits. L'en-tête de message devrait être exact et conforme aux documents RFC pertinents, notamment le RFC 822 et le RFC 2822, et les domaines de référence et les adresses IP devraient comporter des données d'enregistrement exactes et à jour.**

Un en-tête de message exact permet aux FSI et aux autres exploitants de réseaux de repérer les sources de pourriel et de maliciel électronique au sein de leur réseau FSI. Prière de consulter la

recommandation 10 concernant le maintien des fichiers à l'aide de renseignements exacts, complets et courants.

Bien que les réseaux internes utilisent souvent des adresses IP privées (conformément au document RFC 1918 — Address Allocation for Private Internets) qui ne sont pas routables ni identifiables extérieurement, les fournisseurs de service de courriel devraient s'assurer que les sources de messages électroniques sont correctement identifiables à des fins d'application des politiques et des lois.

## **Conclusion**

Le pourriel est un problème global et multiple exigeant l'adoption de mesures concertées à plusieurs niveaux afin d'arriver à des résultats réels et mesurables. La mise en œuvre des recommandations présentées dans ce document peut aider à réduire un grand nombre des pires formes de pourriel, de contrefaçon et d'usurpation d'identité que l'on retrouve dans les courriels. À défaut de mettre fin au pourriel, ces mesures amélioreront grandement la capacité de la communauté Internet d'en repérer la source et de tenir les expéditeurs responsables de leurs gestes. Ces mesures devraient également servir de base aux solutions futures.