

@@@
FREINONS LE
POURRIEL



@@@
CRÉER UN
INTERNET
PLUS FORT ET
PLUS SÉCURITAIRE

On peut obtenir cette publication sur supports multiples, sur demande. Communiquer avec le Centre de diffusion de l'information dont les coordonnées suivent.

Pour obtenir des exemplaires supplémentaires de cette publication, s'adresser également au :

Centre de diffusion de l'information
Direction générale des communications et du marketing
Industrie Canada
Bureau 268D, tour Ouest
235, rue Queen
Ottawa (Ontario) K1A 0H5

Téléphone : (613) 947-7466
Télécopieur : (613) 954-6436
Courriel : publications@ic.gc.ca

Cette publication est également offerte par voie électronique sur le Web (www.e-com.ic.gc.ca).

Autorisation de reproduction

À moins d'indication contraire, l'information contenue dans cette publication peut être reproduite, en tout ou en partie et par quelque moyen que ce soit, sans frais et sans autre permission d'Industrie Canada, pourvu qu'une diligence raisonnable soit exercée afin d'assurer l'exactitude de l'information reproduite, qu'Industrie Canada soit mentionné comme organisme source et que la reproduction ne soit présentée ni comme une version officielle ni comme une copie ayant été faite en collaboration avec Industrie Canada ou avec son consentement.

Les opinions et déclarations contenues dans cette publication n'engagent que leur auteur et ne reflètent pas nécessairement la politique d'Industrie Canada ou celle du gouvernement du Canada.

Pour obtenir l'autorisation de reproduire l'information contenue dans cette publication à des fins commerciales, faire parvenir un courriel à copyright.droitdauteur@tpsgc.gc.ca.

N.B. Dans cette publication, la forme masculine désigne tant les femmes que les hommes.

N° de catalogue lu64-24/2005F-PDF
ISBN 0-662-79853-8
514279B



Couverture : 10 %
Pages intérieures : 10 %



Mai 2005

L'honorable David L. Emerson, C. P., député
Ministre de l'Industrie
Édifce C. D. Howe
tour Ouest, 5^e étage
235, rue Queen
Ottawa (Ontario) K1A 0H5

Monsieur le Ministre,

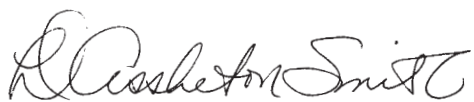
Le 11 mai 2004, le gouvernement du Canada a annoncé le lancement du *Plan d'action anti-pourriel pour le Canada* et a mis sur pied un groupe de travail mixte des secteurs public et privé pour coordonner la mise en œuvre de ce plan. Nous disposions d'un an pour ce faire. Après cette période, nous devons faire rapport des progrès accomplis et proposer toute autre mesure qui pourrait s'avérer nécessaire.

Nous sommes heureux de vous informer que nous avons fait d'importants progrès dans la lutte contre le pourriel, progrès rendus possibles grâce à l'assistance de nombreuses personnes représentant tous les groupes d'intervenants qui ont contribué à nos travaux.

Nous comptions 10 membres lors de notre première réunion de comité, dans un bureau d'Ottawa, mais nous avons grandi rapidement pour former un réseau à l'échelle du pays et même au-delà. Nous avons accompli la majeure partie de notre travail en ligne, par courrier électronique. L'expérience nous a fait comprendre à quel point Internet peut transformer la façon dont nous faisons les choses et nous a convaincus de l'importance de mettre un frein au pourriel et aux autres menaces à l'utilisation d'Internet.

Notre mandat est terminé, mais il reste encore beaucoup à faire. En effet, notre expérience nous a appris que le pourriel n'est pas la seule menace à la sécurité de la plate-forme de communication et de commerce qu'est le réseau Internet. Nous avons donc recommandé une série de mesures qui contribueront à lutter contre le pourriel et les problèmes qui s'y rattachent, au Canada. Ces mesures mettront notre pays à l'avant-garde de la lutte contre un problème croissant et mondial. Nous sommes persuadés que le Canada ne doit viser rien de moins, étant donné le rôle de chef de file qu'il occupe depuis longtemps dans le domaine des communications.

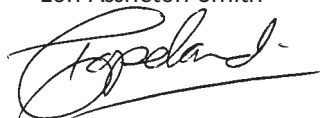
Nous vous prions d'agréer, Monsieur le Ministre, l'assurance de notre très haute considération.



Lori Assheton-Smith



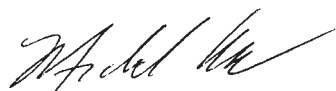
Michael Binder (président)



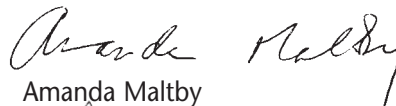
Tom Copeland



Bernard Courtois



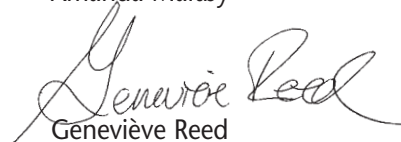
Michael Geist



Amanda Maltby



Suzanne Morin



Geneviève Reed



Neil Schwartzman



Roger Tassé

TABLE DES MATIÈRES

Lettre de présentation	iii
Sommaire	1
Recommandations	3
1. Freiner le pourriel	7
2. Clarifier les règles	11
3. Gérer les réseaux pour contrer le pourriel	18
4. Rétablir la confiance à l'égard du courriel	22
5. Sensibilisation du public	26
6. Résoudre un problème mondial	29
7. Coordonner l'action future	32
Appendices	
A. Membres des sous-groupes du Groupe de travail et secrétariat	35
B. Pratiques exemplaires recommandées pour les fournisseurs de service Internet et les autres exploitants de réseaux	39
C. Pratiques exemplaires recommandées pour le marketing par courriel ..	45
D. Trois conseils importants pour lutter contre le pourriel	52
E. Rapports complémentaires et documents de travail	55
Glossaire	57

SOMMAIRE

QU'EST-CE QUE LE POURRIEL ET POURQUOI POSE-T-IL UN PROBLÈME?

Le *Plan d'action anti-pourriel pour le Canada* de mai 2004 définissait le pourriel comme étant « des messages électroniques commerciaux non sollicités ». Utilisant cette définition, le cabinet MessageLabs a estimé que le pourriel représentait 80 p. 100 du courriel global à la fin de 2004, comparativement à environ 10 p. 100 en 2000.

Le pourriel est plus qu'un ennui croissant. Il s'agit d'une question d'intérêt public qui pose aux gouvernements, aux fournisseurs de service Internet (FSI), aux autres exploitants de réseaux, aux expéditeurs de courriels commerciaux et aux consommateurs, le défi de collaborer d'une façon nouvelle à la solution d'un problème qui menace les intérêts de tous.

Sur une grande échelle, le pourriel menace directement la viabilité d'Internet comme moyen efficace de communication. À cause de cela, il est aussi une menace directe à la croissance de la prospérité économique, à l'efficacité des services publics et au développement d'une cyberéconomie qui englobe tous les Canadiens.

Sur une petite échelle, le pourriel agace et offense les internautes. Il constitue également un véhicule pour des activités qui sont clairement illicites ou devraient l'être. Celles-ci comprennent :

- les activités nuisibles qui endommagent les ordinateurs, les réseaux ou les données, ou qui utilisent des biens personnels à des fins non autorisées (par exemple virus, vers, chevaux de Troie, attaques par déni de service, réseaux zombies);

- les pratiques commerciales trompeuses et frauduleuses, y compris les versions électroniques de fraudes postales classiques (par exemple le compte bancaire du Nigeria ou arnaque 419 et les sites Web qui personnalisent des entreprises légitimes);
- les courriels hameçons visant l'usurpation d'identité ou le vol de sommes d'argent;
- les atteintes à la vie privée (par exemple collecte d'adresses électroniques, logiciels espions).

Qui le pourriel affecte-t-il?

Les menaces mentionnées minent la confiance des consommateurs à l'égard du cybercommerce et entravent les transactions électroniques entre les citoyens et leurs gouvernements. Le pourriel occasionne également des coûts importants pour l'ensemble de l'économie.

Ces coûts frappent un vaste éventail d'acteurs, notamment :

- les FSI et autres exploitants de réseaux (par exemple les grandes entreprises, les universités et les ministères gouvernementaux), qui doivent affecter des ressources techniques, financières et humaines au déploiement de technologies anti-pourriel au lieu d'investir dans des services nouveaux ou améliorés, en plus de consacrer des ressources au traitement des plaintes des clients;

- les expéditeurs de courriels commerciaux légitimes et autres utilisateurs des services de courriel, dont les messages sont filtrés par les technologies anti-pourriel avant d'atteindre leurs destinataires;
- les organismes des secteurs privé et public, dont les employés perdent du temps à s'occuper du pourriel envoyé à leur adresse de courriel professionnelle.

Au bout du compte, ces coûts frappent directement ou indirectement les consommateurs et utilisateurs finaux d'Internet. En effet, la lutte anti-pourriel occasionne des frais d'achat de logiciels de protection, empêche les améliorations de service et fait augmenter le prix des produits achetés en direct.

Que devons-nous faire pour lutter contre le pourriel?

Pour lutter contre le pourriel, le Canada doit adopter une stratégie multiple qui engage tous les intervenants. Le *Plan d'action anti-pourriel pour le Canada* de mai 2004 fut un bon départ. Il a déterminé les outils principaux pour freiner le pourriel. Ce sont :

- l'application vigoureuse des lois existantes qui interdisent le pollupostage et l'adoption d'une nouvelle loi pour combler les lacunes des lois actuelles;
- des amendes et mécanismes d'application de la loi plus puissants pour décourager les polluposteurs plus efficacement;
- des normes industrielles et des pratiques recommandées pour aider les FSI, les autres exploitants de réseaux et les entreprises de marketing par courriel dans la conduite légitime de leurs activités;
- l'éducation et la sensibilisation du public;
- la coopération internationale dans la lutte contre le pourriel.

L'année passée, le Groupe de travail sur le pourriel a dirigé l'élaboration d'une approche canadienne unique à l'égard de la lutte anti-pourriel, avec l'aide de centaines de personnes représentant différents groupes d'intervenants. Le présent rapport décrit ses activités ainsi que le travail qui reste à faire. Au cours de ses travaux, le Groupe de travail a retenu plusieurs leçons d'importance dans la lutte anti-pourriel, non seulement au Canada mais également dans le monde.

L'importance d'une démarche multiple, regroupant divers intervenants

La leçon la plus importante est la suivante : une démarche anti-pourriel multiple, regroupant divers intervenants, fonctionne, et c'est sans doute la seule qui sera efficace à long terme.

Certains pays ont choisi de combattre le pourriel principalement à l'aide de lois et de règlements. Les travaux du Groupe de travail ont confirmé qu'il fallait mettre en œuvre des lois claires et des sanctions sévères et les appliquer rigoureusement pour lutter de façon efficace contre le pourriel. Ils ont également démontré l'importance de combler les lacunes de la législation canadienne actuelle et de corriger les faiblesses du système d'application de la loi. Mais, malgré leur importance, les démarches juridiques à elles seules ne garantiront pas la victoire.

Des pratiques commerciales solides, la sensibilisation des consommateurs, l'éducation du public et la collaboration internationale sont des composantes tout aussi importantes de l'approche de type « boîte à outils » pour combattre le pourriel. Pour obtenir les meilleurs résultats possibles, on doit élaborer et utiliser ces outils d'une façon coordonnée, au sein d'un cadre juridique solide renforcé par un système d'application efficace.

L'importance de la communication et de la coopération entre intervenants

La deuxième leçon retenue est la suivante : les différents groupes d'intervenants concernés par la lutte anti-pourriel doivent communiquer et travailler ensemble.

Lorsqu'il a entamé ses travaux, le Groupe de travail a rapidement découvert que la structure du groupe des intervenants était cloisonnée et qu'il se devait de combler l'écart pouvant exister normalement entre le gouvernement, le secteur privé et les défenseurs de l'intérêt public, écart dû aux intérêts et aux points de vue divergents.

Les travaux pratiques effectués en commun se sont avérés un moyen très efficace d'éliminer ces obstacles. En plus d'améliorer les communications, la démarche multilatérale adoptée par le Groupe de travail a produit des résultats très significatifs

en ce qui concerne la création de précédents liés à l'établissement de mesures d'application de la loi anti-pourriel, de pratiques exemplaires à l'avant-garde mondiale pour le secteur industriel ainsi que de campagnes de sensibilisation et d'éducation du public fort efficaces.

L'obtention de résultats pratiques dans la lutte anti-pourriel exigera une coordination continue des travaux des intervenants au moyen de bonnes communications.

L'importance d'une stratégie globale dans la lutte contre les menaces à Internet

La troisième leçon retenue est la suivante : la lutte anti-pourriel n'est qu'un élément d'un combat beaucoup plus vaste qui s'engage contre les dangers nouveaux et potentiellement plus sérieux qui menacent Internet en matière de communications et de commerce.

Lorsque le Canada a commencé l'élaboration du *Plan d'action anti-pourriel pour le Canada*, il y a deux ou trois ans, le pourriel était considéré comme un ennui qui occasionnait des pertes de temps aux consommateurs et aux entreprises. C'était encore l'opinion générale qui existait au moment où le Groupe de travail a entamé ses travaux.

Durant l'année passée, le Groupe de travail s'est rendu compte que le pourriel était devenu plus qu'un ennui mineur. Le pourriel est une source croissante d'activités visant à tromper, à enfreindre la vie privée, à faire un usage non autorisé du matériel des consommateurs et des entreprises, à endommager les ordinateurs et les réseaux, à commettre de la fraude et à voler des renseignements personnels.

Pendant cette même période, le pourriel et les autres genres de menaces ont commencé à se propager du courriel à la messagerie instantanée et aux communications sans fil.

C'est pourquoi, en préparant le rapport, le Groupe de travail a tenté d'aller au-delà du problème familier du courriel commercial non sollicité et d'effectuer une analyse exhaustive et stratégique des défis que le Canada devra relever pour venir à bout du pourriel et des autres menaces à Internet.

Recommandations

Pour lutter contre le pourriel, le Groupe de travail recommande les démarches suivantes :

Leadership et partenariat

1. Le gouvernement fédéral, en association avec d'autres intervenants, devrait continuer à préconiser une stratégie à facettes multiples pour mettre fin au pourriel.

Législation, réglementation et application de la loi

2. Le gouvernement fédéral devrait adopter un ensemble de règlements judiciaires précis, visant à interdire le pourriel et les nouvelles menaces à la sécurité du réseau Internet (par exemple réseaux d'ordinateurs zombies, logiciels espions et logiciels de surveillance des entrées au clavier de l'utilisateur) et, pour ce faire, adopter une nouvelle loi et modifier les lois actuelles au besoin.

3. À cette fin, les activités et pratiques de multi-postage abusif suivantes devraient constituer des infractions au titre d'une loi anti-pourriel spécifique (ces dispositions peuvent également être énoncées, en totalité ou en partie, dans les lois actuelles) :

- le défaut de se conformer à des procédures d'inclusion pour l'envoi de courriels non sollicités;
- l'utilisation d'en-têtes ou de lignes de mention objet faux ou trompeurs (c'est-à-dire transmission de faux renseignements) destinés à déguiser l'origine, le but ou le contenu d'un courriel, que l'objectif soit de tromper le destinataire ou de contourner les filtres techniques;
- la construction d'adresses URL et de sites Web faux ou trompeurs dans le but de recueillir des renseignements personnels par escroquerie ou à des fins criminelles (ou pour commettre les autres infractions énumérées);
- la collecte d'adresses de courriel sans consentement, ainsi que la diffusion, l'utilisation ou l'acquisition de ces listes;
- les attaques de dictionnaire.

4. Les sanctions et recours suivants devraient s'appliquer à ces nouvelles infractions :

- les nouvelles infractions établies devraient être d'ordre civil et de responsabilité stricte, et prévoir une responsabilité criminelle pour les infractions plus flagrantes ou répétées. Il devrait y avoir des sanctions statutaires importantes pour toutes les infractions énumérées à la recommandation 3;
- un droit privé d'action approprié devrait être offert aux personnes, individus et entreprises. Des dommages-intérêts statutaires significatifs devraient être prévus pour les personnes qui entament une poursuite civile;
- les entreprises dont les produits ou services sont promus par le truchement du pourriel devraient aussi être tenues responsables du pourriel. La responsabilité devrait également incomber aux tiers qui bénéficient du pourriel.

5. En ce qui concerne l'application et l'administration de la nouvelle loi :

- l'administration de la nouvelle loi anti-pourriel devrait être du ressort du ministre de l'Industrie, et l'on devrait établir un centre de responsabilité pour la surveillance et la coordination des politiques, l'éducation et la sensibilisation du public, et l'octroi d'un soutien aux organismes d'application;
- l'application des nouvelles dispositions législatives anti-pourriel devrait relever des organismes existants.

6. Le gouvernement fédéral devrait accorder la priorité à l'application des mesures anti-pourriel en renforçant le soutien et les ressources destinés aux organismes responsables de l'application des lois anti-pourriel nouvelles et actuelles.

7. Le gouvernement fédéral, de concert avec les provinces et les territoires, devrait conclure et mettre en œuvre des accords de coopération en matière d'application des lois avec d'autres pays. Toutes les dispositions législatives actuelles devraient être examinées et modifiées au besoin pour permettre la mise en œuvre d'enquêtes coopératives et de mesures de mise en application homogènes, à l'échelle internationale.

Pratiques exemplaires pour les fournisseurs de service Internet et les autres exploitants de réseaux

8. Les FSI et autres exploitants de réseaux devraient mettre en œuvre les pratiques exemplaires recommandées par le Groupe de travail sur le pourriel.

9. Les FSI et autres exploitants de réseaux, en coopération avec l'organisme de coordination établi par le ministre de l'Industrie (mentionné à la recommandation 5), devraient mesurer de façon continue l'ampleur du problème du pourriel au Canada et évaluer les répercussions des pratiques recommandées. Ils devraient continuer à cerner les questions qui pourraient mériter davantage d'examen et mener à la formulation de recommandations additionnelles.

10. Afin de faciliter de façon continue la surveillance des tendances du pourriel et l'élaboration de mesures et de techniques anti-pourriel, le gouvernement devrait jouer un rôle de leadership en créant une base de données canadienne sur les pourriels (« congélateur à pourriels »).

11. Les FSI et autres exploitants de réseaux devraient adopter et appliquer des Politiques d'utilisation acceptable interdisant clairement le pollupostage sur leurs réseaux.

Pratiques exemplaires pour le marketing par courriel

12. Les entreprises de marketing par courriel devraient mettre en œuvre les pratiques exemplaires recommandées par le Groupe de travail sur le pourriel et, de concert avec l'organisme de coordination mis sur pied par le ministre de l'Industrie, devraient évaluer continuellement l'efficacité de ces pratiques.

13. Le secteur industriel canadien, en coordination avec les organismes internationaux d'élaboration de normes, devrait continuer d'étudier diverses méthodes de certification et leurs frais connexes pour déterminer quelle méthode, s'il en est, constituerait le régime de certification le plus approprié au Canada.

14. Pour déterminer la portée du problème de non-livraison du courriel légitime au Canada, l'organisme de coordination mis sur pied par le ministre de l'Industrie devrait étudier officiellement cette question de façon permanente, avec l'aide des intervenants appropriés.

FREINER LE POURRIEL

QU'EST-CE QUE LE POURRIEL ET POURQUOI POSE-T-IL UN PROBLÈME?

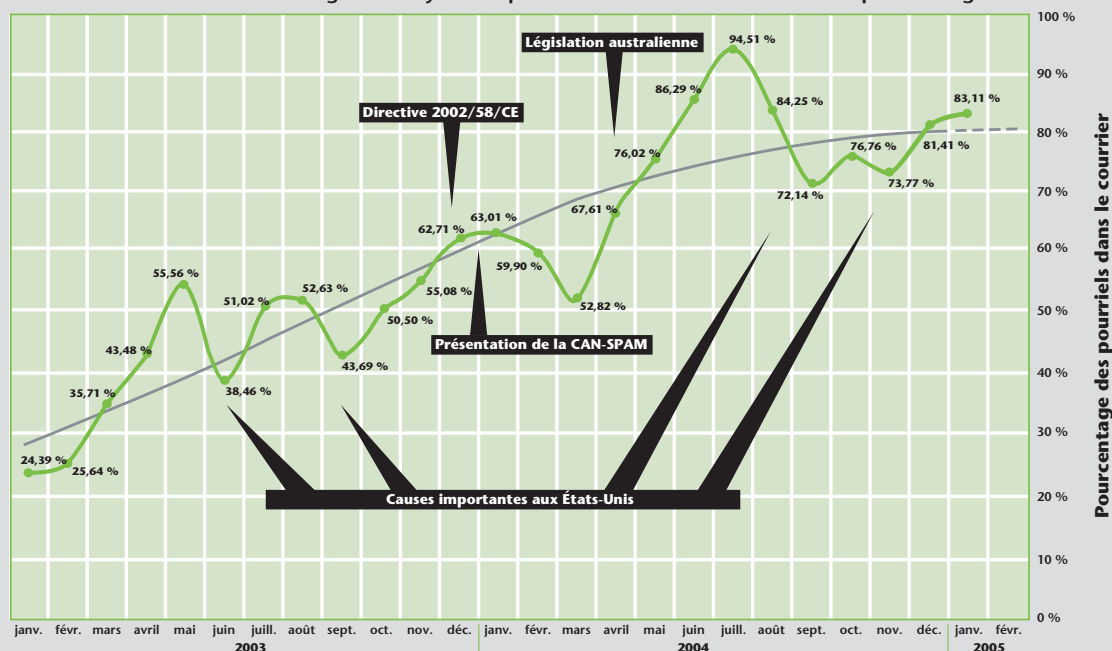
En quelques années seulement, le volume de messages électroniques commerciaux non sollicités, communément appelés « pourriels », est devenu, de l'ennui mineur qu'il était, un problème social et économique important qui mine la productivité individuelle et commerciale des Canadiens, ainsi qu'une couverture aux activités criminelles. Le pourriel entrave l'utilisation efficace du courriel pour les communications personnelles et commerciales, et menace la croissance et l'acceptation du commerce électronique légitime.

Les rapports sur la circulation du courriel indiquent que le pourriel représentait environ 10 p. 100 du volume total de courriels en 2000. Comme l'illustre la figure 1 :

- à la fin de 2002, il en représentait 30 p. 100;
- au milieu de 2003, le nombre de messages électroniques commerciaux non sollicités avait dépassé celui des communications légitimes;
- à la fin de 2004, le pourriel représentait 80 p. 100 du courriel global.

Figure 1 — Tendances globales du pourriel, 2003-2005

Ratio global moyen des pourriels dans les courriels scannés par MessageLabs



Source : www.message-labs.com (traduction)

MessageLabs Ltd., Tous droits réservés, 2005.

Il est maintenant reconnu que le volume croissant du pourriel a une influence sur le prix demandé par les entreprises qui fournissent des services Internet. Ce coût est au bout du compte assumé par les organismes et les entreprises qui utilisent les communications électroniques pour leurs affaires, et il est reflété dans les frais de service des particuliers qui utilisent Internet afin de communiquer avec leur famille, leurs amis et d'autres correspondants.

La nature de la menace posée par le pourriel évolue à mesure que le volume global de pourriels augmente. Il est vrai que les techniques de filtrage améliorées et autres mesures de protection adoptées par les FSI et les consommateurs ont contribué à réduire le nombre de pourriels qui entrent dans les boîtes aux lettres des internautes. D'ailleurs, un sondage d'opinion publique publié dans le *Canadian Inter@ctive Reid Report* d'Ipsos-Reid pour le quatrième trimestre de 2004, rapporte que les Canadiens croient recevoir moins de pourriel qu'il y a un an. Néanmoins, la tendance persistante à la hausse, illustrée dans la figure 1, demeure un problème important pour les FSI et les utilisateurs qui doivent assumer le fardeau des coûts associés au filtrage ou à l'élimination du pourriel.

Une tendance est cependant encore plus importante. On constate que, même si le volume de pourriels traditionnels diminuait, les menaces posées par les nouvelles formes de pourriel augmenteraient. Ces menaces plus vastes à la sécurité d'Internet incluent entre autres les logiciels espions, les virus, l'hameçonnage et les réseaux d'ordinateurs zombies. Des rapports récents démontrent que ces menaces ont considérablement augmenté depuis le début des travaux du Groupe de travail il y a un an. Par exemple :

- MessageLabs a fait rapport de 18 millions de courriels hameçons en 2004.
- L'étude *Online Safety Study* d'AOL®—National Cyber Security Alliance, publiée en octobre 2004, rapporte que 80 p. 100 des utilisateurs américains ont des logiciels espions ou publicitaires sur leurs ordinateurs et que 89 p. 100 d'entre eux en ignorent la présence.

Les récentes formes de pourriel minent la confiance des consommateurs à l'égard d'Internet en tant que plate-forme de commerce électronique et de communication. À cause de cela, la capacité des technologies de l'information et des communications d'appuyer la productivité, et celle du commerce électronique d'attirer l'investissement, de créer des emplois et d'enrichir nos vies, sont entravées par le poids des pourriels et des activités trompeuses, frauduleuses et nuisibles qui l'accompagnent parfois.

Principes directeurs du Plan d'action anti-pourriel pour le Canada

L'ampleur des préoccupations suscitées au sein du grand public et le coût croissant que doit subir notre économie indiquent clairement qu'il est temps que les pouvoirs publics, le milieu des affaires, le secteur du marketing et les consommateurs fassent front commun afin de réduire et de contrôler les pourriels.

Il est évident que le pourriel est un problème multiple qui demande que l'on prenne des mesures concertées à plusieurs niveaux, afin d'arriver à des résultats réels et mesurables. Intervenants canadiens et partenaires internationaux s'entendent sur les principes suivants :

- Les courriels commerciaux envoyés avec le consentement préalable et continu du destinataire ne sont pas des pourriels et occupent une place légitime dans le commerce électronique.
- Les courriels commerciaux envoyés sans consentement préalable, ou qui sont trompeurs, frauduleux ou nuisibles, sont des pourriels et doivent être interdits.
- Le recours aux lois actuelles et à d'éventuelles nouvelles lois pour lutter contre le pourriel mérite d'être examiné. Toutefois, à moins que les organismes d'application de la loi accordent une grande priorité et suffisamment de ressources aux actions anti-pourriel, les lois à elles seules n'endigueront pas la circulation des pourriels, ni les menaces connexes, même si ces lois sont assorties de mesures techniques, de meilleures pratiques commerciales et d'un changement de comportement de la part des consommateurs.

- On s'entend pour affirmer que le gouvernement devrait éviter de prescrire des solutions techniques détaillées. Au lieu de cela, il devrait encourager et aider tous ses partenaires à utiliser et à partager les meilleures solutions techniques et pratiques commerciales et de consommation.
- Une solution efficace au problème du pourriel exige non seulement une action concertée de la part de tous les partenaires canadiens, mais également une collaboration accrue à l'échelle internationale. Bien que, malheureusement, le Canada demeure une source de pourriel, la majorité des pourriels reçus par des Canadiens émane de l'étranger. Une démarche anti-pourriel internationale efficace nécessitera une action concertée de la part des gouvernements et autres intervenants.

Mandat, structure et méthodes de travail du Groupe de travail sur le pourriel

Le 11 mai 2004, la ministre de l'Industrie a annoncé le lancement du *Plan d'action anti-pourriel pour le Canada* visant à réduire le volume des courriels commerciaux non sollicités et a mis sur pied le Groupe de travail sur le pourriel afin de coordonner la mise en œuvre du Plan d'action. Présidé par Industrie Canada, le Groupe de travail réunit des experts et des intervenants clés représentant les FSI, les entreprises canadiennes qui utilisent le courriel à des fins commerciales légitimes et les consommateurs.

Le Groupe de travail disposait d'un an pour voir à la mise en œuvre du Plan d'action et la coordonner. Après cette période, il devait faire rapport sur les progrès accomplis et proposer toute autre initiative pouvant s'avérer nécessaire, y compris des mesures législatives.

Malgré le nombre réduit de ses membres, le Groupe de travail représentait un vaste éventail d'organisations qui s'intéressaient à l'avenir des communications par courriel, allant des utilisateurs individuels aux grands concepteurs et fournisseurs des logiciels et du matériel qui alimentent la croissance d'Internet. Afin d'organiser ses travaux et de recruter d'autres intervenants, le Groupe de travail a mis sur pied cinq sous-groupes pour traiter des points précis abordés dans le Plan d'action :

- la législation et son application
- les technologies et la gestion de réseaux
- la validation du courriel commercial
- l'éducation et la sensibilisation du public
- la collaboration internationale

La participation aux groupes de travail était ouverte à toute personne ou organisation intéressée. Environ 60 organisations ont répondu à l'appel (voir la liste à l'appendice A).

On a demandé au Groupe de travail, durant son mandat, de réunir les principaux intervenants afin d'examiner la mise en œuvre du Plan d'action et de cerner d'autres domaines susceptibles d'exiger une nouvelle initiative. Pour ce faire, il a organisé une table ronde des intervenants le 3 décembre 2004.

On a également demandé au Groupe de travail de consulter tous les intervenants et les Canadiens intéressés à exprimer leur opinion ou à contribuer à ses travaux. À cette fin, il a publié un avis dans la *Gazette du Canada* durant l'été 2004 et a établi un forum en ligne où les particuliers pouvaient exprimer leur opinion sur n'importe quel sujet étudié par le Groupe de travail.

Recommandation générale

L'expérience du Groupe de travail a démontré l'importance et la nécessité d'avoir recours à une approche multiple pour lutter contre le pourriel. Bien que la lutte contre les courriels commerciaux non sollicités ait considérablement progressé pendant l'année qui vient de s'écouler, il reste encore beaucoup à faire.

De plus, l'apparition de nouvelles menaces bien plus graves à la sécurité d'Internet, tels les logiciels espions et l'usurpation d'identité découlant du hameçonnage et autres activités illicites en ligne, souligne l'importance de conserver l'élan des différents intervenants, dans la foulée des travaux du Groupe de travail.

Le Groupe de travail a conclu que la réussite de la lutte anti-pourriel exigeait l'établissement d'un organisme central chargé de coordonner les démarches visant à contrer le pourriel et les activités illicites connexes.

C'est pourquoi nous formulons la recommandation suivante :

Recommandation 1 :

Le gouvernement fédéral, en association avec d'autres intervenants, devrait continuer à préconiser une stratégie à facettes multiples pour mettre fin au pourriel.

CLARIFIER LES RÈGLES

LE DÉFI

Les marchés traditionnels des biens et services sont régis par des lois et des règlements destinés à promouvoir la concurrence loyale et à protéger les consommateurs. Pour fonctionner efficacement, le cybercommerce requiert des règlements semblables pour guider le comportement commercial. Tel que discuté dans le chapitre précédent, le pourriel pose une menace de taille au développement du cybercommerce, car il occasionne des coûts, crée de l'inefficacité, cause du tort et entrave la confiance des entreprises et des consommateurs.

Des mesures telles que le renforcement des lois actuelles, la sensibilisation des entreprises et des consommateurs et la promotion de l'éducation du public permettraient d'éliminer certaines menaces attribuables au pourriel. Toutefois, il est peu probable que ces mesures viennent à bout des polluposteurs vraiment malhonnêtes — ceux qui entendent commettre une fraude, usurper l'identité ou enfreindre la vie privée des gens, obtenir un accès non autorisé ou endommager les ordinateurs et le matériel de réseau. Il faut donc mettre en œuvre des lois plus précises interdisant le comportement illicite, prévoir des peines sévères et appliquer rigoureusement les lois pour traiter ce genre de menace et appuyer la démarche anti-pourriel de type « boîte à outils » du Canada.

La mise en œuvre d'un cadre national solide sera encore plus essentielle, à mesure que le pourriel deviendra de plus en plus le véhicule d'activités telles que l'hameçonnage et de technologies comme les logiciels espions, les virus et les

réseaux d'ordinateurs zombies, qui, en minant la confiance, menacent sérieusement l'utilisation d'Internet en tant que plate-forme pour le commerce. Internet fait maintenant partie de l'infrastructure essentielle du pays, et il faut être capable d'éliminer ces menaces à sa sécurité.

Un cadre national solide permettrait également au Canada de prendre part à la lutte internationale contre le pourriel. La grande majorité des pourriels envoyés aux citoyens et aux entreprises du Canada provient de l'étranger. Cependant, avec un cadre législatif précis et solide, ainsi que des mécanismes d'application efficaces, le Canada serait bien positionné pour contribuer à la mise au point de démarches internationales harmonisées et de mesures d'application concertées.

L'une des premières questions qui s'est posée au Groupe de travail sur le pourriel était la mesure dans laquelle le cadre juridique et les mesures d'application actuellement en vigueur au Canada pourraient servir à combattre le pourriel.

Lors de l'élaboration du *Plan d'action anti-pourriel pour le Canada*, bon nombre d'intervenants ont déclaré qu'une meilleure application des lois fédérales existantes pourrait réduire sensiblement le volume du pourriel. Ils ont cité, notamment, la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), la *Loi sur la concurrence* et le *Code criminel du Canada* comme étant des outils pouvant servir à la réduction du courriel commercial non sollicité. Les motifs invoqués étaient les suivants.

- La LPRPDE, conçue de manière à protéger les renseignements personnels à l'ère électronique, interdit la collecte, l'utilisation ou la divulgation des renseignements personnels d'une personne, y compris son adresse de courriel, sans son consentement. Cette loi précise également que les renseignements personnels ne peuvent être utilisés à des fins autres que celles pour lesquelles ils sont recueillis, et que les propriétaires de ces renseignements doivent consentir à toute utilisation secondaire qui en est faite. Par conséquent, tout courriel non sollicité envoyé à l'adresse de courriel d'un particulier qui n'a pas consenti à le recevoir pourrait enfreindre cette loi fédérale et, peut-être, d'autres lois provinciales essentiellement similaires.
- La *Loi sur la concurrence* renferme des dispositions formelles à l'égard des représentations déloyales et trompeuses auxquelles on a souvent recours pour traiter la publicité mensongère publiée dans les médias traditionnels. L'application de la Loi aux revendications trompeuses contenues dans les sollicitations par courriel, est un domaine digne d'examen.
- Le *Code criminel du Canada* renferme des dispositions traitant spécifiquement de l'accès non autorisé aux systèmes et aux réseaux informatiques, de l'endommagement des données, ainsi que des dispositions plus générales concernant la fraude. Vu que bon nombre de polluposteurs enchâssent dans les courriels des « chevaux de Troie » pouvant être activés par les multiposteurs pour transmettre un pourriel, on pourrait éventuellement utiliser le *Code criminel du Canada* afin de punir ces délits. Ses dispositions prévoient des amendes importantes et même des peines d'emprisonnement.

Bien que les lois actuelles comportent des dispositions potentiellement utilisables dans la lutte contre le pourriel, le Groupe de travail a noté que leur efficacité était une question discutable, étant donné que la majorité d'entre elles n'ont pas encore été appliquées à des cas de pourriels.

Le premier défi du Groupe de travail consistait donc à examiner l'application du cadre juridique et des mécanismes d'application actuels du Canada à la lutte contre le pourriel. Pour ce faire, il a décidé de travailler avec les ministères et les organismes du gouvernement à l'examen des lois et des mécanismes d'application actuels

pour déterminer s'ils comportent des lacunes susceptibles de les rendre inefficaces dans la lutte anti-pourriel.

Puisque cela s'est révélé être le cas, le deuxième défi était de déterminer quelles mesures il faudrait adopter pour combler ces lacunes et doter le Canada d'un cadre juridique efficace et d'une démarche nationale concertée afin de contrer le pourriel et les activités connexes.

Activités du Groupe de travail

Sensibilisation et action catalytique des organismes d'application de la loi

La première tâche du Groupe de travail a été d'organiser des entretiens entre des sociétés privées et les organismes d'application des lois fédérales responsables de la législation susceptible d'être utilisée afin de contrer le pourriel, notamment le Bureau de la concurrence, le Commissariat à la protection de la vie privée du Canada et la Gendarmerie royale du Canada (GRC). L'objectif était d'évaluer l'efficacité de chaque loi pour les poursuites fondées sur des infractions liées au pourriel.

En première étape, le Groupe de travail a identifié toutes les lois fédérales pouvant s'appliquer aux diverses facettes du pourriel. Il a décidé de concentrer ses efforts sur les facettes ayant les liens les plus clairement associés aux lois actuelles. Le Groupe de travail a créé quelques sous-groupes pour aborder les exigences des diverses situations de fait, associées aux poursuites selon chaque loi. Au moment de la publication de ce rapport, trois plaintes ont été réglées en vertu de la LPRPDE, et une l'a été en vertu de la *Loi sur la concurrence* (voir l'encadré 1 — Récentes poursuites reliées au pourriel).

Peu de progrès ont été réalisés quant à l'application du *Code criminel du Canada*, à cause d'un manque de priorisation et de questions de compétence. En effet, les poursuites relèvent des administrations provinciales et des organismes locaux d'application de la loi. Cependant, le Groupe de travail a collaboré avec ces groupes pour faire progresser les travaux. En outre, il a travaillé avec Justice Canada et la Direction de la criminalité technologique de la GRC, afin de cerner les éléments de preuve voulus pour tenter une poursuite en vertu de dispositions précises du *Code criminel*.

Encadré 1 — Récentes poursuites reliées au pourriel

Décisions relatives à des plaintes déposées devant le Commissariat à la protection de la vie privée du Canada

Deux membres du Groupe de travail sur le pourriel ont porté plainte en vertu de la LPRPDE.

Michael Geist a reçu deux courriels l'invitant à acheter des billets de saison d'une équipe de football locale. Le bureau de l'équipe avait obtenu son adresse de courriel sur les sites Web de son université et de son cabinet juridique. M. Geist a déposé une plainte auprès du Commissariat à la protection de la vie privée, à la réception du deuxième courriel, après avoir demandé d'être rayé de la liste d'envoi.

Le commissaire à la protection de la vie privée a déterminé qu'une adresse de courriel commerciale est un renseignement personnel protégé par la LPRPDE. Ce genre de renseignement peut être recueilli et utilisé sans le consentement de la personne concernée, mais uniquement aux fins prévues (c'est-à-dire associées aux activités professionnelles de M. Geist). Le commissaire a conclu que l'équipe de football ne pouvait invoquer cette exception, étant donné que ses intentions étaient totalement étrangères aux fins pour lesquelles l'adresse de courriel avait été publiée.

Suzanne Morin a reçu des sollicitations par courriel, à son adresse de courriel commerciale, d'une société différente de celle de M. Geist. L'adresse de courriel provenait du répertoire électronique des membres d'une association professionnelle. M^{me} Morin a déposé une plainte auprès du Commissariat à la protection de la vie privée. Le commissaire a jugé, encore une fois, qu'en vertu de la LPRPDE, une adresse de courriel commerciale est un renseignement personnel. Le commissaire a déterminé que la collecte et l'utilisation subséquente de l'adresse de courriel aux fins de sollicitations commerciales avaient été effectuées par la société de marketing sans le consentement de M^{me} Morin et qu'il y avait eu violation de la Loi.

Dans les deux cas, les organismes ont présenté des excuses, retiré les adresses de courriel de leurs listes de marketing et modifié leurs procédures internes en conséquence.

Règlement d'un cas par le Bureau de la concurrence

Performance Marketing Ltd. a fait de fausses représentations selon lesquelles les timbres Zypex et Dyapex étaient des produits naturels et sans danger qui permettaient de perdre du poids, donnant ainsi la fausse impression que, sans suivre de régime ni effectuer d'exercice physique, une personne pourrait perdre du poids, avoir moins d'appétit, contrôler son envie de manger et accélérer son métabolisme. Ces allégations ont été faites par courriel. Performance Marketing a aussi échoué à mettre en œuvre sa politique anti-pourriel, ce qui a incité ses filiales à avoir recours au pourriel pour vendre les produits.

La cause a été jugée en vertu du Projet FrancNet du Bureau de la concurrence, destiné à éliminer la publicité trompeuse qui se retrouve dans Internet. Aux termes du consentement intervenu avec Performance Marketing en décembre 2004, la société s'est engagée à veiller à ce que le pourriel ne soit pas un véhicule de commercialisation de ses produits, à afficher un avis correctif dans son site Web et à rembourser intégralement les consommateurs qui avaient acheté les timbres coupe-faim.

Suite à des entretiens avec le secteur canadien des communications sans fil, on a soulevé la possibilité d'appliquer les dispositions de la *Loi sur les télécommunications* au pourriel envoyé aux combinés sans fil. L'adoption du projet de loi C-37 (prévoyant la création d'une liste nationale de numéros de téléphone exclus) pourrait renforcer la capacité du Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) de mettre un frein au pourriel acheminé par les appareils sans fil — précisément l'envoi électronique de pourriels par messagerie texte aux combinés sans fil. Le pouvoir du CRTC d'imposer des amendes revêtirait une importance particulière. Mais avant l'adoption du projet de loi C-37, il est peut-être encore trop tôt pour juger du rôle que la *Loi sur les télécommunications* pourrait jouer.

Problème de la mise en application des lois

Durant les étapes initiales de ses travaux, le Groupe de travail sur le pourriel a informé les deux organismes d'application de la loi de l'ampleur et de la gravité du problème du pourriel, et a mis les sociétés privées au fait des exigences juridiques et des critères de preuve relatifs aux poursuites. Parallèlement à ces travaux, certains organismes d'application de la loi ont entamé une action directe contre les polluposteurs (voir l'encadré 1 ci-dessus). Néanmoins, les mesures d'application ont été peu efficaces jusqu'à présent.

En effet, les organismes d'application ont de la difficulté à appliquer leur loi à toutes les facettes du pourriel. Qui plus est, les deux organismes d'application concernés, tout comme la GRC et les autorités policières locales, ont des ressources restreintes et des priorités conflictuelles qui limitent leur capacité d'intervention. L'application

est également entravée par la pénurie chronique d'experts nécessaires pour retracer, mener des enquêtes et tenter des poursuites contre les polluposteurs. Enfin, dans bien des cas, les pouvoirs d'application actuels n'ont pas encore été utilisés, et les mesures législatives qui permettraient d'attaquer certaines facettes du pourriel ont une application trop incertaine ou sont simplement inexistantes.

Le Groupe de travail croit fermement qu'il faut renforcer le processus d'application. Pour ce faire, il faut tout d'abord s'engager politiquement à freiner le pourriel et les activités semblables, non seulement en répondant aux plaintes, mais en menant des enquêtes proactives et en intentant des poursuites contre les polluposteurs. L'augmentation des ressources financières et techniques est essentielle, mais le soutien accordé aux organismes d'application devrait également prendre la forme de mécanismes plus efficaces pour la collecte, la coordination et le traitement des renseignements sur le pourriel, notamment ceux qui sont fournis par les gens qui déposent des plaintes. Le chapitre 7 du présent rapport aborde ces mécanismes. Enfin et surtout, il importe de combler les lacunes du régime juridique et réglementaire qui s'applique au pourriel et aux autres menaces pour Internet, tels les logiciels espions.

Recherche juridique

Pour établir le contexte de ses délibérations, le Groupe de travail a entrepris une analyse des lois anti-pourriel des autres pays, particulièrement des États-Unis, du Royaume-Uni et de l'Australie. L'analyse avait pour but de comparer la situation actuelle du Canada à celle de ces compétences. L'encadré 2 intitulé « Lois internationales anti-pourriel » énonce le titre des lois en vigueur dans quelques pays clés.

Encadré 2 — Lois internationales anti-pourriel

États-Unis — *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003* (CAN-SPAM Act of 2003)

Australie — *Spam Act 2003*

Royaume-Uni — *Privacy and Electronic Communications Regulations 2003*

France — *Loi pour la confiance dans l'économie numérique 2004*

Union européenne — *Directive 2003/58/CE*

En outre, le Groupe de travail a commandé une étude du droit privé d'action contre le pourriel au Canada, qui abordera notamment le cadre législatif existant, les principaux éléments constitutifs d'un tel droit et l'opinion des entreprises canadiennes sur l'importance de ce dernier.

Identification des lacunes législatives

Après avoir examiné les lois et les mécanismes d'application, l'expérience des pays ayant déjà adopté des lois générales anti-pourriel, l'issue des poursuites de ses membres et les leçons retenues, le Groupe de travail a conclu qu'il y avait des lacunes évidentes dans les lois et les mécanismes d'application canadiens.

En effet, bien qu'elles soient applicables à certaines facettes du pollupostage, les dispositions des trois lois pertinentes ne peuvent être utilisées avec suffisamment de certitude pour contrer efficacement les méthodes et les moyens des polluposteurs, les intrusions plus agressives et envahissantes, ni les nouvelles menaces à la sécurité du réseau Internet. Pour leur part, les pouvoirs d'application des organismes sont limités par la portée et les objectifs des lois qui les régissent, et, selon leur libellé actuel, ces lois excluent un grand nombre d'activités de pollupostage et d'activités connexes.

On a cerné une autre lacune sur le plan de la dissuasion. Au regard des lois applicables, on s'est posé la question suivante : « Les sanctions sont-elles suffisamment sévères pour décourager le pollupostage? ». Le Groupe de travail a déterminé que, bien que les mécanismes actuels soient adéquats dans le cas des sociétés légitimes qui se sont adonnées au pollupostage par erreur, il n'est pas évident qu'ils dissuaderaient les véritables contrevenants. En outre, même lorsque des sanctions significatives sont prévues, par exemple dans le *Code criminel*, l'aspect pratique de leur application aux poursuites fondées sur des infractions liées au pourriel est limité.

Un cadre pour les lois anti-pourriel et leur mise en application

Après avoir systématiquement évalué l'utilité des lois et des mesures d'application actuelles à la lumière des menaces posées par le pourriel et les activités connexes, le Groupe de travail a conclu ce qui suit :

- Bien que les lois actuelles traitent de facettes précises du pourriel, elles ne permettent pas, individuellement ou ensemble, d'atteindre l'objectif global, à savoir décourager les polluposteurs au Canada.
- Une loi autonome, neutre quant aux techniques visées et traitant clairement du pourriel, des infractions liées au pourriel et des nouvelles menaces (par exemple réseaux d'ordinateurs zombies, logiciels espions et logiciels de surveillance des entrées au clavier de l'utilisateur) s'impose. Des modifications aux lois actuelles pourraient également s'avérer nécessaires.

Nature des infractions, recours et sanctions

- Le défaut de se conformer à des procédures d'inclusion pour l'envoi de messages électroniques non sollicités devrait constituer une infraction au titre d'une loi anti-pourriel autonome, neutre quant aux techniques visées.
- L'utilisation d'en-têtes ou de lignes de mention objet faux ou trompeurs (c'est-à-dire transmission de faux renseignements) destinés à déguiser l'origine, l'objectif ou le contenu d'un courriel devrait constituer une infraction et ce, que le but soit de tromper les destinataires ou de contourner les filtres techniques.
- La construction d'adresses URL et de sites Web faux ou trompeurs dans le but de recueillir des renseignements personnels par escroquerie ou à des fins criminelles (ou pour commettre les autres infractions énumérées) devrait constituer une infraction.
- La collecte d'adresses de courriel sans consentement, ainsi que la diffusion, l'utilisation ou l'acquisition de ces listes, devraient constituer une infraction.

- Les attaques de dictionnaire devraient constituer une infraction.
- Les nouvelles infractions établies devraient être d'ordre civil et de responsabilité stricte, et prévoir une responsabilité criminelle pour les infractions plus flagrantes ou répétées. Il devrait y avoir des sanctions statutaires importantes pour toutes les infractions susmentionnées.
- Un droit privé d'action approprié devrait être offert aux personnes, individus et entreprises. Des dommages-intérêts statutaires significatifs devraient être prévus pour les personnes qui entament une poursuite civile.
- Les entreprises dont les produits ou services sont promus par le truchement du pourriel devraient être tenues également responsables du pourriel. La responsabilité devrait aussi incomber aux tiers qui bénéficient du pourriel.

Administration et application de la loi

- L'administration de la nouvelle loi anti-pourriel devrait être du ressort du ministre de l'Industrie, et l'on devrait établir un centre de responsabilité pour la surveillance et la coordination des politiques, l'éducation et la sensibilisation du public et l'octroi d'un soutien aux organismes d'application de la loi.
- L'application des nouvelles dispositions législatives anti-pourriel devrait relever des organismes existants.
- On devrait augmenter les ressources et l'aide destinées aux organismes responsables de l'application des dispositions anti-pourriel nouvelles et actuelles.
- Étant donné que le pourriel est un problème sans frontière, on devrait prévoir des dispositions favorisant l'application des lois et la tenue d'enquêtes à l'échelle internationale. Toutes les dispositions actuelles devraient être examinées et modifiées au besoin pour permettre la mise en œuvre de démarches anti-pourriel homogènes.

Mesures réglementaires

Bien que les discussions du Groupe de travail aient porté principalement sur l'interdiction du pourriel et des activités connexes, les participants à la Table ronde des intervenants de décembre 2004 et les membres du Groupe de travail ont discuté du bien-fondé de mesures réglementaires plus vastes. Certains favorisaient une démarche coréglementaire fondée sur le modèle australien qui énoncerait les responsabilités des FSI dans des secteurs tels que la protection des réseaux contre le pourriel. D'autres préféraient la pratique canadienne axée sur la coopération volontaire et la pression unificatrice du secteur industriel, mentionnant qu'elle serait une méthode de lutte anti-pourriel plus rapide et efficace que la démarche coréglementaire. Le sujet a été longuement débattu, mais on a convenu à l'unanimité que le gouvernement ne devrait pas dicter de solutions techniques précises et que les règles fondamentales législatives (y compris celles qui sont décrites précédemment) devraient être plus neutres quant aux techniques utilisées et visées.

Le secteur industriel s'efforce déjà de régler le problème du pourriel, mais l'expérience du Groupe de travail démontre que le dialogue gouvernement-secteur industriel peut contribuer à mobiliser les énergies du secteur privé. Par conséquent, le Groupe de travail accorde énormément d'importance à la poursuite du dialogue entre le gouvernement et le secteur industriel dans ce domaine. Il croit également que les questions plus vastes concernant la réglementation d'Internet doivent être étudiées dans le cadre de l'examen de la politique des télécommunications annoncé par le gouvernement du Canada dans le budget fédéral de 2005.

Recommandations

Après avoir analysé la situation canadienne et l'expérience des autres pays, le Groupe de travail a conclu que le Canada ne pourrait pas combattre efficacement le pourriel au pays à moins d'intégrer à sa démarche anti-pourriel multiple, un ensemble de lois plus précises, exhaustives et appliquées de façon active, qui protègent les internautes et favorisent la croissance du cybercommerce.

En conséquence, nos recommandations sont les suivantes :

Recommandation 2 :

Le gouvernement fédéral devrait adopter un ensemble de règlements judiciaires précis, visant à interdire le pourriel et les nouvelles menaces à la sécurité du réseau Internet (par exemple réseaux d'ordinateurs zombies, logiciels espions et logiciels de surveillance des entrées au clavier de l'utilisateur) et, pour ce faire, adopter une nouvelle loi et modifier les lois actuelles au besoin.

Recommandation 3 :

À cette fin, les activités et pratiques de multipostage abusif suivantes devraient constituer des infractions au titre d'une loi anti-pourriel spécifique (ces dispositions peuvent également être énoncées, en totalité ou en partie, dans les lois actuelles) :

- **le défaut de se conformer à des procédures d'inclusion pour l'envoi de courriels non sollicités;**
- **l'utilisation d'en-têtes ou de lignes de mention objet faux ou trompeurs (c'est-à-dire transmission de faux renseignements) destinés à déguiser l'origine, le but ou le contenu d'un courriel, que l'objectif soit de tromper le destinataire ou de contourner les filtres techniques;**
- **la construction d'adresses URL et de sites Web faux ou trompeurs dans le but de recueillir des renseignements personnels par escroquerie ou à des fins criminelles (ou pour commettre les autres infractions énumérées);**

- la collecte d'adresses de courriel sans consentement, ainsi que la diffusion, l'utilisation ou l'acquisition de ces listes;
- les attaques de dictionnaire.

Recommandation 4 :

Les sanctions et recours suivants devraient s'appliquer à ces nouvelles infractions :

- les nouvelles infractions établies devraient être d'ordre civil et de responsabilité stricte, et prévoir une responsabilité criminelle pour les infractions plus flagrantes ou répétées. Il devrait y avoir des sanctions statutaires importantes pour toutes les infractions énumérées à la recommandation 3;
- un droit privé d'action approprié devrait être offert aux personnes, individus et entreprises. Des dommages-intérêts statutaires significatifs devraient être prévus pour les personnes qui entament une poursuite civile;
- les entreprises dont les produits ou services sont promus par le truchement du pourriel devraient être tenues également responsables du pourriel. La responsabilité devrait également incomber aux tiers qui bénéficient du pourriel.

Recommandation 5 :

En ce qui concerne l'application et l'administration de la nouvelle loi :

- l'administration de la nouvelle loi anti-pourriel devrait être du ressort du ministre de l'Industrie, et l'on devrait établir un centre de responsabilité pour la surveillance et la coordination des politiques, l'éducation et la sensibilisation du public et l'octroi d'un soutien aux organismes d'application;
- l'application des nouvelles dispositions législatives anti-pourriel devrait relever des organismes existants.

Recommandation 6 :

Le gouvernement fédéral devrait accorder la priorité à l'application des mesures anti-pourriel en renforçant le soutien et les ressources destinés aux organismes responsables de l'application des lois anti-pourriel nouvelles et actuelles.

Recommandation 7 :

Le gouvernement fédéral, de concert avec les provinces et les territoires, devrait conclure et mettre en œuvre des accords de coopération en matière d'application des lois avec d'autres pays. Toutes les dispositions législatives actuelles devraient être examinées et modifiées au besoin pour permettre la mise en œuvre d'enquêtes coopératives et de mesures de mise en application homogènes, à l'échelle internationale.



GÉRER LES RÉSEAUX POUR CONTRER LE POURRIEL

LE DÉFI

Toute mesure visant à protéger la sécurité des communications Internet de menaces comme les pourriels, les virus et les logiciels espions doit s'appuyer sur autre chose que des démarches gouvernementales. De plus en plus d'intervenants reconnaissent que les FSI et les autres exploitants de réseaux (par exemple les grandes entreprises, les universités et les ministères gouvernementaux) peuvent adopter plusieurs mesures pour rétablir la confiance à l'égard des communications Internet.

Certaines de ces mesures portent sur la mise au point et l'application de la technologie, d'autres sur la mise en œuvre de pratiques exemplaires et de Politiques d'utilisation acceptable interdisant le pourriel au sein du secteur industriel. Elles sont fondées sur un objectif commun : veiller à ce que le courriel reste un outil valable pour les communications d'affaires et personnelles légitimes.

De par sa conception et son architecture, Internet est un « réseau de réseaux » ouvert qui permet la libre circulation de l'information. L'élaboration et la mise en œuvre de nouvelles normes techniques pour améliorer la sécurité et éliminer les abus se poursuivront pendant de nombreuses années.

Certaines pratiques connues de gestion des réseaux peuvent cependant favoriser le pourriel et d'autres formes d'abus du réseau. Par exemple, en laissant les serveurs ouverts pour relayer ou envoyer des messages, on permet que des systèmes informatiques soient la proie de ceux qui les transforment en serveurs mandataires pour le pollupostage. Plusieurs organismes ont entrepris d'avertir les entreprises et les

gestionnaires de réseaux de l'importance d'assurer la sécurité des systèmes et des réseaux, mais l'adoption des pratiques proposées reste inégale.

Bien que le problème du pourriel, à l'instar d'Internet, soit un phénomène mondial, des démarches en matière de gestion des réseaux adoptées au Canada peuvent contribuer à le résoudre. Les propriétaires et les gestionnaires de réseaux doivent envisager et adopter des pratiques de gestion qui mettront un frein au pourriel et aux menaces connexes.

Les intervenants du secteur industriel canadien peuvent se mettre d'accord sur des pratiques de base d'exploitation des réseaux qui mettront un frein au pourriel et faire preuve de leadership en exigeant l'adoption de ces pratiques par les installations et réseaux établis au Canada.

Activités du Groupe de travail

La création du Groupe de travail sur le pourriel représente le tout premier effort de collaboration entre un vaste éventail d'organisations, y compris la plupart des plus grands et plus petits FSI à large bande et par réseau commuté, d'autres exploitants de réseaux, les grandes entreprises qui utilisent Internet, les concepteurs de logiciels, les groupes de lutte contre le pourriel et le gouvernement. L'accord des intervenants, en matière de collaboration à l'élaboration et à la mise en œuvre de solutions au problème du pourriel à l'échelle de tout le secteur industriel, représente un énorme accomplissement. Cependant, ce n'est que le début d'un engagement à long terme à l'égard de l'adoption des mesures nécessaires pour mettre fin au pourriel.

L'expérience des autres pays a démontré que les FSI, particulièrement les leaders du marché, peuvent favoriser l'adoption de pratiques exemplaires techniques et commerciales anti-pourriel au sein du secteur industriel. En fait, certains FSI canadiens ont déjà mis en œuvre les pratiques exemplaires recommandées, et leur esprit d'initiative a encouragé d'autres FSI à faire de même.

Tout cela semble prometteur, mais il faudra surveiller systématiquement la mise en œuvre des pratiques exemplaires recommandées, afin d'en évaluer les répercussions et de repérer les nouveaux problèmes qui pourraient exiger des amendements ou des ajouts aux dispositions des pratiques exemplaires. À défaut de cela, le secteur industriel, les décideurs gouvernementaux et les autres intervenants auront de la difficulté à déterminer le niveau d'adoption des pratiques recommandées ou à évaluer leur contribution à la lutte anti-pourriel.

Le secteur industriel ayant fait valoir qu'il peut s'autoréglementer, le Groupe de travail encourage les principaux FSI et exploitants de réseaux à continuer à faire preuve de leadership par la mise en œuvre des pratiques exemplaires recommandées et à encourager les autres à suivre leur exemple.

Le Groupe de travail invite également les principaux joueurs et les associations concernées du secteur industriel à s'associer à l'organisme de coordination décrit au chapitre 7, pour élaborer un système efficace de mesure et de rapport public des répercussions des pratiques exemplaires recommandées.

Base de données canadienne sur les pourriels (« congélateur à pourriels »)

Le Groupe de travail a examiné la possibilité d'établir, dans le cadre d'un partenariat des secteurs public et privé, une base de données canadienne sur les pourriels ou « congélateur à pourriels », dont la conception serait semblable à la base de données « réfrigérateur à pourriels » que maintient et gère la Federal Trade Commission (FTC) des États-Unis.

La base de données canadienne servirait d'archivage des copies de pourriels arrivés dans les boîtes aux lettres électroniques. Un organisme canadien chargé de coordonner la lutte anti-pourriel inventorierait ces pourriels et les conserverait pour une période de temps donnée.

Ainsi, les organismes d'application de la loi du Canada et, éventuellement, des autres pays, les FSI, les autres exploitants de réseaux et les divers paliers de gouvernement auraient accès à des données à des fins d'analyse statistique et de collecte de preuves pour l'application des lois anti-pourriel.

Pourriel acheminé sur les appareils sans fil

Contrairement à Internet qui a été conçu comme un réseau ouvert et public, les technologies mobiles ont été originellement déployées sur des réseaux privés et fermés.

Cependant, vu la convergence des technologies et l'interaction accrue entre Internet et les technologies mobiles, certains problèmes qui, à l'origine, affectaient uniquement Internet, commencent à toucher les réseaux mobiles. Ces problèmes sont associés à la récupération du courriel (y compris du pourriel) au moyen d'appareils mobiles. Ils découlent également de la réception de nouvelles formes de pourriel émanant des réseaux sans fil et transmis par messagerie texte, messagerie multimédia et messagerie instantanée aux combinés sans fil. Applications réussies de la technologie mobile, ces services de messagerie ouvrent la voie à des services innovateurs, mais fournissent de nouvelles possibilités aux polluposteurs.

Le pourriel dit « mobile » ou « sans fil » peut poser des problèmes plus graves que le pourriel envoyé aux ordinateurs de bureau car il suit le client, et ce dernier paie parfois des frais pour chaque message reçu. Très gênant pour les abonnés des services mobiles, le pourriel sans fil pourrait devenir beaucoup plus dérangentant que le pourriel envoyé à un ordinateur personnel.

Le Groupe de travail a consulté le secteur des communications sans fil canadien pour discuter du problème et envisager des mesures aptes à empêcher le pourriel de devenir un problème majeur pour les réseaux sans fil. Lors de ces entretiens, il a appris que les exploitants des réseaux sans fil considèrent le pourriel émanant des réseaux sans fil comme une menace grave. Pour protéger ses clients, le secteur des communications sans fil est d'ailleurs en train de mettre en place des mesures techniques et il envisage également des recours juridiques et réglementaires qui pourraient contribuer à prévenir le pourriel mobile.

Le Groupe de travail et les représentants du secteur des communications sans fil ont convenu que toute mesure anti-pourriel adoptée par le gouvernement fédéral et autres parties concernées, suite aux travaux et aux recommandations du Groupe de travail, devrait être neutre quant aux techniques utilisées et visées, et s'appliquer au secteur des communications sans fil au moyen de mécanismes appropriés.

Partage des renseignements techniques entre les fournisseurs de services Internet et les autres exploitants de réseaux

Le secteur industriel a accompli beaucoup de travail pour endiguer le pourriel et ses efforts ont mené à des améliorations notoires, mais il reste encore beaucoup à faire sur le plan de la collaboration.

Un meilleur partage des renseignements entre les FSI et les autres exploitants de réseaux représente un facteur clé de succès. La lutte anti-pourriel repose sur une démarche concertée à l'égard des problèmes, axée notamment sur une communication rapide et efficace des questions et problèmes d'intérêt commun et sur l'établissement de procédures intersociétés appropriées pour répondre aux rapports d'incidents.

Recommandations

Les FSI et autres exploitants de réseaux sont aux premières lignes de la lutte anti-pourriel. Point de contact entre les expéditeurs et les destinataires du pourriel, ils sont dans une position unique pour combattre le pourriel.

En conséquence, nos recommandations sont les suivantes :

Recommandation 8 :

Les FSI et autres exploitants de réseaux devraient mettre en œuvre les pratiques exemplaires recommandées par le Groupe de travail sur le pourriel.

Recommandation 9 :

Les FSI et autres exploitants de réseaux, en coopération avec l'organisme de coordination établi par le ministre de l'Industrie (mentionné à la recommandation 5), devraient mesurer de façon continue l'ampleur du problème du pourriel au Canada et évaluer les répercussions des pratiques recommandées. Ils devraient continuer à cerner les questions qui pourraient mériter davantage d'examen et mener à la formulation de recommandations additionnelles.

Recommandation 10 :

Afin de faciliter de façon continue la surveillance des tendances du pourriel et l'élaboration de mesures et de techniques anti-pourriel, le gouvernement devrait jouer un rôle de leadership en créant une base de données canadienne sur les pourriels (« congélateur à pourriels »).

Recommandation 11 :

Les FSI et autres exploitants de réseaux devraient adopter et appliquer des Politiques d'utilisation acceptable interdisant clairement le pollupostage sur leurs réseaux.

4

RÉTABLIR LA CONFIANCE À L'ÉGARD DU COURRIEL

LE DÉFI

Avant la mise sur pied du Groupe de travail sur le pourriel, la majorité des initiatives canadiennes visant à endiguer le volume croissant de courriels commerciaux non sollicités associaient des technologies de filtrage et le recours aux « listes noires » de serveurs et de domaines identifiés comme étant des sources de pourriel. Cependant, à mesure que ces services de contrôle du pourriel se perfectionnent, les polluposteurs se montrent eux-mêmes très ingénieux lorsqu'il s'agit de trouver de nouvelles façons de contourner les obstacles qu'on leur crée.

Les diverses technologies de filtrage et outils de blocage utilisés par les FSI et autres exploitants de réseaux, de même que les batailles cycliques entre polluposteurs et services de filtrage de pourriel, ont eu des effets non désirés. Les courriels commerciaux légitimes, comme les courriels non commerciaux et les courriels personnels légitimes, sont souvent interceptés par les filtres, parfois à l'insu de l'expéditeur ou du destinataire. Ces pratiques et techniques de filtrage, bien que mises en œuvre dans un but fort louable, ont donc contribué indirectement à miner la confiance du consommateur à l'égard de la fiabilité du courriel.

Pour cette raison, certains organismes commerciaux envisagent maintenant de se tourner vers des réseaux fermés, ce qui minerait l'utilisation efficace d'Internet comme plate-forme pour le commerce. On peut comprendre les motifs pour lesquels ils envisagent cette solution, mais l'abandon du réseau public Internet en faveur de réseaux privés pour les activités commerciales pourrait avoir des effets indésirables.

Des choix moins radicaux que le réseau fermé commencent à s'offrir sous la forme de techniques favorisant la circulation des courriels commerciaux légitimes plutôt que le filtrage des communications non désirées. Bien que l'utilisation de ces techniques puisse entraîner des frais pour les expéditeurs de courriels commerciaux et les propriétaires et gestionnaires de réseaux Internet, ces coûts seraient plus que contrebalancés par les avantages suivants :

- pour les expéditeurs de courriels commerciaux, une livraison améliorée;
- pour les fournisseurs de services, une réduction des frais de gestion du service de courriel et des préférences des clients;
- pour les utilisateurs du courriel, des outils de gestion du courriel plus efficaces.

La certification est une des techniques envisagées pour améliorer la livraison. L'obligation pour l'expéditeur de divulguer sa véritable identité et la nature de sa communication constituerait une exigence minimale pour l'établissement d'un régime de certification du courriel. Un tel régime devrait aussi prévoir un solide moyen de mesurer l'efficacité de la méthode ainsi que des sanctions appropriées s'appliquant aux détenteurs de certificats qui enfreignent les règles.

Outre la certification, on dispose maintenant de techniques qui facilitent la circulation du courriel légitime en authentifiant les sites d'envoi et de réception. Cependant, ces techniques ne protègent pas nécessairement les destinataires des courriels faux, trompeurs et frauduleux provenant de sites authentiques.

Encadré 4 — Pratiques exemplaires recommandées pour le marketing par courriel

- Les courriels de marketing devraient être envoyés uniquement aux destinataires qui ont consenti à recevoir les renseignements.
- Les courriels de marketing doivent fournir aux destinataires un moyen évident, clair et efficace de refuser, par courriel ou Internet, de recevoir d'autres courriels d'affaires et/ou de marketing de l'organisme.
- Le processus interne utilisé pour obtenir le consentement devrait être clair et transparent. Les organismes devraient conserver un dossier des types de demandes reçues des destinataires, afin de pouvoir mettre leurs listes d'envois de courriels à jour avant les campagnes de publicité.
- Chaque communication de marketing par courriel devrait clairement identifier l'expéditeur du courriel. La ligne de mention objet et le corps du texte devraient refléter correctement le contenu, l'origine et le but de la communication.
- Tout courriel devrait fournir un lien vers la politique de l'expéditeur sur les renseignements personnels. Celle-ci devrait expliquer le mode d'utilisation et de communication des renseignements personnels pouvant être recueillis par le biais du parcours de l'utilisateur ou d'autres techniques de surveillance des sites Web.
- Les entreprises de marketing, les courtiers et les propriétaires de listes d'adresses devraient prendre des mesures raisonnables pour s'assurer que les personnes dont l'adresse figure sur leurs listes de diffusion ont donné le consentement approprié.
- Les entreprises de marketing qui font du marketing par courriel auprès des personnes mineures devraient faire preuve de discrétion et de sensibilité et tenir compte de l'âge, des connaissances, du caractère averti et de la maturité de cet auditoire.
- Lorsque le contenu d'un courriel est destiné à des adultes, l'expéditeur devrait, avant de l'envoyer, vérifier si le destinataire est en âge de recevoir et de consulter légalement ce contenu.
- Tout courriel renfermant un contenu sexuellement explicite devrait inclure la balise de préface « SEXUELLEMENT EXPLICITE » dans la ligne de mention objet.
- Les organismes devraient mettre en place un système de traitement des plaintes juste, efficace, confidentiel et facile à utiliser.
- Les organismes peuvent divulguer les adresses de courriel de leurs clients à des tiers affiliés ou au sein d'une famille de sociétés si :
 - ils ont obtenu leur consentement;
 - ils utilisent les adresses aux fins pour lesquelles ils les ont recueillies (c'est-à-dire pour un marketing relié à l'achat original ou la prestation de services associés à cet achat);
 - les destinataires savent pourquoi ils reçoivent des courriels;
 - il y a un moyen facile de refuser de recevoir davantage de courriels.

Les résultats faux positifs posent un problème, d'une part aux entreprises en entravant l'efficacité du courriel comme outil de marketing, et d'autre part aux utilisateurs finaux qui comptent de plus en plus sur la livraison des courriels à destination et en provenance de sources professionnelles (par exemple, collègues de travail), commerciales (par exemple, suite au marketing et à des achats en ligne qu'ils ont effectués) ou personnelles (par exemple, correspondance privée).

Les entreprises de marketing et autres ont de plus en plus recours à des entreprises imparties spécialisées dans la livraison de leur courriel pour améliorer le rendement de leur investissement ou à l'embauche de personnel à temps plein pour traiter de ces questions.

Les FSI devraient envisager de publier des politiques et des procédures claires à l'égard du courriel d'arrivée, et de fournir des points de contact pour améliorer la livraison du courriel légitime.

Plusieurs des grands sites de réception, notamment AOL®, MSN® Hotmail et Yahoo!®, ont publié des politiques et procédures décrivant les exigences applicables aux expéditeurs de courriels légitimes souhaitant figurer sur une liste blanche. Le contournement des filtres anti-pourriel, grâce à ce statut, varie d'un site à l'autre.

Certification du courriel

Plusieurs techniques sont actuellement utilisées pour lutter contre le pourriel, mais certaines d'entre elles ne peuvent pas toujours distinguer le courriel légitime du pourriel. Par exemple, certains filtres anti-pourriel interceptent les envois en vrac de courriels légitimes simplement parce qu'ils ressemblent au pourriel. D'autres analysent le contenu des messages à l'aide de mots clés utilisés dans le courriel légitime et le pourriel pour déterminer s'ils doivent ou non être filtrés. Pour compliquer les choses davantage, il arrive que les polluposteurs déguisent leurs messages en courriels légitimes et utilisent d'autres techniques pour déjouer les filtres.

Tel que mentionné dans la section de ce chapitre intitulée « Le défi », la certification du courriel pourrait éventuellement permettre aux filtres anti-pourriel d'autoriser la livraison du courriel légitime aux destinataires prévus. Elle pourrait également servir à distinguer le courriel légitime du courriel hameçon.

En collaboration avec le Conseil consultatif canadien sur les normes de technologies de l'information et des télécommunications, le Groupe de travail sur le pourriel a examiné les régimes de certification existant au Canada, leurs principes, leurs modèles fonctionnels et leurs techniques. Un document de référence présentera les résultats de cette analyse et examinera ensuite les possibilités inhérentes à la mise en œuvre d'un régime de certification du courriel au Canada.

Recommandations

Les expéditeurs de courriels commerciaux sont ceux qui ont le plus à perdre et le plus à gagner dans la lutte anti-pourriel. De plus, parmi les divers groupes d'intervenants engagés dans la lutte anti-pourriel, ce sont ces expéditeurs de courriels commerciaux qui auront sans doute le plus de difficultés à s'organiser pour entreprendre des démarches concertées contre les polluposteurs et à participer à la mise en œuvre de l'approche de type « boîte à outils ».

Le groupe des intervenants composés des expéditeurs de courriels commerciaux rassemble des organismes très distincts, notamment :

- les entreprises qui ont recours au courriel de masse non sollicité pour commercialiser leurs produits et services;
- les entreprises de marketing par courriel;
- les concepteurs et gestionnaires de campagnes de marketing;
- les fournisseurs de services de courriel commercial;
- les fournisseurs de listes d'adresses de courriel.

Certaines sociétés qui fournissent ces produits et services sont verticalement intégrées dans divers segments de la chaîne de production du courriel commercial. D'autres sont autonomes et exercent leurs activités sur une base contractuelle.

La plupart des sociétés du groupe des intervenants composés des expéditeurs de courriels commerciaux exercent leurs activités dans le respect des lois et conformément aux pratiques commerciales généralement reconnues. Comme l'ont démontré les causes jugées en vertu de la LPRPDE, ces sociétés s'empressent généralement d'offrir compensation s'il est constaté qu'elles se sont adonnées à des activités ou à des pratiques contraires à ces normes.

Malheureusement, chaque segment de la chaîne de production du courriel compte des polluposteurs, entreprises et particuliers qui enfreignent de façon délibérée les lois interdisant l'envoi de courriels commerciaux non sollicités ou qui se servent du courriel pour s'adonner à des activités destinées à tromper le public, à endommager les ordinateurs et les réseaux, et à s'appropriier des renseignements personnels à des fins frauduleuses.

Pour arrêter le pourriel, il faut arrêter les polluposteurs. À défaut d'y arriver, nous risquons que les Canadiens perdent confiance en l'utilité d'Internet pour le marketing et la promotion des produits et services, et comme moyen efficace de communication. Or, une perte générale de confiance à l'égard du courriel, d'une part, entraverait sérieusement l'émergence d'une cyberéconomie au Canada et d'autre part, nuirait aux intérêts des nombreuses entreprises, organismes, institutions et instances gouvernementales associées à la chaîne de production du courriel professionnel.

En conséquence, nos recommandations sont les suivantes :

Recommandation 12 :

Les entreprises de marketing par courriel devraient mettre en œuvre les pratiques exemplaires recommandées par le Groupe de travail sur le pourriel et, de concert avec l'organisme de coordination mis sur pied par le ministre de l'Industrie, devraient évaluer continuellement l'efficacité de ces pratiques.

Recommandation 13 :

Le secteur industriel canadien, en coordination avec les organismes internationaux d'élaboration de normes, devrait continuer d'étudier diverses méthodes de certification et leurs frais connexes pour déterminer quelle méthode, s'il en est, constituerait le régime de certification le plus approprié au Canada.

Recommandation 14 :

Pour déterminer la portée du problème de non-livraison du courriel légitime au Canada, l'organisme de coordination mis sur pied par le ministre de l'Industrie devrait étudier officiellement cette question de façon permanente, avec l'aide des intervenants appropriés.

SENSIBILISATION DU PUBLIC

LE DÉFI

Les législateurs, les organismes d'application de la loi, les FSI et les autres exploitants de réseaux, ainsi que les utilisateurs du courriel commercial peuvent prendre une part très active à la lutte contre le pourriel. Toutefois, on s'entend généralement pour dire que tous les utilisateurs finaux d'Internet, les employés, les étudiants et les consommateurs ont un rôle important à jouer dans la lutte constante contre ce fléau.

Par ailleurs, pour aider les internautes à remplir leur rôle, on doit de toute évidence mieux les renseigner sur les mesures s'offrant à eux afin de limiter le volume de courriels commerciaux indésirables qu'ils reçoivent, se protéger et protéger les autres utilisateurs contre les virus, échapper aux pratiques frauduleuses et empêcher que des pirates ne contrôlent leur ordinateur pour envoyer des pourriels à leur insu.

L'information abonde sur les mesures que peuvent prendre les utilisateurs afin de limiter le volume de pourriels qu'ils reçoivent et échapper aux pratiques trompeuses et frauduleuses ou aux autres pratiques criminelles associées à ces pourriels. Toutefois, il ressort des sondages d'opinion publique que l'on doit redoubler d'efforts pour diffuser ces renseignements, en particulier ceux qui concernent les nouvelles menaces risquant de perturber le fonctionnement des appareils, de léser les consommateurs et de compromettre la sécurité d'Internet.

Les utilisateurs n'ont pas tous reçu ou compris certains messages très simples, comme « n'ouvrez pas les courriels non sollicités », « n'effectuez aucun achat auprès des polluposteurs » et « ne transmettez pas de renseignements personnels si vous ne connaissez pas avec certitude l'identité

du destinataire ». Par exemple, selon *The Ipsos Trend Report Canada* de mai-juin 2004 publié par Ipsos-Reid, plus du tiers des Canadiens branchés ouvrent les pourriels qu'ils reçoivent, et la curiosité constitue la principale raison invoquée à cet égard.

Une étude menée récemment par Option consommateurs a par ailleurs indiqué que certains groupes pourraient bénéficier d'une intensification des activités d'éducation et de sensibilisation adaptées à leurs besoins particuliers, entre autres les personnes de moins de 30 ans qui ont déclaré recevoir davantage de pourriels que les autres groupes et les personnes âgées.

Compte tenu qu'un faible taux de participation des consommateurs suffit pour assurer la viabilité commerciale des activités de pollupostage, l'approche de type boîte à outils doit mettre davantage en évidence le lien existant entre le volume de pourriels et le comportement des consommateurs.

En raison du lien direct qui les unit aux internautes, les FSI et les vendeurs légitimes de produits et services sont bien placés afin de mener une campagne d'éducation et de sensibilisation du public en partenariat avec les groupes de défense des consommateurs et les gouvernements. Pour le Groupe de travail sur le pourriel, le défi consistait donc à faciliter l'élaboration d'une campagne de marketing social et de communications s'adressant aux utilisateurs et à la mettre en œuvre en collaboration avec des groupes de défense des consommateurs, des ministères et organismes gouvernementaux et des partenaires internationaux intéressés.

Activités du Groupe de travail

En plus d'examiner la recherche actuelle sur l'opinion des consommateurs concernant les pourriels, le Groupe de travail a analysé les campagnes d'éducation et de sensibilisation en cours au Canada et dans d'autres pays. Plusieurs de ces initiatives ont bénéficié d'une visibilité limitée, mais les principaux messages véhiculés n'étaient pas toujours uniformes. Après l'examen de la recherche et des initiatives, le Groupe de travail a élaboré une stratégie de communications globale afin de définir les objectifs, les publics cibles et les outils nécessaires à une campagne potentielle d'éducation à grande échelle pour renseigner le public sur le pourriel.

Campagne « Arrêtez le pourriel ici / Stop Spam Here »

La première étape de la stratégie fut la mise sur pied d'une campagne bilingue d'éducation des utilisateurs dans Internet. Le succès de cette initiative reposait sur la formulation de messages clés cohérents, présentés de façon uniforme, et sur une vaste diffusion de trois conseils clés, par un large éventail de partenaires, pour aider les utilisateurs à se protéger et à lutter contre le pourriel.

En collaboration avec des spécialistes des communications et du marketing, le Groupe de travail sur le pourriel a conçu une icône que les partenaires pouvaient afficher dans leur site Web et qui renfermait un lien donnant accès aux conseils à l'intention des utilisateurs, affichés à <http://arretezlepourrielici.ca> et <http://stopspamhere.ca>. On trouve dans les deux versions du site Web la marche à suivre afin de participer à la campagne.

Le Groupe de travail a recruté des partenaires gouvernementaux et non gouvernementaux pour afficher l'icône dans leur site Web.

Les organismes des secteurs privé et public et la population en général ont répondu en grand nombre à la campagne « Arrêtez le pourriel ici / Stop Spam Here ». Entre le 25 novembre 2004, date de son entrée en service, et avril 2005, le site a reçu plus de 500 000 visites, et quelque 200 organismes ont participé à la campagne.

Recommandations

La campagne « Arrêtez le pourriel ici / Stop Spam Here » a commencé à éduquer les internautes canadiens sur les moyens qui s'offrent à eux pour réduire le volume de pourriels se retrouvant dans leur boîte de réception et échapper aux pratiques trompeuses, nuisibles, frauduleuses ou autrement illégales associées à certains types de pourriels.

Toutefois, il reste encore beaucoup à faire afin de permettre aux Canadiens de jouer leur rôle dans la lutte contre le pourriel, à commencer par l'amélioration du site Web « Arrêtez le pourriel ici / Stop Spam Here » et la diffusion de l'information qui s'y trouve dans d'autres médias.

Les messages d'ordre général qui s'appliquent à tous les consommateurs, tels que les trois conseils clés présentés ci-dessous, fournissent une base solide pour l'éducation et la sensibilisation du public. Toutefois, d'après le Groupe de travail, il faut aussi mener des campagnes d'éducation et de sensibilisation concordant avec les besoins et les intérêts particuliers de différents groupes de la population canadienne, afin de continuer à progresser.



Arrêtez le pourriel ici : trois conseils clés

1. Protégez votre ordinateur

Le pourriel est une source croissante de virus informatiques. Il est essentiel que vous protégiez votre ordinateur contre les messages transportant des virus. Installez un logiciel anti-virus et anti-pourriel et mettez-le à jour régulièrement. Procurez-vous aussi la protection supplémentaire d'un coupe-feu.

2. Protégez votre adresse de courriel

Réservez une adresse de courriel pour les contacts personnels et professionnels en qui vous avez confiance. Créez une adresse de courriel extensible distincte pour d'autres utilisations en ligne.

3. Protégez-vous

N'essayez rien, n'achetez rien et ne répondez pas aux pourriels. Supprimez-les. C'est une bonne façon de ne pas en recevoir d'autres dans l'avenir.

Le Groupe de travail estime qu'il est primordial de faire participer les petites et moyennes entreprises à la lutte contre le pourriel, car elles seront parmi les plus grands bénéficiaires d'un environnement commercial électronique exempt de pourriels.

C'est pourquoi nous formulons les recommandations suivantes :

Recommandation 15 :

Dans le cadre des efforts continus qu'il déploie pour accroître la sensibilisation et l'éducation des utilisateurs, le gouvernement fédéral, en collaboration avec les intervenants intéressés, devrait continuer de promouvoir la campagne axée sur les conseils aux utilisateurs « Arrêtez le pourriel ici / Stop Spam Here », en encourageant les responsables d'autres sites Web à placer dans leur site un lien qui y donne accès et en utilisant d'autres méthodes et médias appropriés.

Recommandation 16 :

Le gouvernement fédéral, en collaboration avec les intervenants intéressés, devrait continuer de maintenir et d'enrichir les deux versions du site Web « Arrêtez le pourriel ici / Stop Spam Here ». Le but est d'en faire un mécanisme plus efficace comme outil d'éducation et source de liens utiles donnant accès à d'autres ressources de lutte contre le pourriel, et de veiller à ce que les deux versions demeurent à jour et pertinentes (par exemple, en y affichant de l'information sur les pratiques exemplaires du secteur industriel, la future législation anti-pourriel et les procédures à suivre pour déposer une plainte).

Recommandation 17 :

Le gouvernement fédéral, en collaboration avec les intervenants intéressés, devrait élaborer des campagnes de sensibilisation et d'éducation efficaces et cohérentes adaptées aux besoins de différents groupes de destinataires cibles en matière de lutte contre le pourriel.

RÉSOLVRE UN PROBLÈME MONDIAL

6

LE DÉFI

Selon les estimations, une faible proportion des pourriels reçus par les Canadiens provient du Canada. Cela s'explique par la nature ouverte d'Internet, qui fait en sorte que les pourriels peuvent être acheminés entre n'importe quels endroits de la planète. Par conséquent, l'harmonisation des politiques anti-pourriel ainsi que la collaboration entre différents pays en ce qui concerne l'application des lois dans le domaine sont essentielles pour faire échec au pourriel.

Depuis plusieurs années déjà, le Canada participe activement aux tribunes internationales consacrées à Internet. Les récentes discussions ont porté en grande partie sur les différentes mesures législatives, réglementaires et d'application prises par certains pays pour lutter contre le pourriel, ainsi que sur la nécessité de veiller à ce que les approches adoptées soient compatibles avec l'environnement mondial d'Internet.

Grâce à ces travaux, on progresse sur le front de la coordination des politiques anti-pourriel entre les pays et de la coopération internationale dans l'application des lois et règlements anti-pourriel. Certains pays y sont parvenus en greffant les mesures d'application sur les accords de collaboration en vigueur comme celui qui existe entre le Bureau de la concurrence du Canada et la Federal Trade Commission des États-Unis. Toutefois, on n'a eu recours à ces accords que dans une mesure limitée, et il faudrait en élaborer de nouveaux portant expressément sur l'application des lois et règlements anti-pourriel.

Il reste beaucoup de travail à faire pour promouvoir une coordination et une collaboration efficaces dans la lutte mondiale contre le pourriel. La coordination de la législation, de la

réglementation et de leur application revêt une grande importance, mais il ne fait aucun doute à l'heure actuelle qu'une approche plus large s'impose à l'échelle internationale. De nombreux pays reconnaissent maintenant qu'une approche multiple, de type « boîte à outils », et mettant à contribution différents intervenants, approche similaire à celle que le Canada n'a cessé de préconiser, s'avère le mécanisme le plus efficace pour lutter contre le pourriel et résoudre d'autres problèmes en ligne.

Pour cette raison, le Groupe de travail sur le pourriel prône l'élaboration et l'adoption de pratiques exemplaires, afin d'assurer la coordination à l'échelle internationale de la gestion des réseaux et des entreprises de marketing par courriel. Il encourage par ailleurs les FSI, les entreprises de marketing par courriel, les utilisateurs de courriel commercial et les représentants des consommateurs canadiens à participer activement aux efforts déployés sur la scène internationale pour lutter contre le pourriel grâce à des initiatives telles que la mise en place de mécanismes d'authentification et de certification de courriel compatibles dans le monde entier.

Activités du Groupe de travail

Le Groupe de travail sur le pourriel préconise que le gouvernement du Canada et tous les intervenants canadiens participent de façon dynamique et coordonnée à l'élaboration et à la mise en œuvre d'approches bilatérales et multilatérales pour lutter contre le pourriel. À cette fin, ses membres ont pris une part active à plusieurs tribunes internationales importantes.

Collaboration multilatérale

1) Groupe de réflexion de l'Organisation de coopération et de développement économiques (OCDE)

Le Canada participe activement au Groupe de réflexion de l'OCDE sur le « spam », qui a mis au point une boîte à outils reposant sur une approche multiple similaire à celle adoptée par le Canada.

Différents pays ont proposé de diriger l'élaboration d'éléments de la boîte à outils ou d'y participer. Pour sa part, le Canada s'est porté volontaire pour effectuer une analyse comparative des cadres législatifs en place dans le monde. Il a offert également sa contribution à plusieurs autres aspects, notamment l'éducation et la sensibilisation du public, les technologies anti-pourriel ainsi que les mesures chapeautées par le secteur industriel dans la foulée des travaux du Groupe de travail canadien sur le pourriel, y compris les pratiques exemplaires que le Groupe de travail a recommandées à l'intention des FSI et des autres exploitants de réseaux.

2) Plan d'action de Londres

En octobre 2004, les représentants des secteurs public et privé de 15 pays, dont le Canada, se sont réunis à Londres, en Angleterre, pour explorer les moyens d'améliorer la collaboration internationale dans l'application des lois et règlements anti-pourriel. Comme ces différents pays possèdent différents cadres législatifs anti-pourriel, la réunion a permis de regrouper un large éventail d'organismes d'application de la loi qui ne travaillent généralement pas ensemble, notamment les organismes chargés de la protection des données et de la vie privée, de la défense des consommateurs ainsi que de la réglementation de la concurrence et des communications.

De cette réunion est sorti le Plan d'action de Londres sur la coopération internationale relative à l'application des lois anti-pourriel, qui a pour objet de trouver des moyens d'améliorer la collaboration internationale dans la lutte contre le pourriel et la résolution des problèmes connexes.

Ce plan d'action ne remplace pas les accords internationaux déjà conclus entre des organismes d'application de la loi. Le but premier est plutôt d'améliorer la communication entre les différents organismes engagés dans la lutte contre le pourriel. Le Groupe de travail a indiqué qu'il appuierait le Plan d'action de Londres et, par l'intermédiaire d'Industrie Canada, il a participé à sa mise en œuvre. Le Commissariat à la protection de la vie privée du Canada y prend part également.

3) Autres mécanismes de collaboration multilatérale

Le Groupe de travail a participé aux activités de lutte contre le pourriel du Forum de coopération économique Asie-Pacifique, de l'Union internationale des télécommunications et du Sommet mondial sur la société de l'information, y compris les travaux du Groupe de travail sur la gouvernance d'Internet de l'Organisation des Nations Unies.

Le Groupe de travail sur le pourriel a également appuyé les efforts déployés dans le domaine par la Conférence des Nations Unies sur le commerce et le développement, l'Internet Engineering Task Force et le Réseau international de contrôle et de protection des consommateurs.

Par ailleurs, le Groupe de travail sur le pourriel aimerait souligner l'importance du travail que le secteur privé a effectué par l'intermédiaire d'organismes comme l'Alliance technique anti-pourriel, le Messaging Anti-Abuse Working Group et différentes associations du secteur industriel.

Initiatives bilatérales

Le Canada encourage fortement la collaboration internationale pour les besoins de l'élaboration de politiques et de stratégies anti-pourriel en vertu d'accords stratégiques bilatéraux conclus avec des partenaires clés, notamment l'Australie, le Royaume-Uni, les États-Unis, Taiwan et la Commission européenne. Des accords sont déjà conclus avec l'Australie et le Royaume-Uni, et le Groupe de travail prévoit que l'on en conclura d'autres d'ici la fin de 2005 avec les États-Unis, Taiwan et la Commission européenne.

COORDONNER L'ACTION FUTURE

LE DÉFI

Le succès de la mise en œuvre de la stratégie canadienne multiple regroupant divers intervenants, pour lutter contre le pourriel et les menaces connexes, exige une démarche hautement synchronisée et coordonnée en matière de prévention et d'application de la loi. Le Groupe de travail a constaté qu'une communication et une collaboration plus étroites s'imposaient dans le domaine de l'application en particulier, car il y a un grand nombre d'organismes d'application et de réglementation, et que chacun d'eux est partiellement responsable de la lutte anti-pourriel.

L'adoption de l'approche de type « boîte à outils » découle de la complexité du problème du pourriel. Celle-ci ne disparaîtra pas à la fin du mandat du Groupe de travail. On peut s'attendre, à l'avenir, à ce que le gouvernement et les autres intervenants soient confrontés à la même série de questions qui ont mené à la création du Groupe de travail. En voici quelques exemples :

- Des questions se poseront de façon continue sur l'application des lois anti-pourriel, dont celle de la coordination entre les divers organismes et compétences, celle de l'expertise technique requise pour la poursuite des enquêtes et celle de la disponibilité des ressources consacrées à la poursuite des contrevenants.
- Il faudra que les FSI et autres exploitants de réseaux continuent de partager les pratiques exemplaires et les stratégies efficaces, afin de contrer les nouvelles menaces et de mettre au point un système adéquat pour mesurer la portée du problème du pourriel au Canada et l'efficacité des mesures anti-pourriel.

- Les internautes canadiens auront un besoin constant de renseignements fiables et exacts sur les mesures à prendre pour se protéger contre le pourriel et les pratiques trompeuses, nuisibles et frauduleuses connexes. Ils auront également besoin d'un point central et d'un processus simple pour le dépôt des plaintes.
- Le besoin de coordonner la participation des intervenants canadiens dans la lutte internationale contre le pourriel sera constant et s'amplifiera.

Activités du Groupe de travail

Tenant compte de sa propre expérience et de celle des autres pays, le Groupe de travail sur le pourriel a conclu que, pour relever avec succès les défis que pose le pourriel, le gouvernement du Canada devrait établir ou désigner un point central ou centre, qui mènerait la lutte contre le pourriel et les menaces connexes. Ce centre devrait assumer deux principales fonctions : la supervision et la coordination des politiques et un appui aux organismes d'application de la loi.

Pour être un centre efficace en matière d'élaboration et de coordination des politiques, le Groupe de travail est d'avis que ce dernier devrait recevoir un mandat et des ressources lui permettant de :

- formuler des politiques visant à traiter le problème du pourriel et les menaces connexes, notamment par le suivi et l'analyse des questions et la consultation régulière des principaux intervenants;

En conséquence, nos recommandations sont les suivantes :

Recommandation 21 :

Afin de poursuivre la démarche multiple, de type « boîte à outils » et regroupant divers intervenants formulée par le Groupe de travail sur le pourriel et de fournir un point central pour faciliter la mise en œuvre de ses recommandations, le gouvernement devrait établir un centre relevant du ministre de l'Industrie, qui assumerait la supervision et la coordination des politiques, l'éducation et la sensibilisation du public et fournirait un appui aux organismes d'application des lois.

Recommandation 22 :

Le gouvernement fédéral, par le truchement de cet organisme de coordination, devrait surveiller les répercussions de la mise en œuvre des recommandations du Groupe de travail, évaluer les résultats, faire rapport régulièrement au public et, en consultation avec les intervenants, prendre toutes les mesures supplémentaires requises pour lutter contre le pourriel.

Technologies et gestion de réseaux

Coprésidents

Tom Copeland, président, Association canadienne des fournisseurs Internet
Lori Assheton-Smith, première vice-présidente et avocate, Association canadienne de télévision par câble

Organisations membres

Agence canadienne d'enregistrement Internet
Allstream
AOL Canada
Association canadienne des télécommunications sans fil
Bell Canada
BorderWare Technologies Inc.
CANARIE Inc.
CipherTrust
Coalition canadienne contre le pourriel
Cogeco Câble inc.
Delta Cable Communications
easyDNS Technologies Inc.
E-Gate Communications Inc.
Groupe Télécom
Interlink Connectivity
Internet Light and Power
Internet Research Task Force Anti-Spam Research Group
Le groupe interstructure
LinuxMagic
MessageLabs Americas
Microsoft Canada
Nortel Networks
PhoneBusters
Rogers Communications Inc.
Secteur de l'agent principal de l'information, Industrie Canada
Secteur du spectre, des technologies de l'information et des télécommunications, Industrie Canada
SecuritySage Inc.
Shaw Communications Inc.
Spamhaus
TELUS Communications Inc.
Université de la Colombie-Britannique
Université du Manitoba
Vidéotron Télécom ltée
Vircom inc.

Collaboration internationale

Coprésidents

Bernard Courtois, président, Association canadienne de la technologie de l'information
Michael Geist, titulaire de la Chaire de recherche du Canada en droit d'Internet et du commerce électronique, Université d'Ottawa

Organisations membres

Bell Canada
Bureau de la concurrence
Chambre de commerce du Canada
Commission européenne
LinuxMagic
Microsoft Canada
Ministère des Communications, de la Technologie de l'information et des Arts d'Australie
Ministère du Commerce et de l'Industrie du Royaume-Uni
Organisation de coopération et de développement économiques
Secteur du spectre, des technologies de l'information et des télécommunications, Industrie Canada

Secrétariat du Groupe de travail

Secteur du Spectre, des technologies de l'information et des télécommunications, Industrie Canada

Richard Simpson, directeur général, Direction générale sur le commerce électronique
Shari Scott, directrice, Direction générale sur le commerce électronique
David Charter, Direction générale sur le commerce électronique
Gérard Desroches, Direction générale sur le commerce électronique
Peter Ferguson, Direction générale sur le commerce électronique
Lisa Foley, Direction générale sur le commerce électronique
Angie Forte, Direction générale sur le commerce électronique
Jennifer Kealey, Direction générale sur le commerce électronique
Serge Presseau, Direction générale sur le commerce électronique
Howard Chatterton, Services techniques d'homologation et de télécommunications
David Gibson, Services techniques d'homologation et de télécommunications

Don MacLean, auteur du rapport, MacLean Consulting
John Levine, auteur du glossaire et réviseur technique

APPENDICE B

PRATIQUES EXEMPLAIRES RECOMMANDÉES POUR LES FOURNISSEURS DE SERVICE INTERNET ET LES AUTRES EXPLOITANTS DE RÉSEAUX



Contexte

En août 2004, le Sous-groupe sur les technologies et la gestion de 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'Anti-Spam Technical Alliance (ASTA) et du Messaging Anti-Abuse Working Group (MAAWG), ainsi que ceux de plusieurs associations du secteur d'activités. Un certain nombre de fournisseurs de service Internet (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 industriel 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 à facettes multiples plus vaste visant à le régler.

Intention

Les pratiques exemplaires en matière de lutte anti-pourriel recommandées au secteur industriel 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, et 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.

Actuellement, certains fournisseurs se restreignent quant à la limitation de la quantité de courriels expédiés. 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 informaticiens 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 les technologies et la gestion de 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, celui 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 courriels 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 de courriel.

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 courriels 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 courriels 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.

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 courriel 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 courriels 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.

APPENDICE C

PRATIQUES EXEMPLAIRES RECOMMANDÉES POUR LE MARKETING PAR COURRIEL



Contexte

Le Groupe de travail sur le pourriel du gouvernement fédéral a mis sur pied le Sous-groupe sur la validation du courriel commercial chargé d'élaborer une série de pratiques exemplaires pour le marketing par courriel. Ces pratiques exemplaires encourageront les organismes canadiens à adopter des techniques de marketing anti-pourriel et renforceront le fait que le pourriel n'a aucun rôle légitime à jouer dans le marketing canadien.

La majorité des organismes responsables respectent déjà les codes du secteur industriel ou ont adopté des pratiques exemplaires. Au Canada, les organismes observent le *Code de déontologie et les Normes de pratiques* de l'Association canadienne du marketing. Ce document renferme des lignes directrices s'appliquant au marketing par courriel et à la collecte en ligne de données pour le marketing. Les membres des organismes faisant partie du Conseil canadien de la recherche par sondage, qui mènent des sondages en ligne, sont également en train d'élaborer un code de pratique uniforme.

Le présent document regroupe une liste de pratiques exemplaires fondées sur les codes actuels, destinées à servir de fondement à l'usage du courriel à des fins commerciales ou de marketing.

Les fournisseurs de services Internet et les fournisseurs de services de courriel utilisent de plus en plus souvent les filtres et les listes blanches et noires pour bloquer le pourriel, mais ce faisant, ils empêchent les courriels légitimes d'atteindre leurs destinataires. Les organismes sont encouragés à adopter les pratiques exemplaires énoncées ci-dessous pour s'assurer que leurs courriels légitimes atteignent les destinataires prévus.

Ces pratiques exemplaires ne sont pas juridiquement contraignantes, mais elles sont un complément aux lois canadiennes actuelles régissant le pourriel, la protection des renseignements personnels, le marketing par courriel et le marketing auprès des enfants. À titre d'exemple, la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), entrée en vigueur au Canada en janvier 2004, énonce les obligations des personnes qui recueillent, utilisent et communiquent les adresses de courriel personnelles. D'autres lois fédérales, notamment la *Loi sur la concurrence*, la *Loi sur les télécommunications* et le *Code criminel*, sont pertinentes. Les organismes devraient se familiariser avec ces lois et régir leurs activités en conséquence.

Les pratiques exemplaires, accompagnées de notes explicatives et d'exemples, sont décrites dans les pages suivantes.

Pratiques exemplaires recommandées

1. Les courriels de marketing devraient être envoyés uniquement aux destinataires qui ont consenti à recevoir les renseignements.

Cette pratique exemplaire est directement liée à l'envoi de courriels commerciaux non sollicités pour offrir des biens ou des services. Les organismes qui n'ont pas obtenu le consentement explicite des destinataires avant d'envoyer ce type de courriels envoient du pourriel.

Un organisme peut, pour ses relations d'affaires existantes (voir le glossaire), se fier au consentement implicite. En vertu de la loi canadienne actuelle, l'organisme possède le consentement implicite d'une personne pour lui envoyer un courriel lorsque celle-ci a participé à un concours, a fait un don, s'est enregistrée en ligne pour obtenir un produit ou un bulletin; a fourni son adresse de courriel suite à

une transaction; avait l'option de se retirer de l'envoi de futurs courriels mais a omis de le faire. En utilisant cette forme de consentement, l'entreprise de marketing devrait expliquer au destinataire visé pourquoi il reçoit le courriel en question. Au cours des communications de suivi, l'organisme devra fournir au destinataire l'option de se retirer de l'envoi futur de courriels de marketing (voir la pratique exemplaire 2).

Les organismes ne devraient pas envoyer des courriels de marketing aux destinataires qui ont indiqué qu'ils ne voulaient pas recevoir de courriels de leur part. Bien qu'un organisme puisse envoyer des courriels durant une relation commerciale active, il doit en tout temps respecter la volonté des personnes qui ont demandé d'être retirées des listes d'envoi de courriels de marketing. L'inclusion d'une option de retrait dans chaque message envoyé peut servir à cette fin (voir la pratique exemplaire 2).

L'envoi de courriels en dehors d'une relation d'affaires courante, ou si le dossier d'un client est devenu inactif, est justifié uniquement si l'organisme a des renseignements sur le service, la garantie ou la mise à jour d'un produit ou si l'achat d'un produit soulève des questions de santé et de sécurité. Cependant, il doit agir avec discrétion car toute tentative de vente de gamme supérieure ou de vente croisée pourrait porter ses clients à considérer le message comme du pourriel.

2. Les courriels de marketing doivent fournir aux destinataires un moyen évident, clair et efficace de refuser, par courriel ou Internet, de recevoir d'autres courriels d'affaires et/ou de marketing de l'organisme.

Tous les courriels envoyés aux clients doivent comporter une option de retrait. Cette option ne doit pas être cachée dans le courriel et doit, au minimum, être accessible dans un site Web ou par courriel. Le message devrait être aussi simple que celui-ci : « Si vous ne voulez plus recevoir d'offres promotionnelles de cet organisme, veuillez **cliquer ici** ou envoyer un courriel à **info@societeABC.com**. »

La procédure de retrait devrait être simple et explicite, et les organismes devraient confirmer par courriel que le retrait est ou sera respecté sans nouvelle démarche de la part du consommateur.

Au Canada, la pratique exemplaire du secteur industriel relativement aux fichiers téléphoniques ou de courrier « ne pas contacter » énonce que les demandes de retrait sont respectées pendant trois ans. Après ce délai, les organismes peuvent recommencer à présenter des offres de marketing aux particuliers. Cependant, à cause de la nature sensible des communications par courriel et des problèmes dus au pourriel, les organismes devraient considérer une demande de retrait comme finale et retirer le demandeur de leurs listes de marketing jusqu'à ce que celui-ci exprime sa volonté de recommencer à recevoir des courriels.

3. Le processus interne utilisé pour obtenir le consentement devrait être clair et transparent. Les organismes devraient conserver un dossier des types de demandes reçues des destinataires, afin de pouvoir mettre leurs listes d'envois de courriels à jour avant les campagnes de publicité.

Les organismes devraient s'assurer qu'ils ont les moyens de respecter les demandes de retrait en temps voulu et mettre leurs listes à jour en conséquence.

De plus, les organismes devraient mettre en place une procédure interne d'enregistrement des preuves de consentement, notamment la date, l'heure, l'adresse de protocole Internet (IP) d'origine et l'emplacement (y compris l'URL) où l'adresse a été recueillie ainsi que le mode d'obtention du consentement s'il est différent (par exemple, carte d'affaires, formulaire de concours, téléphone, communication verbale ou carte de crédit [par exemple, par l'entremise d'un abonnement payant à une liste]). Les organismes devraient pouvoir fournir ces renseignements à un destinataire sur demande.

4. Chaque communication de marketing par courriel devrait clairement identifier l'expéditeur du courriel. La ligne de mention objet et le corps du texte devraient refléter correctement le contenu, l'origine et le but de la communication.

Le nom de l'expéditeur et la source du courriel devraient être clairement indiqués et mis en évidence et, dans la mesure du possible, placés au-dessus du pli (partie du courriel visible sans défilement).

Exemple 1 : Courriel envoyé directement d'un organisme à un abonné

Date : mardi, 5 oct. 2004 07:32:02 -0400
De : Bell Canada – Facture électronique <facture.presentation@bell.ca>
À : JOE CONSOMMATEUR <joe@consommateur.ca>
Objet : Votre facture électronique Bell est prête / Your Bell e-bill is ready

Exemple 2 : Courriel d'un tiers fournisseur de courriel au nom d'un organisme

De : PUBLICATIONS peteMOSS <bounces@peteMOSS.com>
<v2user-13990-IXoyuP.CahrNet_0bkttg@mailier.whitehat.com>
Sujet : spamNews 07/21/04
À : <joe@consommateur.ca>
Date : Sam. 24 juil. 2004 18:50:17 -0700

Même si le contenu correspond à la ligne de mention objet, les organismes doivent éviter d'utiliser les termes « offres gratuites » ou « prix à gagner » et ce, parce que certains filtres anti-pourriel utilisent ce genre de mot-clé pour signaler un pourriel.

Les courriels devraient inclure l'adresse postale principale de l'expéditeur. Les organismes canadiens sont fortement encouragés à se familiariser avec les dispositions des lois canadiennes à ce sujet et les lois connexes des autres compétences, notamment de l'Australie, des États-Unis et de l'Union européenne.

5. Tout courriel devrait fournir un lien vers la politique de l'expéditeur sur les renseignements personnels. Celle-ci devrait expliquer le mode d'utilisation et de communication des renseignements personnels pouvant être recueillis par le biais du parcours de l'utilisateur ou d'autres techniques de surveillance des sites Web.

En vertu de la LPRPDE, les organismes doivent faire preuve de beaucoup de transparence lorsqu'ils communiquent leurs pratiques de collecte et de traitement des renseignements personnels. Une politique sur la protection des renseignements personnels pourrait articuler la politique de l'organisme concernant le genre de renseignements recueillis et/ou utilisés, la communication des renseignements à des tiers, l'usage de mouchards (« cookies », en anglais) ou autres mesures passives de collecte de données et les procédures de sécurité, de responsabilité et d'application.

Les organismes doivent afficher leur politique complète sur la protection des renseignements personnels bien en évidence sur leur site Web, laquelle explique leurs procédures à l'égard de la collecte de renseignements en ligne. La politique devrait également inclure un lien actif vers un mécanisme d'option de retrait.

6. Les entreprises de marketing, les courtiers et les propriétaires de listes d'adresses devraient prendre des mesures raisonnables pour s'assurer que les personnes dont l'adresse figure sur leurs listes de diffusion ont donné le consentement approprié.

Les organismes, les courtiers et les propriétaires de listes d'adresses devraient assumer la responsabilité conjointe des envois de courriels aux destinataires qui n'ont pas fourni un consentement approprié. L'organisme, le courtier ou le propriétaire de listes d'adresses qui sait ou aurait dû savoir que le consentement approprié n'a pas été obtenu devrait être tenu responsable. Voici quelques mesures raisonnables qu'un organisme peut adopter pour s'assurer que ses listes sont correctes :

- consulter la politique en matière de protection des renseignements personnels du courtier ou propriétaire de la liste;
- examiner les procédures d'inclusion utilisées pour obtenir les adresses de courriel;
- demander au courtier ou au propriétaire de signer un contrat garantissant qu'il s'est conformé aux exigences de la LPRPDE (voir l'exemple de lettre à la fin du présent appendice).

7. Les entreprises de marketing qui font du marketing par courriel auprès des personnes mineures devraient faire preuve de discrétion et de sensibilité et tenir compte de l'âge, des connaissances, du caractère averti et de la maturité de cet auditoire.

Les organismes devraient consulter les Considérations spéciales se rapportant au marketing destiné aux enfants et aux adolescents, énoncées dans le *Code de déontologie et les Normes de pratiques* de l'Association canadienne du marketing (www.the-cma.org/consumer/ethics.cfm), ainsi qu'aux lois canadiennes (voir www.justice.gc.ca) pour obtenir des directives.

La façon dont les mineurs perçoivent les courriels de marketing et y réagissent est fonction de leur âge, de leur expérience et du contexte du message. Par exemple, le marketing approprié aux adolescents ne convient pas nécessairement aux enfants. En outre, on ne peut savoir avec certitude l'âge d'une personne qui s'inscrit à une liste de diffusion de courriels. Par conséquent, les organismes devraient faire preuve de discrétion et de sensibilité lorsqu'ils font du marketing auprès des mineurs et tenter d'obtenir l'autorisation des parents pour envoyer ce type de communication.

8. a) Lorsque le contenu d'un courriel est destiné à des adultes, l'expéditeur devrait, avant de l'envoyer, vérifier si le destinataire est en âge de recevoir et de consulter légalement ce contenu.

Le contenu destiné aux adultes inclut le matériel de nature sexuellement explicite et le matériel portant sur les jeux de hasard, le tabac, l'alcool, les armes à feu et autres armes.

b) Tout courriel renfermant un contenu sexuellement explicite devrait inclure la balise de préface « SEXUELLEMENT EXPLICITE » dans la ligne de mention objet.

On pourrait demander par exemple au récipiendaire de fournir un numéro de téléphone pour que l'organisme puisse vérifier s'il a l'âge de la majorité. Il importe de noter que les contrats mettant en cause des mineurs ne sont pas applicables.

9. Les organismes devraient mettre en place un système de traitement des plaintes juste, efficace, confidentiel et facile à utiliser.

Toutes les plaintes des particuliers concernant l'usage de leur adresse de courriel devraient être traitées avec courtoisie et dans un délai raisonnable.

10. Les organismes peuvent divulguer les adresses de courriel de leurs clients à des tiers affiliés ou au sein d'une famille de sociétés si :

- ils ont obtenu leur consentement;
- ils utilisent les adresses aux fins pour lesquelles ils les ont recueillies (c'est-à-dire pour un marketing relié à l'achat original ou à la prestation de services associés à cet achat);
- les destinataires savent pourquoi ils reçoivent des courriels;
- il y a un moyen facile de refuser de recevoir davantage de courriels.

Les organismes peuvent divulguer l'adresse de courriel de leurs clients à un tiers affilié ou au sein d'une famille de sociétés à des fins de marketing croisé seulement s'ils offrent à ces clients un moyen facile de refuser de recevoir d'autres courriels de marketing avant de divulguer leur adresse de courriel.

Le motif des offres de marketing additionnelles reliées (par exemple portant la marque d'une société) devrait être évident pour les clients. L'organisme ne devrait pas présumer que les clients comprennent une relation ou une structure organisationnelle.

Pour obtenir d'autres directives, les organismes sont encouragés à consulter les pratiques exemplaires énoncées dans le *Code de déontologie et Normes de pratique*, à la section E4.1.3 du *Guide de conformité de l'ACM sur les communications de marketing électronique*, de l'Association canadienne du marketing (ACM). La section énonce qu'une entreprise ne peut divulguer l'adresse de courriel d'un particulier à une tierce partie (par exemple société de location de listes) sans d'abord obtenir le consentement explicite (ou demande d'adhésion ou consentement positif) du particulier. Pour divulguer des adresses de courriel à des partenaires de marketing ou à des courtiers de listes d'adresses, la société doit obtenir un consentement positif. De même, elle doit obtenir une autorisation appropriée pour utiliser les adresses de courriel qu'elle a obtenues d'autres parties.

L'ACM définit le terme « tierces parties » comme suit :

« Le terme "tierce partie" fait référence à un organisme distinct de celui avec lequel le client a originellement fait affaire (société de location de listes), y compris un organisme associé à l'organisme original (ou société de bienfaisance) ou faisant partie du groupe, mais dont la relation n'est pas évidente pour le client. Les tiers ne comprennent pas les organismes de traitement des données agissant au nom de l'organisme avec lequel le particulier a établi une relation d'affaires. »

Conseils techniques pour les entreprises de marketing électronique

1. Les expéditeurs devraient mettre en œuvre les spécifications techniques standard suivantes :

- Tous les serveurs (par exemple entrée, sortie, sites Web) doivent avoir des pointeurs de système de noms de domaine (DNS) inverse — rDNS PTR — dans les fichiers DNS; les outils de recherche avant et inverse de l'hôte doivent correspondre et les appareils d'envoi doivent utiliser ce nom pour la commande HELO/EHLO.
- Les fichiers Sender Policy Framework (SPF) (par exemple <http://spf.pobox.com>) et clef de domaine (domain-key) (par exemple <http://antispam.yahoo.com/domainkeys>) devraient être publiés par les expéditeurs et les sites tierces parties associés à un envoi (par exemple sites Web, processeurs de services prolongés, etc.) et tenus à jour en tout temps. On devrait envisager l'adoption de technologies semblables à mesure qu'elles sont mises au point et sont normalisées.
- Les adresses IP distinctes des autres serveurs de site devraient être assignées aux serveurs de courriel sortant.
- Les fichiers des domaines d'expéditeur de la base de données WHOIS doivent toujours être exacts et complets.
- Les noms de famille (par exemple postmaster@ et abuse@) doivent être fonctionnels et activement surveillés pour tous les domaines d'expéditeur, y compris les sites Web, mentionnés dans le contenu du courriel.

2. Les expéditeurs doivent traiter les messages de non-livraison comme suit :

- Ils doivent promptement retirer les adresses « hard » générant un message de non-livraison permanente (5xx : Utilisateur non existant / boîte aux lettres non disponible, etc.) des listes qu'ils contrôlent lorsque le nombre total de refus excède 3, en 14 jours. Si une non-livraison permanente indique un blocage de pourriel, ils peuvent réactiver l'adresse en retirant le blocage de pourriel.
- Ils doivent retirer les adresses « soft » générant un message de non-livraison temporaire (4xx : Échecs isolés) lorsque le nombre total de refus est supérieur à 5 lors de campagnes consécutives à partir d'une seule liste ou totalise 5 à partir de plusieurs listes en 10 jours.

Les politiques de traitement des messages de non-livraison sont expliquées en détails sur les sites suivants :

- <http://help.yahoo.com/help/us/mail/defer>
- www.isipp.com/standards.php
- <http://postmaster.info.aol.com/guidelines/bestprac.html>

3. Les pixels espions (éléments en HTML cachés) et les avis de réception sont des façons inexactes de déterminer les statistiques de taux d'ouverture des envois des campagnes. Les expéditeurs sont vivement encouragés à cesser de les utiliser et à adopter d'autres mesures de la performance.

Les pixels espions sont des mesures de l'efficacité des campagnes de marketing par courriel extrêmement inexactes et leur usage est déconseillé.

Les pixels espions ne sont plus fiables pour plusieurs raisons, mais surtout à cause des changements techniques apportés aux principaux logiciels d'envoi de courriel (par exemple dans le cadre de ses mesures de sécurité anti-virus, Outlook ne les téléchargera plus par défaut et ne les affichera pas dans le panneau de prévisualisation). De plus, les clients utilisent de plus en plus souvent un logiciel anti-virus qui, par défaut, interdit le téléchargement des pixels espions.

On déconseille également le recours aux éléments d'images d'un pixel sur un pixel, blanc sur blanc pour mesurer les taux d'ouverture. On recommande plutôt d'utiliser les parcours des usagers sur des adresses URL codées, enchâssées et d'autres méthodes de mesure des actions des abonnés (par exemple rendement des investissements, actes d'achat).

Les expéditeurs qui entendent utiliser les pixels espions devraient se familiariser avec les implications pour la vie privée soulevées, notamment, dans l'étude publiée par la Network Advertising Initiative (www.networkadvertising.org/Web_Beacons_11-1-04.pdf) et respecter les modalités qui y sont énoncées.

À l'heure actuelle, la rétention des abonnés — soit le nombre de personnes qui continuent de s'abonner après chaque courriel — est une des mesures les plus utiles pour évaluer la réussite d'un programme de courriels. Clairement, l'objectif est de ne pas avoir de désabonnements, ce qui indiquerait que l'organisme fournit un contenu en temps voulu, pertinent et apprécié. À leur tour, ces avantages fidéliseront la clientèle et gagneront sa confiance — un atout pour n'importe quel organisme.

Exemple de lettre de conformité à la *Loi sur la protection des renseignements personnels et les documents électroniques*

Nom de la liste : _____

En qualité de chef de file des services de publipostage, la **SociétéABC** est fière de son engagement à l'égard de la protection de la vie privée des consommateurs et de la conformité aux lois applicables, notamment à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). Par conséquent, nous profitons de l'occasion pour mettre à jour les renseignements que nous avons au sujet de la liste susmentionnée.

Un examen de la LPRPDE et du respect de la vie privée des consommateurs

La LPRPDE porte uniquement sur les dossiers des consommateurs (destinés à une adresse domiciliaire). La loi affirme, entre autres choses, que les consommateurs inscrits sur une liste doivent avoir consenti à la collecte de leurs renseignements personnels et à leur communication à des tiers à des fins de marketing ou de communication. En outre, en vertu de la loi, les options de retrait offertes aux consommateurs doivent être mises en vigueur avant que leur nom soit communiqué à des fins de marketing.

Ce dont nous avons besoin

Il arrive de plus en plus souvent que les expéditeurs demandent des renseignements à propos des messages de confidentialité utilisés par les propriétaires de listes. Nous devons conserver les renseignements suivants dans nos dossiers pour assurer l'expédition rapide des commandes.

Veuillez fournir un spécimen du formulaire de consentement ou de retrait que vous utilisez présentement. Nous en conserverons un exemplaire dans nos dossiers à titre de référence aux fins d'usage éventuel et répété de cette liste.

Veuillez cocher une des cases ci-après, puis signer, dater et renvoyer ce document à l'attention de la **SociétéABC** au numéro de télécopieur (XXX) XXX-XXXX. Veuillez communiquer avec notre département des XXXXXXXXXX au (XXX) XXX-XXXX ou à **info@societeABC.com** si vous avez des questions.

Je garantis et je fais valoir que cette liste EST CONFORME à la LPRPDE. Mon organisation a obtenu le consentement de tous les consommateurs inscrits sur cette liste pour recueillir leurs renseignements personnels et les communiquer à des tiers à des fins de marketing ou de communication, et a veillé à ce que les options de retrait soient mises à la disposition des consommateurs avant que leur nom ne soit communiqué à des fins de marketing. Mon organisme observera toutes les lois provinciales ou fédérales portant sur la protection des renseignements personnels pouvant entrer en vigueur à compter d'aujourd'hui, dans la mesure où elles s'appliquent aux renseignements personnels recueillis, utilisés ou communiqués par lui.

Je garantis et fais valoir que cette liste N'EST PAS CONFORME à la LPRPDE. Mon organisme n'a pas obtenu le consentement de tous les consommateurs inscrits sur cette liste pour recueillir leurs renseignements personnels et les communiquer à des tiers à des fins de marketing ou de communication, et/ou n'a pas veillé à ce que les options de retrait soient mises à la disposition des consommateurs avant que leur nom ne soit communiqué à des fins de marketing.



APPENDICE D

TROIS CONSEILS IMPORTANTS POUR LUTTER CONTRE LE POURRIEL

Les pourriels sont des courriels non sollicités, généralement de nature commerciale, annonçant un produit ou un service, qui diffusés massivement à des milliers d'adresses de courriel à la fois, inondent les boîtes de réception. Il ne s'agit pas d'un courriel commercial légitime auquel le consommateur a consenti. Le pourriel est souvent un véhicule pour la fraude, les virus et les documents à contenu offensant.

Le pourriel est un problème d'envergure qui fait perdre beaucoup de temps et d'argent aux consommateurs, aux entreprises et au gouvernement. Chacun doit faire sa part pour se protéger et protéger les autres du pourriel. Le **Groupe de travail canadien sur le pourriel** a formulé trois conseils pour vous aider à vous protéger et à lutter contre le pourriel.



Arrêtez le pourriel ici : trois conseils clés

1. Protégez votre ordinateur

Le pourriel est une source croissante de virus informatiques. Il est essentiel que vous protégiez votre ordinateur contre les messages transportant des virus. Installez un logiciel anti-virus et anti-pourriel et mettez-le à jour régulièrement. Procurez-vous aussi la protection supplémentaire d'un coupe-feu.

2. Protégez votre adresse de courriel

Réservez une adresse de courriel pour les contacts personnels et professionnels en qui vous avez confiance. Créez une adresse de courriel extensible distincte pour d'autres utilisations en ligne.

3. Protégez-vous

N'essayez rien, n'achetez rien et ne répondez pas aux pourriels. Supprimez-les. C'est une bonne façon de ne pas en recevoir d'autres dans l'avenir.

1. Protégez votre ordinateur

Protégez votre ordinateur avec des logiciels anti-pourriel et anti-virus et autres logiciels de protection.

Les logiciels anti-pourriel peuvent vérifier automatiquement vos courriels pour détecter les pourriels avant qu'ils ne parviennent à votre boîte de réception, et les envoient à la poubelle. Vous ou un membre de votre famille ne risquez donc plus d'ouvrir accidentellement un pourriel, et vous pouvez gérer vos courriels de façon plus efficace.

Pour vous protéger contre les pourriels et les pièces jointes contenant des virus, installez des correctifs de sécurité et des programmes anti-virus dans votre système d'exploitation et mettez-les à jour régulièrement.

Un coupe-feu procure une protection supplémentaire contre le piratage informatique et protège vos renseignements personnels.

N'entrez jamais en ligne sur un ordinateur non protégé contre les pourriels et les virus et dépourvu de coupe-feu.

Vérifiez toujours la source.

N'ouvrez jamais de pièce jointe, sauf si vous en attendez d'une personne sûre. Un polluposte peut s'emparer du compte courriel d'un particulier ou d'une entreprise (processus appelé « mystification ») pour transmettre un virus à votre ordinateur. Si vous avez des soupçons au sujet d'une pièce jointe, vérifiez sa provenance auprès de l'expéditeur avant de l'ouvrir.

Ne mordez pas à l'hameçon d'un polluposteur. Protégez vos données personnelles.

Un polluposteur peut s'emparer de vos données personnelles en pratiquant « l'hameçonnage » (pêche aux données personnelles). Voici comment. Vous recevez un courriel provenant d'une source fiable avec qui vous faites affaire, comme une banque ou une cyberentreprise. Souvent, ce courriel prétend que vous devez absolument fournir des données personnelles, comme votre nom d'utilisateur, votre mot de passe et même le numéro de vos cartes de crédit. Il arrive aussi qu'on menace de bloquer votre compte si vous ne fournissez pas ces renseignements. Le lien Web qui est alors indiqué vous dirige vers un faux site bien imité. Sachez qu'une entreprise ne communique JAMAIS de cette manière avec ses clients. Si vous avez des soupçons, appelez l'entreprise concernée pour vérifier si le courriel est légitime. Ne répondez jamais à ce genre de courriel et n'entrez pas dans un site par le lien inclus dans un pourriel que vous soupçonnez de pratiquer l'hameçonnage. Si un site Web vous intéresse, consultez-le directement à l'aide d'un navigateur Web.

APPENDICE E

RAPPORTS COMPLÉMENTAIRES ET DOCUMENTS DE TRAVAIL

Les documents suivants présentent de la documentation complémentaire sur les travaux du Groupe de travail sur le pourriel et les conclusions des sous-groupes. On peut consulter ces documents à l'adresse : **www.e-com.ic.gc.ca**.

Ouvrages généraux

- Sommaire des commentaires reçus, Avis publié dans la *Gazette du Canada* concernant le *Plan d'action anti-pourriel pour le Canada*
- Groupe de travail sur le pourriel : Table ronde des intervenants clés
- Sommaire des contributions au Forum en ligne de consultation publique du Groupe de travail sur le pourriel

Documents des sous-groupes

- Aperçu des technologies anti-pourriel
- Document de conception de la Base de données canadienne sur les pourriels
- Document d'accompagnement des *Pratiques exemplaires recommandées pour les fournisseurs de services Internet et autres exploitants de réseaux*
- Conclusions du Sous-groupe de travail sur l'examen de la législation et son application

Documents d'information

- Un droit privé d'action prévu par la loi contre les polluposteurs au Canada
- Évaluation de la certification du courriel
- Vue d'ensemble du problème du pourriel acheminé sur les appareils sans fil au Canada
- Propositions concernant le Centre canadien de lutte contre le pourriel
- Comparaison internationale des mesures anti-pourriel



GLOSSAIRE

Adresse de courriel (*Email address*)

Nom identifiant l'expéditeur ou le destinataire d'un courriel. L'adresse prend la forme de **boiteauxlettres@dom.ain**, où **dom.ain** est un nom de domaine consultable dans le DNS, et **boiteauxlettres** est un identifiant arbitraire utilisé par le gestionnaire du domaine pour identifier un internaute.

Adresse IP (*IP address*)

Adresse numérique utilisée pour identifier de manière unique un ordinateur ou autre appareil connecté à Internet. Une adresse IP se compose d'habitude d'une série de quatre nombres décimaux séparés par des points, comme 168.0.1.10.

Adresse URL (*URL*)

Chaîne de caractères normalisés servant à identifier une page Web ou une autre ressource en ligne. Prend habituellement la forme **http://www.mondomaine.ca/unepage**.

Attaque de dictionnaire (*Dictionary attack*)

Technique servant à deviner les adresses de courriel. L'arnaqueur essaie de livrer du courriel à un grand nombre d'adresses fictives, utilisant des termes tirés d'un dictionnaire ou des combinaisons de lettres, par exemple **aaaa@exemple.ca**, **aaab@exemple.ca**, ou **zzzz@exemple.ca**.

Attaque par déni de service (*Denial of service attack - DoS ou DOS*)

Attaque informatique destinée à empêcher un serveur ou réseau d'opérer en noyant son trafic. Par exemple, un arnaqueur pourrait envoyer des milliers de courriels à un serveur de courrier, dans le but de le submerger et de l'empêcher de distribuer les courriels. Les attaques peuvent frapper les serveurs de courrier, les serveurs Web, les serveurs DNS et les routeurs de réseaux. Le pourriel en vrac peut causer une attaque par déni de service.

Base de données WHOIS (*WHOIS*)

Service Internet utilisé pour demander des renseignements sur les domaines et les réseaux d'Internet. N'a pas été universellement mise en œuvre.

Blocage du port 25 (*Port 25 blocking*)

Théoriquement, chaque ordinateur sur Internet a la capacité technique d'envoyer du courrier à un autre ordinateur. En pratique, la majorité des internautes envoient leur courriel au destinataire final par l'entremise du serveur de leur FSI. Ces dernières années, la majorité du courrier envoyé directement (plutôt que par un FSI) a été du pourriel et des virus. Bon nombre de FSI empêchent maintenant leurs clients d'envoyer leur courrier directement, exigeant que celui-ci soit acheminé par le truchement de leur serveur où ils peuvent filtrer les virus et prendre d'autres mesures contre les abus. Comme le protocole de contrôle de transmission (TCP) attribue un numéro de port à chaque service, et que le courriel est expédié par le port 25, les FSI procèdent ainsi au blocage du port 25.

Le blocage du port 25 pour les usagers du réseau commuté et les abonnés à large bande constitue une pratique exemplaire.

Cheval de Troie (*Trojan Horse*)

Programme qui, en plus de sa fonction nominale, accomplit secrètement une deuxième fonction.

Clefs de domaine (*Domain keys*)

Technologie proposée par Yahoo!® qui ajoute aux messages une signature cryptographique identifiable par les destinataires. Elle permet de vérifier si le message provient du domaine de l'expéditeur du courriel et s'il a été modifié en transit.

Collecte (*Harvesting*)

Abrégé de « collecte d'adresses »

Collecte d'adresses (*Address harvesting*)

Action de recueillir des adresses de courriel automatiquement à partir de sites Web et d'autres sources en ligne.

Compte fonctionnel (*Role account*)

Compte de courriel devant être établi et maintenu par tous les secteurs ayant une connectivité Internet, conformément à la série de documents Request for Comments (RFC) de l'Internet Engineering Task Force (IETF). De tels comptes comprennent **postmaster@sampledomain.ca**, **abuse@sampledomain.ca** et **hostmaster@sampledomain.ca**.

Consentement actif (*Opt-in*)

Également appelé « consentement explicite » ou « positif ». Selon cette forme de consentement, que l'on appelle généralement le « consentement explicite », l'organisme offre à la personne concernée la possibilité d'accepter l'utilisation proposée. À moins que la personne ne prenne des mesures pour consentir à l'utilisation prévue – en d'autres mots, dire « oui » – l'organisme ne présumera pas que le consentement a été donné. (Source : Fiche d'information du Commissariat à la protection de la vie privée du Canada)

Consentement implicite (*Implied consent*)

Selon le Code type sur la protection des renseignements personnels de l'Association canadienne de normalisation, « le consentement implicite survient lorsque les actes ou l'inaction de la personne permettent raisonnablement de déduire qu'il y a consentement ». Cela comprend les situations où l'utilisation ou la communication prévue est évidente compte tenu du contexte, et où l'organisme peut présumer avec peu ou pas de risque que la personne, en fournissant les renseignements personnels, est consciente de l'utilisation ou de la communication prévue et y consent. (Source : Fiche d'information du Commissariat à la protection de la vie privée du Canada)

Courriel de marketing (*Marketing email*)

Courriel principalement destiné à annoncer la disponibilité de produits ou services. Comparer avec « courriel transactionnel ».

Courriel transactionnel (*Transactional email*)

Courriel contenant des renseignements sur des transactions commerciales courantes ou antérieures, notamment confirmation d'une vente, numéro d'enregistrement, facture ou confirmation de consentement actif ou de refus. Comparer avec « courriel de marketing ».

Défaillance passagère (*Transient failure*)

Brève défectuosité survenant de façon irrégulière et imprévue.

DNS

Système de noms de domaine, le système qui permet aux utilisateurs de localiser les ordinateurs sur Internet au moyen des noms de domaine. Les serveurs DNS maintiennent une base de données des noms de domaine (c'est-à-dire noms de l'hôte) et de leurs adresses IP correspondantes. Par exemple, si le nom **www.macompagnie.ca** était présenté à un serveur DNS, l'adresse IP 204.0.8.51 pourrait être retournée. Le DNS inclut plusieurs types de données, notamment les fichiers A pour adresses IP et les inscriptions d'échange de courriel (MX) des serveurs de courrier.

Le DNS est réparti entre de nombreux serveurs dont la plupart délèguent la responsabilité des noms à d'autres serveurs. Dans l'exemple qui précède, l'Internet Assigned Numbers Authority (IANA), organe responsable de la gestion de l'ensemble du système DNS, délèguerait tout les **.ca** à l'Agence canadienne d'enregistrement Internet (ACEI). Celle-ci délèguerait tous les **.macompagnie.ca** au déposant de ce nom et ce dernier exploiterait à son tour les serveurs qui ont l'information concernant **www.macompagnie.ca**.

Domaine (*Domain*)

Un nom utilisé sur Internet. Les domaines Internet sont formés de sections multiples séparées par des points comme **ic.gc.ca** ou **www.maccompagnie.com**.

En-tête (*Header*)

Dans un courriel, partie initiale du message composée d'une série de lignes le décrivant. Chaque ligne commence par une étiquette comme « De : » ou « Sujet : » afin de déterminer sa signification. L'en-tête est suivi d'un espace vierge, puis du corps du message.

Filtre (*Filters*)

Logiciel qui distingue le courriel voulu du courriel non voulu à l'aide des caractéristiques du message. Par exemple, il peut vérifier la présence de certaines chaînes de textes, les tendances textuelles approchées, les ressemblances avec d'autres messages ou autres critères.

Fournisseur de services de courriel (*ESP or email service provider*)

Société qui offre des services de courriel aux autres entreprises. Ce sont, notamment, la collecte et le maintien des listes d'adresses de courriel, l'envoi de courriel en vrac aux adresses figurant sur les listes, le retrait des adresses qui génèrent des messages de non-livraison et le traitement des plaintes et des rapports d'abus concernant les envois.

Hameçonnage (*Phishing*)

L'hameçonnage est une tentative d'escroquerie basée sur l'usurpation d'identité d'une personne ou d'une organisation de confiance, dans le but de voler des renseignements personnels. Par exemple, l'envoi d'un faux courriel utilisant l'identité d'une institution financière, dans lequel on demande aux destinataires de visiter un site Web pour confirmer leurs coordonnées bancaires, site qui est en fait contrôlé par un pirate.

HTML

Langage de balisage de texte, ce système de codage permet de formater les pages Web et les courriels formatés. HTML utilise des balises de texte comme `<h2>A Topic</h2>` qui indique un en-tête de deuxième niveau et `important text`, un texte en caractères gras.

Identification de l'expéditeur (*Sender ID*)

Un schéma d'authentification, semblable à SPF, parrainé par Microsoft. Voir « SPF ».

Identité EHLO/HELO (*EHLO/HELO identity*)

Nom utilisé par l'ordinateur d'envoi pour s'identifier à l'ordinateur de réception au début de chaque transaction SMTP. Pour fournir son nom d'identification, l'ordinateur d'envoi se sert de la commande dite EHLO ou HELO.

Ligne de mention objet (*Subject line*)

Ligne faisant partie de l'en-tête d'un courriel. Les programmes de courriel affichent toujours la ligne de mention objet dans la liste des messages. La description exacte du contenu sur la ligne de mention objet est considérée comme une pratique exemplaire.

Liste blanche (*White list*)

Liste contenant les adresses courriel ou IP qui seront automatiquement acceptées par le serveur de courrier. Elle peut être utile en faisant partie d'un système de vérification par un filtre anti-pourriel. Comparer à « liste noire ».

Liste noire (*Black list*)

Liste contenant les adresses IP, adresses de courriel ou noms de domaine dont les courriels ne sont pas acceptés. La forme la plus courante est une liste noire de système de noms de domaine (DNSBL), une liste d'adresses IP distribuée par l'entremise du DNS d'Internet. Les listes noires de DNSBL les plus connues sont la Spamhaus Black List (SBL), la Composite Black List (CBL) et la liste noire DNSBL originale, appelée Mail Abuse Prevention System (MAPS) Reverse Black List (RBL). Comparer avec « liste blanche ».

Logiciel espion (*Spyware*)

Logiciel qui contient un programme espion et qui emploie à l'arrière plan la connexion Internet de l'utilisateur pour recueillir et transmettre, à son insu et sans sa permission, des données personnelles et modifier le fonctionnement de son ordinateur. À titre d'exemples : les logiciels de surveillance des claviers, qui envoient à un tiers une liste des touches sur lesquelles un utilisateur a appuyé, et les logiciels publicitaires affichant des annonces publicitaires choisies par leur propriétaire.

Maliciel, ou programme pirate (*Malware*)

Terme générique désignant les logiciels hostiles, tels virus, vers et chevaux de Troie.

Manœuvre frauduleuse de l'Afrique de l'Ouest, arnaque 419 ou fraude du Nigeria

(*West African 419 or Nigerian scam*)

Fraude axée sur le paiement d'une commission escomptée, selon laquelle une personne prétendant représenter un pays d'Afrique de l'Ouest demande à la victime de l'aider à soutirer d'importantes sommes d'argent d'un compte gouvernemental. Également appelée arnaque 419, d'après le numéro de l'article de la loi nigérienne qui l'interdit.

Avant de déménager en Afrique, elle était connue sous le nom de *Spanish Prisoner* et remonte sous cette forme aux années 1600.

Messagerie texte (*Text messaging*)

Courts messages comportant du texte plutôt que des images. Ils sont accessibles instantanément (messagerie instantanée) ou par l'entremise d'un téléphone mobile.

MI ou messagerie instantanée (*IM or instant messaging*)

Messages de texte livrés immédiatement de l'ordinateur de l'expéditeur aux destinataires. Les systèmes de MI comprennent AOL® Instant Messenger™, Yahoo!® Messenger et MSN® Messenger.

Mouchard, ou témoin (*Cookie*)

Petit fichier créé et stocké dans l'ordinateur de l'internaute par un serveur Web. C'est une façon pour les sites Web d'identifier l'utilisateur d'un site, de connaître ses habitudes de navigation et de le reconnaître lors de ses visites subséquentes. L'historique d'un utilisateur permet aux concepteurs de sites Web d'adapter dynamiquement le contenu des pages Web et de créer des expériences individualisées pour l'internaute. Selon la programmation du serveur Internet, il peut contenir des renseignements personnels tels que des mots de passe de sites et des numéros de compte.

Les mouchards internes émanent du site Web visité, tandis que les mouchards tierce partie émanent généralement des sources de publicité sur le site visité. Ils permettent au publicitaire de déterminer si l'internaute visite plusieurs sites Web qui affichent ses annonces, posant ainsi un risque sur le plan de la sécurité.

Les navigateurs Web modernes permettent de refuser tous les mouchards, les mouchards tierce partie ou les mouchards de sites Web désignés.

Mystification, ou usurpation d'adresse IP (*Spoofing*)

Technique qui consiste à usurper l'identité d'une autre personne ou organisation, ce qui permet de faire croire que le courriel provient d'une source différente de la source véritable.

Parcours (*Clickstream*)

Séquence des requêtes ou de clics effectués par un internaute lors de la visite d'un site Web.

Sur un site Web commercial, le parcours peut inclure une consultation du catalogue, le placement d'articles dans un panier virtuel, la transmission de renseignements sur le paiement et l'expédition et le passage de la commande.

Pixel invisible (*Web bug*)

Également appelé pixel espion, il s'agit d'une image GIF (graphics interchange format) invisible. C'est une façon pour l'expéditeur d'un courriel en HTML de déterminer si et quand le destinataire a ouvert le message et l'a lu.

Port 587 ou SUBMIT (*Port 587 or SUBMIT*)

Port de rechange que de nombreux services de courriel offrent à leurs clients pour l'envoi du courriel au serveur du FSI. L'authentification de l'expéditeur étant exigée avant l'envoi, la vérification du courriel expédié par SUBMIT est plus facile que sur le port 25. SUBMIT est également appelé port 587 car ce dernier lui est associé.

Pourriel (*Spam*)

Il n'y a pas de définition universellement acceptée du pourriel, mais de nombreux pays le considèrent comme étant un courriel commercial diffusé massivement sans le consentement explicite des destinataires.

rDNS ou DNS inversé (*rDNS or reverse DNS*)

Système de noms de domaine inversé, service servant à retracer un nom de domaine à partir d'une adresse IP. Il effectue la fonction inverse du système de retraçage DNS habituel. Le système DNS inversé sert souvent à consigner les messages entrants selon leur nom de domaine à des fins statistiques et de vérification. L'exactitude du rDNS constitue une pratique exemplaire pour les ordinateurs clients et les serveurs.

Refus (*Opt-out*)

Également appelé « consentement négatif ». L'organisme offre à la personne concernée l'occasion de se prononcer en désaccord avec une utilisation proposée. À moins que la personne ne prenne des mesures pour exprimer un consentement négatif à l'égard de l'utilisation prévue – en d'autres mots, dire « non » – l'organisme présume que le consentement a été donné et exécute l'utilisation prévue. La personne devrait être clairement informée que, en omettant d'exprimer son refus, elle consent à ce que les renseignements soient utilisés aux fins proposées. (Source : Fiche d'information du Commissariat à la protection de la vie privée du Canada)

Relation d'affaires existante (*Existing business relationship*)

Une relation d'affaires existe lorsque :

- 1) le destinataire s'est procuré un produit ou service auprès d'un organisme au cours des 18 derniers mois;
- 2) le destinataire n'a pas indiqué qu'il souhaitait se retirer de la liste d'envoi des courriels commerciaux ou promotionnels ni autrement interrompu la relation.

Un affilié ou un tiers ne peut se fier à la relation d'affaires antérieure d'un autre organisme pour envoyer des courriels commerciaux ou promotionnels.

Réseau d'ordinateurs zombies (*Botnet*)

Réseau de « zombies » qui sont utilisés pour envoyer du pourriel dans un autre but. Un seul réseau comprend souvent des centaines ou des milliers d'ordinateurs.

Retour à l'envoyeur (*Bounces*)

Procédé de rejet d'une tentative de livraison d'un courriel. Un courriel retourné à l'expéditeur indique que le courriel précédent n'a pu être livré.

En cas de non-livraison temporaire « soft bounce », l'ordinateur expéditeur peut tenter de livrer le message plus tard. La non-livraison permanente « hard bounce » reflète un échec.

Une boîte aux lettres d'arrivée pleine, un serveur surchargé ou d'autres problèmes temporaires peuvent causer une non-livraison temporaire. La non-livraison permanente indique généralement qu'une adresse est invalide ou que l'hôte a pour politique de rejeter le courrier en provenance de l'expéditeur.

Serveur (*Server*)

Ordinateur qui fournit un ou plusieurs services aux autres ordinateurs, comme le serveur de courriel, le serveur DNS et le serveur Web.

SMTP

« Simple Mail Transfer Protocol », système utilisé pour envoyer un message d'un ordinateur à l'autre dans Internet. Le protocole SMTP est défini dans la série de documents Request for Comments (RFC 2821) de l'Internet Engineering Task Force.

SPF

« Sender Policy Framework », une extension du protocole SMTP dans Internet. SPF vérifie la légitimité d'un courriel en comparant le domaine du courriel de l'expéditeur contre une liste d'ordinateurs autorisés à envoyer des courriels à partir de ce domaine. Pour de plus amples renseignements, voir <http://spf.pobox.com>.

Usurpation d'identité (*Identity theft*)

L'utilisation de renseignements personnels volés pour usurper l'identité de quelqu'un en vue de commettre une fraude. Le vol peut être commis dans le but d'accéder à des comptes bancaires réels, d'obtenir des prêts bancaires ou à d'autres fins frauduleuses.

Vente croisée (*Cross-sell*)

Vente où l'on encourage le client à acheter un produit ou service associé à un produit ou service déjà acheté. Comparer avec « vente de gamme supérieure ».

Vente de gamme supérieure (*Up-sell*)

Vente où l'on offre à un client un article ou un produit ou service plus cher. Comparer avec « vente croisée ».

Ver (*Worm*)

Programme pirate qui se propage directement en se copiant sur d'autres ordinateurs grâce à des défauts de sécurité dans les logiciels informatiques. Le premier ver utilisait un défaut de sécurité dans les systèmes Solaris de Sun Microsystem et les systèmes VAX, mais les vers actuels exploitent les défauts inhérents à Microsoft Windows. Comparer avec « virus ».

Virus

Programme pirate qui se propage en s'attachant à une autre ressource sur un ordinateur. Les premiers virus se propageaient en s'attachant aux programmes d'application, mais les virus actuels se propagent par l'entremise du courriel. Comparer avec « ver ».

Zombie

Ordinateur infecté par un pirate et contrôlé à distance par le créateur, le distributeur ou le contrôleur de ce pirate. À l'heure actuelle, la majeure partie du pourriel est envoyée au moyen de zombies.

