

# SPAM

MARTIN.OUWEHAND@epfl.ch, SIC



Rappelons que le spam est l'envoi de courrier électronique à un grand nombre d'adresses apparemment récoltées au hasard et sans l'accord des destinataires. Les messages envoyés contenant généralement de la publicité de la pire espèce, personne à ma connaissance n'aime en recevoir. Dans cet article, je parlerai du spam selon divers points de vue et vous donnerai quelques conseils pratiques (voir encart sur la page suivante).

## ASPECTS ÉCONOMIQUES

Dans nos sociétés capitalistes, le marché, dit-on, optimise l'utilisation des ressources pour satisfaire les besoins des acteurs économiques et, de fait, les besoins de base (nourriture, habitation, santé) sont satisfaits dans une large mesure. Mais, pour maintenir ou étendre le marché, la publicité est omniprésente afin de stimuler ou créer les besoins et c'est ainsi qu'il est pratiquement impossible de marcher dans nos villes sans passer devant de nombreux panneaux vantant des produits de toutes sortes, de voir un film à la télévision sans qu'il ne soit interrompu par des *spots*. Même le Flash Informatique n'est pas épargné ! Il n'est donc pas étonnant que la publicité se soit aussi répandue dans ce nouveau *médiu*m qu'est Internet: les bannières de nombreux sites Web et le spam en sont des exemples.

Certains *vieux* internautes, se souvenant de l'époque dorée de l'e-mail sans spam et espérant qu'elle pourra revenir *en prenant les dispositions nécessaires*, perdent souvent de vue ce point: le spam est apparu quand Internet a cessé d'être financé par les budgets de la recherche et de l'enseignement pour fonctionner selon les lois du marché (mais d'un autre côté, on rétorquera que grâce à cela Internet est devenu meilleur marché et plus rapide).

Ce point de vue économique explique aussi, je crois, la qualité abyssale de la publicité reçue par e-mail: les grandes compagnies savent que les affiches dans nos rues sont bien acceptées ou du moins tolérées mais que le spam est mal perçu et qu'ils pourraient perdre des clients en l'utilisant (ceci pourrait toutefois changer d'ici quelques années). Le spam est donc réservé à des produits ou des entreprises qui n'ont pas encore de clients ou qui visent des niches restreintes dans les coins les plus obscurs de l'économie, entre la pornographie, la charlatanerie ou carrément l'escroquerie. Il leur importe peu d'énerver des centaines de milliers d'internautes,

il suffit de quelques centaines, voire quelques dizaines, de gogos tombant dans le panneau pour rentrer dans leurs frais (il est en effet extrêmement bon marché d'envoyer du spam: j'estime le budget d'un épisode de spam à quelques centaines de francs, tout au plus).

## ASPECTS JURIDIQUES

Le spam n'est-il pas illégal ? Il faudrait le demander à un juriste pour en être sûr (et encore...), mais à ma connaissance, si des projets de loi interdisant explicitement le spam ont été discutés dans quelques parlements, y compris à Berne (cf. [http://www.parlament.ch/ab/data/ds/4606/27565/d\\_s\\_4606\\_27565\\_27608.htm](http://www.parlament.ch/ab/data/ds/4606/27565/d_s_4606_27565_27608.htm)), elles ne sont en vigueur nulle part. Ceci ne veut pas dire que le spam n'est pas interdit par d'autres lois plus générales par analogie (par exemple les

mêmes que celles interdisant la publicité par fax), comme y fait allusion la parlementaire Sommaruga dans sa proposition devant le parlement suisse (voir l'URL ci-dessus). Mentionnons encore que les lois de quelques Etats Américains exigent bien des spammers qu'ils honorent les demandes d'*opt-out* (cf. <http://www.spamlaws.com/state/summary.html>), mais c'est là une mesure inefficace puisque la plupart des épisodes de spam sont isolés.

Quoi qu'il en soit, même si de telles lois existaient, je pense qu'elles seraient trop difficiles à appli-

quer et ne suffiraient probablement pas à faire disparaître le phénomène, un peu pour les mêmes raisons que les lois protégeant la propriété privée n'empêchent pas les graffitis de couvrir les murs de nos villes: chaque infraction isolée est relativement bénigne et aboutit donc rarement à une sanction, mais l'effet de toutes les infractions réunies est très visible. D'autre part, le spam *vit* sur Internet et traverse donc les frontières: les messages partent d'Aachen pour le compte d'une entreprise basée dans le Delaware, passent par un serveur e-mail aux Philippines, qui les envoient à sa victime de Zywiec. Où est le for? Que se passe-t-il si l'un des pays impliqués est laxiste dans le domaine du spam ? Ou bien si son système judiciaire est tout simplement débordé par des problèmes plus pressants ? Enfin, même dans le cas de spam entièrement *national*, une procédure judiciaire est toujours une entreprise longue et coûteuse qu'il est improbable que l'EPFL entame, même pour le principe.

**p u b l i c i t é**

**Brillez en société ! Epatez vos amis ! N'ignorez plus rien de ce sujet brûlant qu'est la sécurité informatique ! Lisez:**

**<http://slwww.epfl.ch/securite.html>**

# MESURES PRATIQUES À PRENDRE À L'ÉGARD DU SPAM

## NE PAS DISSÉMINER SON ADRESSE E-MAIL

Si les spammers ne connaissent pas votre adresse e-mail, vous ne recevrez pas leurs messages. Pour qu'elle ne soit pas capturée dans leurs filets, il faut donc éviter de mentionner son adresse dans les pages Web, dans les articles des News ou des mailing-lists que vous publiez et ne l'entrer dans aucun formulaire Web (éventuellement utiliser à cet effet une adresse gratuite jetable obtenue auprès de Hotmail, Freesurf ou autre). De manière générale, il faut la considérer comme une information confidentielle. A ce propos, je suis d'avis qu'il faudrait interdire l'accès externe à l'annuaire <http://www.epfl.ch/cgi-bin/csoldap>, où figurent les adresses e-mail de tous les membres de l'École.

## NE PAS ENTRER EN CONTACT AVEC LE SPAMMER

Les adresses e-mail sont une denrée très périssable et les spammers prisent particulièrement celles dont l'existence est *vérifiée*. C'est pourquoi ils vous proposent souvent un URL ou une adresse e-mail pour vous retirer de leur liste: c'est un pur mensonge et si vous utilisez ce service, ils sauront que votre adresse existe bel et bien et vous êtes sûr de recevoir encore plus de spam. La consigne est donc: silence radio! Récemment, on m'a signalé aussi de mystérieux messages où un inconnu vous remercie par exemple pour un récent repas et j'ai l'impression qu'il s'agit aussi d'une ruse pour vérifier votre adresse. Réfrérez donc votre courtoisie et évitez de lui répondre qu'il se trompe sans doute (tel est l'Internet de nos jours!).

## DÉSACTIVER HTML DANS VOTRE OUTIL D'E-MAIL

Sinon, un spammer peut glisser un lien dans son message qui sera activé lors de l'affichage du message, lui permettant ainsi de vérifier à distance que votre adresse est valide (*Web bug*).

## APPRENDRE À GÉRER LE SPAM

Tous les outils d'e-mail modernes offrent la possibilité de trier les messages que vous recevez selon divers critères. Vous pouvez l'utiliser par exemple pour placer dans un dossier à part tous les messages qui ne sont pas destinés à une adresse à laquelle vous vous attendez à recevoir du courrier légitime (il ne s'agit en général que de votre adresse personnelle et de quelques adresses de listes de distribution, comme [personnel.epfl@epfl.ch](mailto:personnel.epfl@epfl.ch)). Après quelques tâtonnements, vous ne retrouverez dans ce dossier pratiquement que du spam et la majeure partie de tout le spam que vous recevez. Un autre talent qu'il est utile de développer est celui de repérer le spam en ne se basant que sur l'expéditeur et le sujet: tous les outils d'e-mail que je connais permettent de présenter chaque message d'un *folder* sur une ligne où figurent ces deux renseignements et de l'effacer d'un simple clic. Ces deux pratiques vous permettront de vous débarrasser de votre dose quotidienne de spam en quelques secondes. Apparemment, certains éprouvent de la gêne à effacer un message sans vérifier son contenu, mais c'est là une relique de l'époque révolue où tous les messages étaient significatifs. A notre époque c'est au contraire à notre correspondant d'introduire son message par un sujet pertinent et informatif s'il veut être lu.

## GARDER SON CALME

Je dois confesser que les premiers spams que j'ai reçus m'ont rendu tout à fait furieux et si j'en crois divers échos, c'est une réaction répandue. Veuillez donc écouter la sagesse de quelqu'un qui est passé par là: il n'est pas bon de s'énerver pour ce que vous ne pouvez pas changer et, si elle n'est pas une bonne maxime en toute circonstance, la résignation apporte souvent la sérénité: face aux goûts musicaux ou vestimentaires de notre jeunesse, face à l'utilisation du téléphone portable dans les transports publics et enfin face au spam. La mesure suivante contribuera aussi à ne pas vous sentir impuissant.

## AVERTIR [abuse@epfl.ch](mailto:abuse@epfl.ch)

Vous pouvez envoyer à cette adresse une copie des spams que vous recevez et une personne compétente en la matière concentrera alors les plaintes et les transmettra aux fournisseurs d'accès utilisés par les spammers pour injecter leurs messages vers Internet. Attention ! pour être utilisable, le message de spam que vous communiquez doit être complet et inclure des en-têtes qui sont souvent cachés par les outils d'e-mail. En particulier, les champs *Received:* doivent y figurer au complet. Si nécessaire, il faut donc demander de l'aide à un informaticien chevronné sur la procédure à suivre.

## ASPECTS TECHNIQUES

Est-il possible de filtrer automatiquement le spam par des moyens techniques ? Bien qu'avec quelques nuances, la réponse est non. Tout d'abord, le spam ne se distingue en rien des autres messages aux yeux du logiciel de routage de l'e-mail et certaines bizarreries qu'on voit souvent dans l'adressage du spam (par exemple le message paraît adressé à quelqu'un d'autre) sont permises par le protocole SMTP (Simple Mail Transfer Protocol) et sont même nécessaires au bon fonctionnement des logiciels de gestion des listes de distribution (*mailing-lists* en jargon anglo-informatique).

Non, le spam est en fait une notion *culturelle*: il faut un être humain pour décider que tel message est ou n'est pas du spam (ce n'est pas une notion définissable formellement avec la précision requise pour être détectée par un programme). On peut bien sûr rendre ce travail plus efficace en s'appuyant sur des moyens techniques adéquats. Par exemple, chaque message marqué comme du spam est entré dans une base de données et tous les messages entrants sont comparés aux spams déjà répertoriés: de cette manière chaque spam différent ne doit être détecté qu'une seule fois. Mais les spams arrivant à toutes les heures du jour et de la nuit, y compris le week-end, il faudrait au moins une dizaine de personnes réalisant ce travail abrutissant pour filtrer les 15'000 à 20'000 messages externes envoyés quotidiennement à l'EPFL. Il est sans doute plus rationnel de confier cette tâche à une entreprise spécialisée, qui peut protéger de la sorte de nombreux sites en réalisant une économie d'échelle certaine, malheureusement les prix demandés reflètent la charge salariale ainsi économisée: par exemple l'abonnement à Brightmail (<http://www.brightmail.com>) démarre à 100'000 dollars par année.

Un système analogue basé sur le volontariat et par conséquent gratuit, Razor (<http://razor.sourceforge.net>), présente quelques inconvénients: la base de données des spams n'est accessible que par Internet (impossible d'en avoir une copie locale, d'où une baisse de fiabilité et de rapidité dans l'acheminement de l'e-mail), l'indexation est basée sur le hachage des messages (les spammers peuvent donc contourner le filtre en ajoutant quelques caractères aléatoires à chaque mes-

sage, comme on commence à le voir de plus en plus souvent) et bien sûr des vandales viennent semer le trouble en déclarant comme spam ce qui n'en est pas. Le leader du projet Vipul Ved Prakash vient d'annoncer que ces problèmes seraient réglés dans la version payante qui sera distribué par Cloudmark, la start-up qu'il vient de fonder.

Parmi d'autres approches possibles, mentionnons SpamAssassin (<http://spamassassin.org>) basé sur une batterie de tests heuristiques détectant certains *tics* des spammers mais assez gourmand en ressources de calcul et les systèmes basés sur des répertoires de relais ouverts (un problème que l'EPFL n'a résolu qu'avec la venue de DIODE, voir <http://sic.epfl.ch/publications/FI01/ft-2-1/2-1-page9.html>) dont les problèmes (injustifiés, de l'avis général) avec les tribunaux ont parfois provoqué la fermeture: c'est le cas d'ORBS et de son successeur ORBZ (voir <http://www.theregister.co.uk/content/6/19460.html> et <http://www.wired.com/news/politics/0,1283,51218,00.html>), alors que MAPS semble avoir les ressources pour faire face à ces attaques (<http://mail-abuse.org/pressreleases/2001-10-03.html>). Sans entrer dans les détails, ces systèmes tiennent à jour une base de données (généralement accessible par Internet, d'où les mêmes inconvénients mentionnés à ce sujet pour Razor) de serveurs e-mail configurés en relais ouvert: les messages en provenance de tels serveurs sont presque toujours du spam.

Tous ces systèmes présentent à des degrés divers le risque de faux positifs, c'est-à-dire de messages *innocents* signalés à tort comme du spam. Quel que soit le système utilisé, il n'est donc pas judicieux de supprimer aveuglément les messages détectés comme étant du spam et il est plus prudent de les marquer de manière adéquate comme n'étant que *probablement* du spam et les transmettre quand même au destinataire final qui pourra se baser sur cette marque pour filtrer lui-même plus rapidement le spam.

Quoi qu'il en soit, nous n'avons pas l'intention d'introduire sur les serveurs mail centraux l'EPFL un des filtres évoqués ci-dessus et nous pensons qu'il vaut mieux que chacun suive les mesures pratiques qui sont présentées dans l'encart de la page précédente. ■



ORDINATEUR PORTABLE SCRIB (1977) AVEC COUPLEUR ACOUSTIQUE DÉVELOPPÉ PAR JEAN-DANIEL NICLOUD AU LAMI

## COMMUNICATION ET CULTURE

Entre Z4, Pascal, Lilith, Smaky, Logitech, cherchez le point commun, ... c'est l'histoire de l'informatique en Suisse. Le musée de la communication à Berne a édité un numéro bilingue d'une centaine de pages, très bien illustré où vous retrouverez avec plaisir des noms comme Jean-Daniel Nicoud, Anton Gunzinger, Robert Cailliau, Georges Abou-Jaoudé. Vous pouvez vous procurer ce livre auprès du musée ([www.mfk.ch](http://www.mfk.ch)) ou en visitant leur exposition **Control-Alt-Collect**, les ordinateurs en retraite.