

## SPAM

### Comment se protéger des intrus ?



*Le volume des envois non sollicités (spam) sur nos e-mails aurait progressé de 600 % entre avril 2001 et avril 2002, pour accaparer désormais 20% de la bande passante du réseau. Les estimations pour l'avenir ne sont plus réjouissantes : d'ici la fin de l'année, 35 % des messages échangés seraient des spams, selon certaines enquêtes.*

Mille milliards ! C'est le nombre total de mails qui s'échangera en 2002. Et parmi eux, un tiers d'envois non sollicités ou, en d'autres mots, de pubs sauvages. Le « spam » - puisque c'est de lui qu'il s'agit - est plus que jamais le cancer d'Internet. Il suffit de poser la question : les personnes qui se plaignent d'être envahies à longueur de journée par des e-mails non sollicités (spam) sont légion. Pourtant, le phénomène n'est pas en soi nouveau. Les publicités non demandées infestent nos boîtes aux lettres classiques depuis des lustres, mais tout reste cependant à une échelle nationale et les citoyens vraiment excédés peuvent toujours apposer sur leur boîte un

autocollant « pas de publicité, merci ». Mais avec Internet, comment faire ? N'importe quelle adresse électronique est potentiellement connue de n'importe quelle société installée dans n'importe quel endroit de la planète. Résultat des courses : un expert-comptable ou l'un de ses clients revient le mardi matin et se retrouve noyé avec des centaines d'e-mails qui vont de voyages en passant par les articles de bureau ou un quelconque régime amaigrissant. Le phénomène n'a cessé de s'amplifier ces dernières années pour atteindre les proportions folles que nous connaissons aujourd'hui. Le volume des envois non sollicités a progressé de 600% entre avril 2001 et avril 2002, pour accaparer désormais 20% de la bande passante du réseau. Les estimations de l'institut américain Jupiter, ne sont plus réjouissantes : d'ici la fin de l'année, 35% des messages échangés seront des spams.

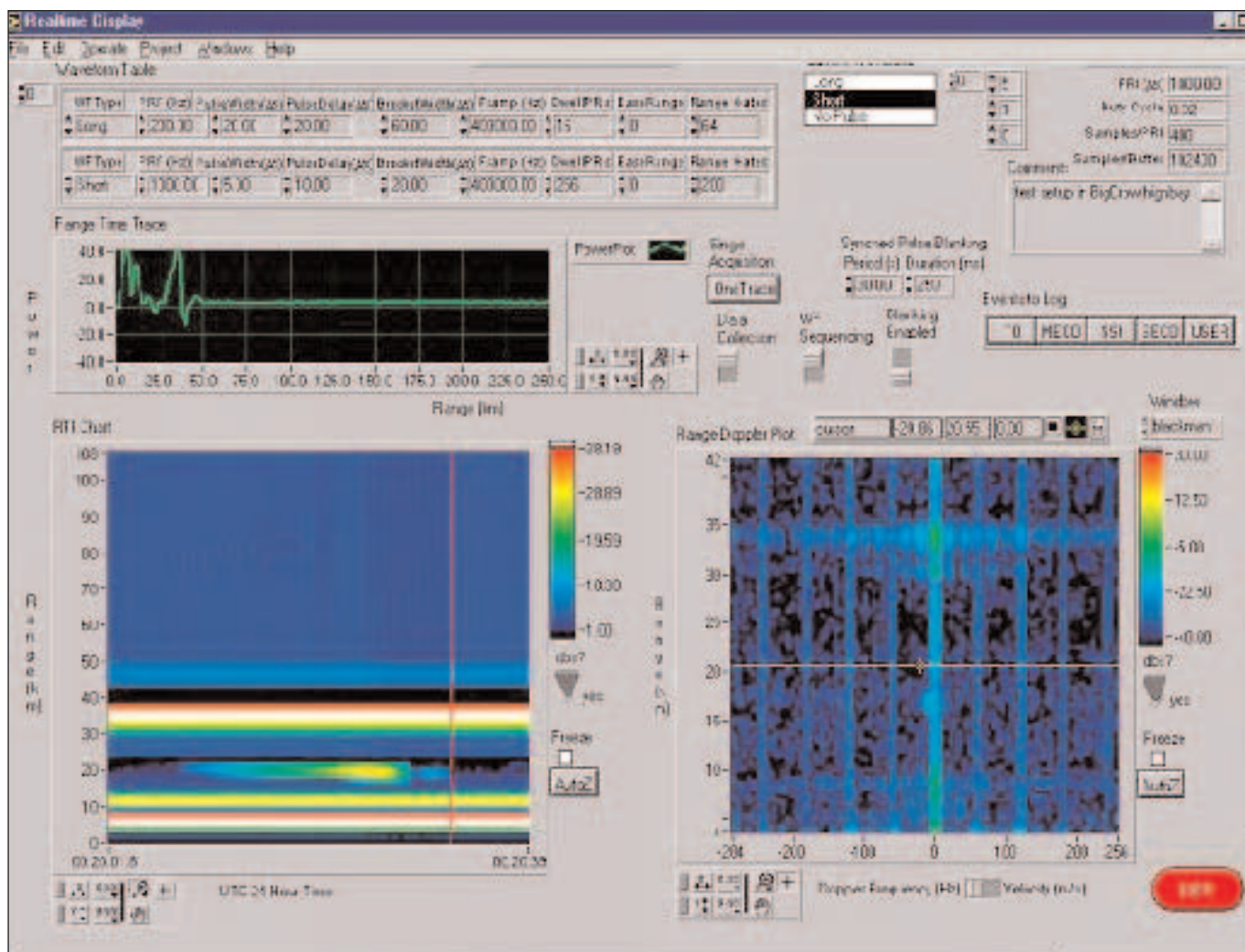
#### Logiciels anti-spam

Bien entendu, comme toujours, le phénomène profite à certains. Et c'est le cas des éditeurs de logiciels anti-spam. A côté d'une série de petites sociétés spécialisées dans les produits spécifiquement conçus pour combattre les spams, des éditeurs comme Mc Afee et Symantec ont commencé à se positionner sur ce marché. Récemment encore, Mc Afee a racheté l'application SpamKiller à un fabricant de logiciels norvégien et l'a intégrée à ses logiciels de sécurité. « Nous avons

repris SpamKiller en janvier, quand nous avons pensé que le marché antispam allait exploser » a expliqué à la presse, Bryson Gordon, responsable produit pour Mc Afee. « Cela ressemble beaucoup à la façon dont le marché des antivirus a commencé au début des années 80. Au départ simple nuisance, le spam est en train de devenir une menace pour la sécurité ». De fait, une proportion croissante des quelque 500.000 vols de cartes de crédit et usurpations d'identité qui surviennent en ligne chaque année, s'effectue par le biais de spams, affirment les spécialistes.

#### Et la vie privée ?

Pareil phénomène ne va pas sans susciter des interrogations : la destruction de la vie privée est-elle à l'économie de l'Internet ce que la destruction de l'environnement est à l'économie industrielle ? La question a été examinée par des spécialistes. Notamment sur le respect de nos quatre droits fondamentaux : celui d'être laissé tranquille, de contrôler les informations qui nous concernent, de vivre sans être observé et enfin, le droit à l'anonymat. Mais autant le dire de suite : la mission s'avère impossible à respecter, lorsqu'un spam marketer peut expédier cinq millions d'e-mails non sollicités pour moins de 50 dollars et que rien n'est fait pour rendre accessibles les fonctions qui pourtant existent et permettent au navigateur soit de refuser les cookies, soit de détecter leur présence. Mais comme le font



remarquer certains, il y a plus grave encore : à savoir, les 22 millions de spywares dissimulés dans l'ordinateur et que l'internaute lui-même rend publiques sans le savoir. Aux Etats-Unis, il semblerait que les employeurs potentiels ou avocats de la partie adverse ratissent déjà les archives des forums pour tenter de mieux cerner la personnalité d'un candidat ou trouver de quoi enfoncer l'adversaire !

### Quelles solutions ?

A priori, il est difficile d'échapper au phénomène du spam... sauf à ne jamais laisser son adresse e-mail sur le site Web. Disons le d'emblée, il n'y a pas de méthode miracle pour échapper au spam. En modifiant notre comportement, on peut cependant diminuer leur nombre. Grâce aux conseils du site arobase ([www.arobase.org](http://www.arobase.org)), nous avons pu

identifier quelle attitude adopter face à ce fléau :



#### Solution n°1 : ne pas laisser traîner son e-mail

Première solution (radicale) : ne pas poster de messages dans les news groups et ne pas mentionner votre adresse sur le web. Un peu difficile... Mais faites un effort, il est possible d'éviter de laisser son adresse e-mail un peu partout.



#### Solution n°2 : s'inscrire sur des listes anti-pub

Vous avez peut-être entendu parler de l'existence de sites qui gèrent des listes d'adresses de personnes ne désirant pas être spammées. Listes que les spammers « gentils » consulteraient

pour exclure des adresses de leurs envois, l'argument étant qu'il est préférable pour leur image de ne pas adresser de pub à quelqu'un que ça ne ferait qu'énerver. Seulement, encore faut-il que les spammers soient « gentils » et fassent l'effort d'aller consulter ces bases de données. Et puis il se dit que le spammers « méchants » utiliseraient ces mêmes listes (voire les créeraient) pour récupérer de nouvelles adresses ou vérifier la validité des adresses existantes... A vous d'agir en connaissance de cause avant de vous inscrire sur ces listes.



#### Solution n°3 : utiliser deux adresses e-mail

L'une, la principale, sera « saine ». Vous ne la communiquerez qu'à vos proches et vos contacts professionnels. Vous ne recevrez donc sur ces adresses que vos

courriers importants.

L'autre vous servira pour tout ce qui ne concerne pas directement vos courriers personnels : abonnement aux listes de diffusion, aux lettres d'informations, renseignements de formulaires, publication sur une page web etc. Elle finira par être spammée, mais vous pourrez quand cela vous paraîtra insupportable, vous en débarrasser aisément. Plus vicieux encore : on peut éventuellement utiliser, pour plus d'efficacité, deux adresses secondaires : l'une pour les listes, l'autre pour tout le reste (inscriptions etc).

Si vous respectez scrupuleusement cette séparation, vous devriez garder une adresse e-mail relativement saine. Quoique vous n'êtes pas à l'abri d'un contact professionnel qui vous inscrit à la lettre d'information de sa société ou d'un ami, qui croyant vous faire plaisir, communique votre adresse à un site de loterie ou de recherche d'anciens camarades de collège.

### Les grandes manœuvres

Et si tout cela ne suffit pas ? Dans ce cas là, il faudra déboursier un peu d'argent et acheter un logiciel anti-spam. Sachez que certains logiciels vous permettent juste de visualiser votre courrier avant de le charger dans votre logiciel de messagerie, pour que vous puissiez supprimer les messages non sollicités. D'autres appliquent automatiquement des règles de filtrage ou utilisent des listes publiques de spammers (DNSBL lists) pour éliminer les messages non désirés. Certains peuvent aussi mener pour vous une enquête, identifier le fournisseur d'accès du spammer et lui envoyer une lettre de plainte (violente ou plus diplomatique, c'est vous qui choisissez). D'autres enfin renvoient à l'expéditeur des faux messages d'erreur (adresse inexistante etc) pour tromper l'ennemi : c'est ce que les spécialistes appellent un « bounce ». A vous de choisir le logiciel qu'il vous faut dans notre sélection. La plupart d'entre eux sont rédigés en anglais. ¶

