Se protéger « Lutter contre les courriels indésirables »

Avec Internet, il est facile d'envoyer un message à des millions de destinataires, sans dépenser d'argent. Du coup, la boîte mail ressemble à une vraie boîte aux lettres : elle est inondée de prospectus.

Qu'est-ce qu'un spam ?

Lorsque vous recevez un courrier électronique, sans l'avoir sollicité, à des fins publicitaires, commerciales ou malhonnêtes, il s'agit d'un spam. En général, il vante les mérites d'un site pornographique, de soins amaigrissants miracles, d'un crédit financier… mais il peut aussi cacher des escroqueries qui promettent de vous enrichir sans effort. Selon la Commission nationale informatique et libertés (CNIL), sur 325 000 spams signalés par les internautes entre juillet et octobre 2002, **85 %** étaient en langue anglaise et **55 %** des messages en français étaient à caractère pornographique.

Pour vous harceler de mails, le spammeur a besoin de listes d'adresses. Il peut soit acheter un carnet d'adresses, soit se constituer son propre fichier en récupérant des adresses sur Internet. Il peut le faire automatiquement grâce à des outils comme l'aspirateur de mails qui parcoure la Toile à la recherche du signe « @ » ou de l'expression « mail to » ou de logiciels qui testent toutes les combinaisons d'adresses d'un nom de domaine (par exemple xxxx@yahoo.fr ou yyyy@caramail.com), attendent les messages d'erreur et envoient des spams aux adresses valides.

Un certain nombre de mots sont apparus pour désigner le spam. En français, le plus courant est **pourriel** (de « poubelle » et « courriel »), mais on utilise aussi polluriel (de « pollution » et « courriel ») et merdiel (là, pas besoin de faire l'étymologie). Des néologismes qui expriment l'exaspération des utilisateurs face à ces messages qui représentent 30 à 40 % du trafic e-mail.

Se protéger « Lutter contre les courriels indésirables »

▷▷▷A la pêche aux mots de passe

Et les usagers ne sont au bout de leur peine ! Une nouvelle forme de spams vient d'apparaître : le **phishing** ou hameçonnage. Inventé par des pirates qui essayaient de voler des comptes AOL, ce terme anglais vient de l'expression password harvesting fishing qui signifie « pêche aux mots de passe ». Leur but : récupérer des données personnelles, des mots de passe par exemple, en attirant les utilisateurs d'un service sur un site fictif où ils peuvent enregistrer leurs actions. Les victimes sont appâtées par un courriel qui les dirigent vers une page web qui semble faire partie d'un vrai site. En fait, dès qu'une information confidentielle est tapée sur cette page, elle est transmise au pirate.

Le **piège**, c'est que le courriel semble avoir été émis par une société digne de confiance et qu'il est rédigé de manière à entraîner une action du destinataire sur un site factice. Par exemple, votre banque vous contacte car votre compte a été désactivé pour une raison quelconque et il ne sera réactivé qu'en cas d'action de votre part. Le message renvoie, via un lien hypertexte, à une page web, similaire à celle de votre banque. Sur cette page, vous rentrez des informations confidentielles qui sont interceptées par le fraudeur. ◁▷

▷▷▷Chasser les spams de sa boîte

Heureusement, quelques règles simples vous éviteront d'avoir votre boîte saturée par des spams.

1. N'ouvrez jamais un spam ou son fichier joint.
2. Ne répondez jamais à un spam, même s'il vous propose de vous désabonner: une réponse indique que votre adresse est valide et donc, vendable. Vous serez désabonner de cette liste, mais entrerez dans de nombreuses autres.
3. Ne laissez jamais votre adresse mail personnelle sur Internet.
4. Créez-vous une 2e adresse mail, différente de votre adresse personnelle, que vous consacrerez à certains usages comme les achats en ligne, les forums, les lettres de diffusion…
5. Evitez de transmettre les « chain mails » (messages transmis massivement pour une bonne cause ou une autre). Les « spammeurs » peuvent s'en servir pour leur collecte d'adresses valides. Mais si vous souhaitez, malgré tout, faire suivre ce type de messa ges, mieux vaut que le corps du texte ne contienne aucune adresse et que les destinatai res soient en copie cachée.

Se protéger « Lutter contre les courriels indésirables »

Si ces conseils contraignent trop votre utilisation d'Internet, vous pouvez aussi décider de camoufler votre adresse. On peut citer plusieurs moyens assez efficaces.

1. Vous pouvez créer un graphique sur lequel on retrouve votre adresse, les robots étant capables de lire du texte, mais pas les images.

2. Vous pouvez aussi ajouter un préfixe ou un suffixe, tout en précisant à vos visiteurs de l'enlever avant de vous écrire.
   Par exemple, si votre adresse est gerardmajax@hotmail.com, vous écrirez nospam_gerardmajax@hotmail.com. Les destinataires devront enlever « nospam_ » pour pouvoir vous répondre, n'oubliez pas de leur signaler.

3. Vous pouvez enfin utiliser un programme qui permet de coder votre adresse mail. Elle sera alors fonctionnelle pour votre carnet d'adresses, mais illisible pour les robots. Vous pouvez par exemple tester Obfuscator ici ou d'autres outils sur ce site là. Il suffit d'entrer son mail dans le champ « obfuscator » et de copier-coller le code donné.

N'oubliez pas non plus que certains logiciels de messagerie comme Thunderbird intègrent des filtres anti-spams efficaces, tout comme la plupart des webmails (caramail, yahoo, etc…).

Si vous êtes partisan des démarches juridiques, vous pouvez certes, saisir la CNIL, et dénoncer les spammeurs.

http://www

La CNIL
http://www.cnil.fr