

Diapo 14 (2005) <http://www.dicodunet.com/definitions/internet/spam.htm>

Terme informatique résultant de la fusion de "courriel" et "poubelle", représentant les courriels-poubelle, des e-mails indésirables.

Aussi appelé par son synonyme plus connu "spam" (ou encore "junk mail" en Amérique), le terme pourriel (courriel-poubelle, courriel-rebut ou encore pub-rebut) aurait été proposé par **l'Office de la langue française du Québec en mai 97**.

Un pourriel est un courriel qui contient dans la plupart des cas une publicité, envoyé sans l'accord de son destinataire.

Des listes d'adresses email sont constituées par les spammeurs qui utilisent des logiciels pour récupérer des adresses email sur les forums ou tout autre forme de site web. Ces listes sont souvent revendues très cher à d'autres spammeurs.

Pourquoi le spam ?

Le but premier du spam est de faire de la publicité à moindre prix par "envoi massif de courrier électronique non sollicité" (junk mail) ou par "multi-postage abusif" (EMP).

Les spammeurs prétendent parfois, pour leur défense, que le courrier est facile à supprimer, et qu'il est par conséquent un moyen écologique de faire de la publicité.

Cela est tel, que certains spammeurs défendent la cause même du spam.

Les critères

La détermination du spam se fait sur un critère de volume. Un courrier électronique envoyé à 5 ou 6 personnes grâce à la fonction [CC](#) ne peut pas être considéré comme du "spam". On considère en effet qu'un envoi supérieur à 20 messages constitue un spam.

Les effets du spamming

Le principal inconvénient du spamming est l'espace qu'il occupe sur le réseau, utilisant inutilement une bonne partie de la bande-passante, rendant internet moins rapide.

Cela induit des coûts supplémentaires pour les Fournisseurs d'Accès à Internet (FAI) car ils doivent:

- mettre en place une plus grande largeur de bande
- acheter des ordinateurs supplémentaires
- disposer d'un plus grand espace disque
- engager du personnel supplémentaire

Branchez-vous 19 juillet 2004

«Phishing» : découverte d'une méthode plus sournoise pour les arnaques par courriel

Il ne s'agit pas d'une nouvelle faille dans les fureteurs Web mais plutôt d'une technique connue qui pourrait être appliquée par des fraudeurs dans des cas d'arnaques par courriel de type «phishing».

Le «phishing», une technique de fraude en ligne de plus en plus répandue sur Internet, consiste à expédier massivement des messages de courriel en prétendant être une banque ou un commerce en ligne, et à demander aux internautes de fournir de nouveau des renseignements confidentiels en prétextant par exemple un problème du système qui aurait causé une perte de données.

Dans [son texte de présentation](#) intitulé «Mastercard est-elle partie en voyage de pêche en laissant la porte grande ouverte?», le spécialiste en sécurité informatique révèle notamment que le site Mastercard est vulnérable à ce type d'attaques, un fait décevant de la part d'une entreprise qui [annonçait justement le mois dernier](#) de nouvelles mesures pour enrayer les fraudes par courriel de type «phishing».

Sam Greenhalgh précise qu'il ne s'agit pas d'une nouvelle faille de sécurité mais que son exploitation sur certains sites vulnérables, notamment à cause de formulaires qui ne s'assurent pas de la validité des données saisies, pourrait constituer une nouvelle menace. Celui qui a découvert l'an dernier [un boque d'Internet Explorer](#) qui facilitait le même type de fraudes par Internet, ajoute que l'utilisation de l'injection de script est cependant «beaucoup plus dangereuse car le site authentique est manipulé pour afficher du contenu non valide» via un script externe qui est appelé dans l'URL.

La meilleure protection contre le «phishing» reste toutefois de ne pas répondre à ce type de courriel (et de rapporter l'événement à l'institution concernée) car les banques et les commerces en ligne n'expédient jamais de message dans le but d'obtenir des renseignements confidentiels tels que numéro de carte de crédit, nom d'utilisateur et mot de passe.