Publié le : 11 décembre 2003
Imprimer cet article

Auteur :
Rémy Louvet

La lutte anti-spam

Vous utilisez votre messagerie électronique depuis quelques semaines ou depuis quelques années et le phénomène est le même pour tous : après votre boîte aux lettres du domicile, après le fax, après le pare-brise de votre voiture, après votre téléphone portable, votre messagerie vient d'être attaquée par des commerciaux peu scrupuleux. Vous recevez des emails à connotation sexuelle ou vaguement commerciale sans oublier les emails carrément pornographiques.

Dans le jargon du web, on appelle cela du spam. Le spam est en fait le symbole d'une boîte de conserve comportant une viande peu ragoutante. Ces mails sont aussi dénommés polluriels, pourriels, courriers-rebut ou UCE (Unsollicited Commercial E-Mail). Selon des études menées par les fournisseurs d'accès internet (FAI), ce phénomène serait de l'ordre de 30 à 40 % du trafic de messagerie ; c'est énorme. Essayons d'y voir plus clair.

Comprendre le spam
Quelle est l'origine du spam ? Comment les spammeurs récupèrent-ils vos adresses email ? Quelle législation à ce propos ?

Prévenir le spam
adoptez les meilleures règles de messagerie et connaissez les manips' à éviter

Réagir au spam
des astuces, des logiciels et des trucs pour utilisateurs et webmasters

---

1) Comprendre le spam

Définition C'est l'envoi en nombre de messages publicitaires ou promotionnels non sollicités par le destinataire. D'ailleurs, la CNIL (Commission Nationale Informatique et Libertés) est très explicite sur ce phénomène :

"Quelle que soit la nature du message (commerciale, politique, religieuse, etc.), la prospection par e-mail est irrégulière si les personnes concernées n'ont pas exprimé leur consentement à l'occasion d'un contact direct et personnel, à un usage de leur adresse électronique à de telles fins.

En fait, des commerciaux peu scrupuleux, des webmasters avides d'être reconnus pratiquent le spamming et finalement embouteillent carrément le web.

Origine du terme
Le mot "SPAM" vient d'une marque américaine de corned-beef, au goût infect ; il a été ensuite

chanté par les Monty Python, de manière crescendo et répétitive et avec un important bruit de fond. Par comparaison, le spam est franchement dégueulasse mais on est bien obligé de s'en accommoder.

Pourquoi est-ce un fléau ?
Le spam est devenu omniprésent sur toutes les messageries de la planète et envahit littéralement nos serveurs puis nos disques durs. Cela provoque des ralentissements du trafic Internet et accroît les risques de virus informatiques. C'est un véritable mal qui comporte trois entités : financières, éthiques et fonctionnelles.

En effet, le spam en tant que publicité ne coûte pas très cher à l'expéditeur ; il peut ainsi arroser des milliers de boîtes aux lettres à peu de frais.

L'éthique est bafouée car il n'y a plus aucune morale dans ce phénomène, le spammeur utilise tous les subterfuges imaginables pour trouver des adresses valides et les saturer de son "corned-beef". Ils trouvent des adresses email sur les sites web de débutants, dans les listes de diffusion, dans les Newsgroups. Il existe bien entendu des logiciels-espions ou robots qui vont carrément fouiller la toile à leur place afin de trouver encore et toujours de nouvelles adresses.

Fonctionnellement, le spam est devenu tout simplement une pollution. De notre adresse email, de notre disque dur, de notre espace privé et du web tout entier car tout le monde y est confronté.

---

2) Prévenir le spam

Tout d'abord, pour ne pas se faire spammer, il ne faut pas divulguer votre adresse email de votre FAI à n'importe qui et sur n'importe quel site. Elle sera inexorablement retrouvée par les spammeurs, revendue à des tiers et ensuite, tout ira malheureusement très vite.

Le mieux est d'avoir plusieurs adresses email :

- une adresse de votre FAI à divulguer uniquement à des correspondants de toute confiance, professionnels, famille ou amis
- une seconde adresse dédiée aux achats, aux inscriptions sur sites ou aux newsletters
- enfin, une adresse "jetable" facile à créer et à communiquer dans la foulée en cas de besoin

Malgré ces règles élémentaires, vous recevrez néanmoins encore des courriels non-sollicités ... il faut alors employer des règles de messagerie dans votre mailer (Outlook, Netscape ou autre).

Les webmasters doivent être particulièrement vigilants : JAMAIS d'adresse email sur une page web, c'est la porte ouverte au mail-bombing, cette invasion par milliers de mails qui saturent très vite une boite aux lettres et la rendent donc invalide. Non, il faut créer un formulaire qui exploitera un script de votre fournisseur afin d'être tout de même joignable par les visiteurs de votre site.

Si malgré tout, un spam arrive dans votre boite, n'y répondez pas ! ! car cela permettrait au spammeur de valider votre adresse et de la rendre encore plus exploitable.

N'achetez jamais rien, n'utilisez aucun service dont un spam fait la pub ! Les spammeurs spamment pour faire de l'argent. Si nous nous abstenons de leur en faire gagner par ce moyen, c'est nous qui gagnerons et qui nous libèrerons du spam !

---

3) Réagir au spam

En amont de la réception, vous pouvez déjà utiliser un logiciel qui permette d'interroger votre BAL, lire l'objet, l'expéditeur et de supprimer déjà pas mal de choses. Les gros fichiers non-sollicités et les virus potentiels seront aussi rapidement supprimés. Certains softs permettent même de "bouncer", c'est-à-dire de renvoyer à l'expéditeur son message, ce qui revient à invalider l'adresse.

MagicMail et MailWasher font partie de ces outils bien pratiques.

Utilisez un filtre de spam : il existe en effet des outils logiciels (payants et gratuits) permettant de screener l'origine du message et de le comparer à une black-list bien connue : SpamPal fonctionne ainsi. Il est gratuit. SpamTerminator est payant quant à lui

Bien sur, si un pourriel pénètre votre messagerie, il sera toujours intéressant de voir qui vous l'envoie. Pour cela, après analyse anti-virale, vous lirez les propriétés du mail et c'est là que vous pourrez avoir divers renseignements :

- adresse IP du serveur par lequel a transité le spam
- adresse IP du spammer
- serveur SMTP utilisé par le spammer
- nom réseau de l'ordinateur du spammer
- adresse où sera acheminée votre réponse éventuelle
- adresse présumée du spammer (peut avoir été supprimée ou falsifiée)
- votre adresse email
- objet du mail
- logiciel de mail utilisé par le spammer
- corps de l'email (où vous trouverez l'adresse du site web du spammeur)

Je rappelle qu'il faut toujours laisser votre logiciel antivirus en veille pour les messages entrants ; il est obligatoire de le mettre à jour très régulièrement (comme Norton et sa mise à jour automatique LiveUpdate), sinon, il ne connaît pas les derniers virus et son intérêt s'en trouvera limité.

Les spams ne sont pas à proprement parler des "virus" car ils ne détruisent rien sur votre configuration mais il faut toujours être extrêmement méfiant. Pour cela, désactivez dans les propriétés de sécurité d'Internet Explorer, les JavaScripts et n'ouvrez jamais de fichier-joint d'origine douteuse.

La réaction que l'on peut avoir est celle de la justice et donc de prévenir d'emblée le fournisseur d'accès web du spammeur. En effet, on peut toujours écrire à abuse@fournisseur.fr et il prendra toutes les mesures pour arrêter le manège de son client. Puis, si cela ne suffit pas, on peut amener l'affaire devant la justice mais les spammeurs envoient leurs messages depuis l'étranger et les lois internationales ne sont pas encore au point et surtout pas uniformes.

En conclusion, je pense qu'il faut surtout être méfiant et vivre dans l'ombre : ne divulguez pas votre adresse principale, utilisez les règles de messagerie, lancez Magicmail pour effacer à distance et laissez SpamPal faire le tri à votre place. On n'est jamais assez vigilant dans ce domaine et une adresse spammée devient très vite un dépotoir que l'on n'ouvrira plus

Imprimer cet article