

# Avoir son serveur de mail en interne

## ► GÉRER SON PROPRE SERVEUR DE MAIL

Le raccordement permanent par DSL ou câble permet le branchement d'un serveur de mail ; il est en effet à l'écoute 24 h/24 des mails entrants et est disponible à tout instant pour l'envoi vers l'extérieur. L'avantage de la connexion permanente a un revers qui est la fragilité aux attaques externes et un serveur de mail mal protégé est une proie de choix pour les spams.

Si vous choisissez d'avoir votre propre serveur de mail, VTX peut devenir votre serveur de mail secondaire. Il faut simplement inscrire (dans le serveur DNS sur lequel pointe le nom de domaine) l'adresse IP de votre serveur de mail en première position et celle de VTX en seconde (MX secondaire).

A noter : le serveur de mail VTX ne peut pas être utilisé comme serveur de mail sortant et nous appliquons des règles anti-spamming à nos propres serveurs.

## ► QU'EST-CE QUE LE SPAM ?

Le spam est l'équivalent sur Internet de la publicité non désirée que vous recevez dans votre boîte aux lettres. S'il est possible d'afficher un petit autocollant ad-hoc sur sa boîte aux lettres, ce n'est pas le cas pour son homologue électronique. Et dans ce cas, ce n'est pas une personne qui devra se déplacer pour remplir votre boîte et le risque de débordement est important, chacun en a fait l'expérience.

Sur Internet, l'étiquette est très stricte et tout message commercial même bien intentionné est considéré comme du spam. C'est une mesure de prévention avant que le réseau ne soit saturé par des millions de messages publicitaires.

## ► COMMENT SPAMER ?

La réponse à cette question permet de mieux comprendre comment chacun pourra se protéger de tels procédés.

Un individu ou une entreprise a quelque chose à vendre ou à promouvoir. Il s'agit tout d'abord de réunir des adresses mail par exemple en les glanant sur des forums de discussion, dans les mailing-lists ou en répertoriant les mailto dans les pages web ; la plupart du temps, les spammeurs n'ont pas ces compétences, alors le plus simple est de les acheter ; il existe un marché florissant de listes de millions de boîtes aux lettres.

L'étape suivante consistera en l'envoi du message. Envoyer des milliers de messages est une opération coûteuse: elle demande des ressources machine et aussi une bande passante importante. Pourquoi ne pas se servir chez des personnes qui laissent leur machine ouverte ? L'idée est simple, si simple qu'elle est devenue très courante. Pour trouver une telle machine, il suffit de parcourir les adresses des machines mail et d'essayer l'envoi d'un message en utilisant les ressources des machines répertoriées. La première qui accepte est aussitôt piégée par un mail dont on va demander la diffusion à quelques milliers d'exemplaires. Ce genre d'opération est généralement effectuée la nuit lorsque le serveur n'est pas sous surveillance, ce serait dommage de n'en profiter que quelques minutes.

Les heureux destinataires de ces messages seront incapables d'identifier la source réelle mais pourront très bien voir que le mail vient de tel serveur non protégé. Et le serveur en question va être réputé comme non sûr et ainsi commence une procédure informelle de mise au ban de la communauté Internet.

Les seuls bénéficiaires seront les expéditeurs de millions de messages qui vont bien récupérer quelques centaines de personnes qui auront pu être attirées par une offre alléchante.

## ► CHACUN EST PERDANT

Du côté de la victime qui reçoit ces mails, il y a une perte de temps certaine et un agacement qui peut se transformer rapidement en gêne.

Du côté du serveur, les conséquences sont bien plus graves rapidement ; un serveur spammé qui ne se protège pas le sera encore et toujours. On rentre ainsi dans une spirale qui fait que la bande passante attribuée ne suffit plus, que la machine doit être renforcée, sans compter les coûts de trafic. De plus, une personne devra se pencher a posteriori sur ces problèmes et répondre aux plaintes des victimes puis rentrer dans une démarche de levée de boycott. Dur chemin qui mérite une prévention d'ailleurs facile.

# Se protéger contre le spamming

## ► COMMENT PROTÉGER SON COMPTE ?

Il n'y a pas de solution miracle, le plus simple étant d'éviter de diffuser son adresse Email à tout va. Lorsque l'on reçoit un spam indiquant qu'il ne s'agit pas de spam car vous avez le choix de vous désabonner en faisant un simple "unsubscribe " à l'adresse [gogo@money.com](mailto:gogo@money.com), c'est le meilleur moyen de confirmer la validité de votre adresse. Notez bien que dans la plupart des cas, l'adresse de l'expéditeur est bien évidemment inconnue.

## ► COMMENT PROTÉGER SON SERVEUR ?

Il faut d'abord être conscient que chaque site peut potentiellement devenir source de spam. L'usage veut que l'adresse " Postmaster@site " soit obligatoire pour tout site abritant une messagerie. Une convention tend à se répandre : la création de l'adresse " abuse@site ", utilisée pour signaler les plaintes. Le simple fait de reconnaître et accepter cette adresse est déjà un gage de bonne volonté : vos correspondants sauront que vous êtes conscient du problème.

La précaution la plus importante est d'éviter le relais de messagerie. Il se trouve que, par défaut, la plupart des serveurs routent les messages sans distinction aucune de l'expéditeur. Ainsi, les spammeurs profitent de cette naïveté pour utiliser vos ressources et envoyer ainsi leurs millions de messages.

Le principe est donc simple : tout courrier provenant de l'extérieur du réseau local du serveur ne doit pas être livré à l'extérieur.

Un autre principe peut être mis en place : seul un utilisateur authentifié est autorisé à envoyer un message.

Vous trouverez ci-dessous quelques liens sur des sites pouvant vous aider à protéger votre système.

## ► MAIS QUE FAIT LA POLICE ?

Il existe justement plusieurs organismes relativement sérieux et terriblement efficaces comme <http://maps.vix.com>.

Ce sont des organismes à but non lucratif dont le seul objectif est de remédier aux dégâts causés par le spamming. Ils disposent d'une ribambelle de tests pour déterminer si un site est ouvert en relais de messagerie. Faut de moyens de pression directs, ils répertorient les sites mal configurés ou délibérément actifs dans le domaine du spam. Ces " black-lists " sont ainsi en libre consultation et chacun a le choix de s'y fier et de configurer son serveur de manière à refuser purement et simplement les messages émanant des systèmes montrés du doigt, ceci dans le but de protéger ses propres utilisateurs.

Il faut savoir que ces sites ne sont pas seulement de vils justiciers mais également une source de documentation très complète pour protéger tout type de serveur et nous vous invitons à vous y rendre.

## ► UN PEU DE VOCABULAIRE

Le terme spam viendrait d'un sketch des Monty Python dans lequel un groupe de vikings chante de plus en plus fort les louanges de Spam, une marque de corned-beef (<http://www.spam.com/>).

Pour les amateurs d'acronymes, une petite classification des courriers non sollicités en plusieurs catégories :

**UBE** (Unsolicited Bulk Email) : il s'agit des courriers non sollicités envoyés en masse, c'est-à-dire les spams. L'acronyme UBE est un terme générique, quel que soit le sujet (commercial, publicité, chaîne, propagande, etc.);

**UCE** (Unsolicited Commercial Email) : ce sont les courriers purement commerciaux. Tout courrier UCE n'est pas forcément envoyé à de multiples destinataires, donc tout UCE n'est pas forcément un spam ;

**MMF** (Make Money Fast) : les chaînes (interdites en France et aux USA entre autres pays), les recettes miracles pour devenir riche rapidement et sans effort, etc.

**MLM** (Multi-Level Marketing) : il s'agit d'une variante de la catégorie précédente, à savoir tous les schémas pyramidaux (analogues aux chaînes).

## QUELQUES LIENS UTILES

---

<http://www.cauce.org>

<http://spam.abuse.net/>

<http://www.cypango.net/spam>

Coalition Against Unsolicited Commercial Email

La référence

Une version en français

Références en français:

<http://www.prism.uvsq.fr/~pda/kit-jussieu/support/node33.html>