# Le Spam

CASES LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE

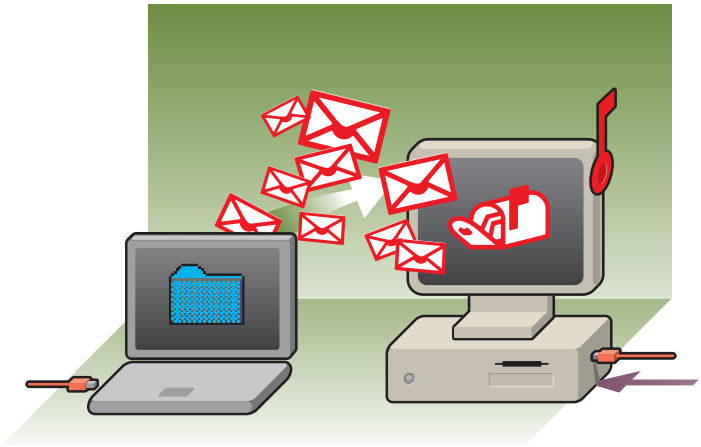
## Résumé

Ce terme a fait son apparition dans l'Internet, au niveau de l'Usenet, où il désignait des articles de news, envoyés en masse à différents newsgroups. Il s'agissait le plus souvent de messages publicitaires qui n'avaient rien à voir avec les newsgroups concernés.

Ce genre de publicité étant le plus souvent véhiculé par e-mail, le terme de spam ou de pourriel a fini par désigner également les e-mails non sollicités en masse. Techniquement, il serait plus juste de parler de UBE (Unsolicited Bulk E-Mail) ou de UCE (Unsolicited Commercial E-Mail).

## Table des matières





## 1 C'est quoi ?

Il n'existe pas de définition officielle du mot « Spam ». Le mot est, à l'origine, une marque anglaise de luncheon meat vendu en conserve. Ce sont les Monthy Pythons qui, dans un de leurs fameux sketchs où ils répétaient sans cesse le mot « Spam » dans une conversation, ont introduit la notion de désagrément.

Aujourd'hui, le mot « Spam » est communément utilisé pour caractériser un courrier électronique non sollicité envoyé en masse à une multitude de destinataires. Ce courrier provoquera donc une gêne pour les destinataires.

Ces courriers ne coûtent pratiquement rien pour l'expéditeur lequel ne génère qu'un seul message à l'adresse d'une multitude de destinataires. Par contre, ils peuvent coûter très cher aux destinataires, en terme de coût de connexion et de volume de transferts de données. On peut parler d'un véritable gaspillage de bande passante et d'espace de stockage pour les administrateurs de réseaux et de serveurs de messagerie mais aussi les destinataires des spams (particuliers ou entreprises) dans le temps passé et perdu à télécharger, trier et éliminer les spams reçus avec le risque d'éliminer par erreur un courrier qui n'est pas un spam.

## 2 Qui pratique le spamming ?

Un peu tout le monde, du simple particulier aux publicitaires et services marketing des entreprises, qui sont les premiers émetteurs de spams pour promouvoir leurs produits et services, ou pour inciter les internautes à visiter leur site web. Il y a quand même lieu de faire une distinction entre les spams ayant un but informatif ou publicitaire et ceux dont l'unique but est de nuire au système de messagerie électronique.

# Le Spam

CASES LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE

## 3 Comment se fait-il que je sois victime de «spam»

Le seul élément nécessaire pour faire de vous une victime potentielle de pourriels est votre adresse électronique (e-mail).

### 3.1 Méthodes de récupération d'adresse e-mail

Les spammeurs disposent de plusieurs moyens pour récupérer votre adresse électronique sur Internet (dans les forums, sur les sites Internet, dans les groupes de discussion, etc.), grâce à des logiciels (appelés « robots » ) parcourant les différentes pages et stockant au passage dans une base de données toutes les adresses e-mail y figurant.

Pour l'anecdote, Bill Gates reçoit 4 millions d'e-mail par jour dont la majorité sont des spams mais seulement 10 parviennent effectivement dans sa inbox, tous les autres étant filtrés par des solutions anti-spams. (source : BBC News – 18 nov. 2004)

**Votre adresse e-Mail a été vendue**
En revendant sa liste d'abonnés à un tiers, qui lui-même l'a revendue à un autre, etc., votre fournisseur d'accès Internet a permis la diffusion de votre adresse en de nombreux exemplaires sur Internet. Attention, l'opération est légale si vous avez accepté que votre adresse soit diffusée.

**Vous l'avez publiée sur Internet**
Vous avez affiché votre adresse électronique sur votre page personnelle ? Vous avez laissé votre adresse sur des forums de discussion sur le Web ou dans les newsgroups ? Sachez que des logiciels permettent de récolter automatiquement les adresses e-mail publiées. Dans tous ces cas, vous êtes susceptible d'intégrer un fichier d'adresses.

**Vous avez communiqué votre adresse à un site web**
En passant une commande sur un site de commerce électronique, en souscrivant à des services via un site web, en vous inscrivant sur une liste de diffusion par courrier électronique, vous avez forcément laissé une adresse e-mail. Si vous avez oublié de décocher la petite case qui figure en bas du formulaire, vous avez autorisé la diffusion de cette adresse.

**Votre adresse a été générée au hasard**
Prenez d'un côté les listes des noms et prénoms les plus courants, de l'autre celle de fournisseurs d'accès connus, en utilisant toutes les combinaisons possibles (prenom.nom, nom.prenom, nprenom, etc.), vous pouvez générer des centaines de milliers d'adresses e-mail, qui ont de fortes chances d'exister ! Et c'est ce que font certains spammeurs.

### 3.2 Exemple de spam


Objet : Make Easy Money from Home !
Brand New - Ultimate Business Opportunity !
Just Released World Wide !

Want an income independant of your job ?
Want To Be Your Own Boss and Own Your Own Business ?
Want To Easily make $200 - $1,000 per day... paid daily ?
Want To Earn Long Term Residual Income for Life ?
Want Unlimited Leads to Start Earning Big Immediately !
Click Here to learn more !

## 4 Comment se protéger ?

### 4.1 Surtout ne pas répondre à un message spam.

Les spammeurs utilisent généralement de fausses adresses d'envoi. Il est donc totalement inutile de répondre. De plus, si l'adresse de l'émetteur est correcte, vous ne feriez que renseigner cet émetteur sur la validité de votre adresse mail et recevoir plus de spams encore.

### 4.2 La meilleure solution reste la prévention.

- N'utilisez jamais publiquement l'adresse e-mail confiée par votre fournisseur d'accès ou votre entreprise, réservez-la à un cercle restreint d'amis ou des collègues en lesquels vous avez toute confiance.
- Vérifiez que votre adresse e-mail ne sera pas diffusée sans votre accord explicite. Certains fournisseurs d'accès ou prestataires peuvent automatiquement vous inscrire dans un annuaire web.
- Evitez au maximum la publication de votre adresse e-mail sur des forums ou des sites Internet.
- Créez une ou plusieurs « adresses poubelles » servant uniquement à vous inscrire ou vous identifier sur les sites jugés non dignes de confiance.
- En cas de doute, saisissez une fausse adresse ou maquillez votre véritable adresse en utilisant par exemple la Spam Safe Notation .

# Le Spam

CASES LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE

### 4.3 Surtout ne pas répondre à un message spam.

Il existe des dispositifs anti-spam permettant de repérer et, le cas échéant, de supprimer les messages indésirables sur la base de règles évoluées. On distingue généralement deux familles de logiciels anti-spam :

- Les dispositifs anti-spam côté client, situés au niveau du client de messagerie. Il s'agit généralement de systèmes possédant des filtres permettant d'identifier les spams, sur la base de règles prédéfinies ou d'un apprentissage. (Junk E-mail dans Outlook 2003)
- Les dispositifs anti-spam côté serveur, permettant un filtrage du courrier avant remise aux destinataires. Ce type de dispositif est de loin le meilleur, car il permet de stopper le courrier non sollicité en amont et d'éviter l'engorgement des réseaux et des boîtes aux lettres des internautes.

## 5 Comment vous protègent les fournisseurs d'accès?

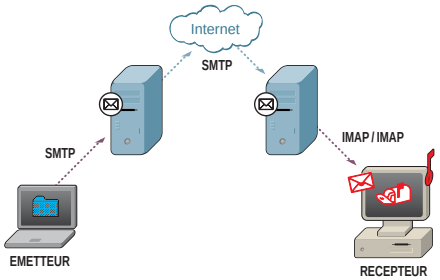
Les fournisseurs de services Internet se rendent bien sûr compte que les pourriels pourraient à l'avenir poser un problème de confiance en la solution technologique de courrier électronique. C'est dans ce but que la plupart d'entre eux mettent en place des solutions visant au filtrage des mails indésirables, par exemple l'utilisation des listes noires.

La qualité de la solution « anti-spam » peut devenir un réel différenciateur entre les fournisseurs pour les utilisateurs tant professionnels que privés.

Cette technique est également utilisable au niveau d'un ordinateur personnel mais elle demande une grande maîtrise de la part de l'utilisateur et une constante maintenance du paramétrage pour s'avérer fonctionnelle.

### 5.1 Comment l'e-mail fonctionne-t-il ?

Un courrier électronique est un flux de données d'un émetteur à un récepteur **transitant par des serveurs ou relais e-mails intermédiaires.** Le schéma suivant illustre ce mode de fonctionnement: Plusieurs protocoles de communication sont utilisés lors des opérations d'envoi et de réception.




Pour rappel, un protocole est un mode de communication déterminé entre deux entités leur permettant d'échanger des informations. Il s'agit ni plus ni moins d'un langage commun que deux entités (généralement un client et un serveur) utiliseront pour pouvoir effectuer un travail donné, dans ce cas-ci envoyer un e-mail.

Le protocole SMTP, utilisé par e-mail, **stocke par exemple la liste des serveurs qui ont relayé** le message électronique.

### 5.2 Quel est le principe des listes noires?

Les spams sont souvent envoyés avec une adresse de l'émetteur incorrecte. Généralement les serveurs de relay (e-mail serveurs) n'acceptent pas comme émetteur des adresses qui ne correspondent pas à leur domaine (p. exemple les P&T n'acceptent que des adresses @pt.lu). Certains serveurs mail ne font cependant pas ce contrôle (appelés open-relay servers). Ces serveurs sont par conséquent souvent utilisés pour envoyer du spam.

On peut trouver sur Internet des listes identifiant les producteurs ainsi que les « relayeurs » de spams. Ces derniers sont des serveurs de messagerie sur Internet qui permettent l'envoi de spams. Ceux-ci sont identifiés sur base de leur adresse IP et de leur domaine. Ces listes sont ensuite utilisées pour configurer les serveurs de messagerie de façon à interroger cette source d'informations et prendre une décision quant aux messages provenant d'émetteurs listés dans ces listes noires. La consultation s'effectue dans la majorité des cas via une requête de type DNS (service Internet assurant la conversion des noms de domaines en adresses IP et vice versa).

Si la réponse indique une source répertoriée comme émettrice de spams, le serveur n'a plus qu'à filtrer le mail. Rien ne s'oppose à ce qu'une autre technique de filtrage et d'analyse ne soit appliquée par la suite aux messages acceptés, par exemple sur leur contenu ou sur leur enveloppe.

### 5.3 Types de listes noires

On peut faire une première distinction entre les listes noires « locales » (par exemple au niveau d'une société ou même d'un internaute), dénommées Local Deny Lists, et les listes noires publiques interrogées à distance.

L'utilisation des listes noires locales nécessite maintenance et expertise de la part de l'utilisateur. Malheureusement, les outils de messagerie standards ne facilitent en rien leur administration.

Les listes publiques sont connues sous le nom de DNSBL (DNS Blackhole List), ou tout simplement listes noires. Certaines sont gratuites, tandis que d'autres sont proposées sous forme de service payant. Quelques-unes de ces listes noires se sont spécialisées selon les critères qui déterminent l'entrée dans la liste, ou selon leur type de fonctionnement. Les plus connues sont Spamcop, MAPS, DSBL, SPEWS ou ORDB.

# Le Spam

CASES LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE

## 5.4 Avantages et inconvénients

Le filtrage sur émetteur évite que le spam arrive sur les serveurs si le filtrage a lieu au niveau des fournisseurs d'accès à Internet. Il en découle des économies de bande passante, de stockage et de CPU. De plus, si on interroge une base locale, le recours à cette technique consomme peu de ressources et est donc rapide. C'est pour ces différentes raisons que le filtrage sur liste a été, et est encore, très utilisé par les fournisseurs d'accès Internet (ISP ou prestataires de messagerie). Très souvent, ces derniers détruisent simplement les messages provenant de listes noires.

## 5.5 Impact de la liste noire sur le poste de travail

L'utilisation de listes noires par les fournisseurs d'accès est souvent couplée avec une autre technique de filtrage. Il s'agit de l'authentification de l'utilisateur lors de l'envoi de messages.

Cette technique évite d'usurper le nom de domaine du fournisseur d'accès utilisant le serveur de messagerie en «Open-Relay» (technique utilisée par les hackers et spammeurs pour usurper une identité ou un domaine et relayer ainsi les messages spam). Cette précaution vise à éviter que le domaine du fournisseur d'accès ne soit déclaré dans les listes noires parce qu'utilisé par des pirates informatiques.

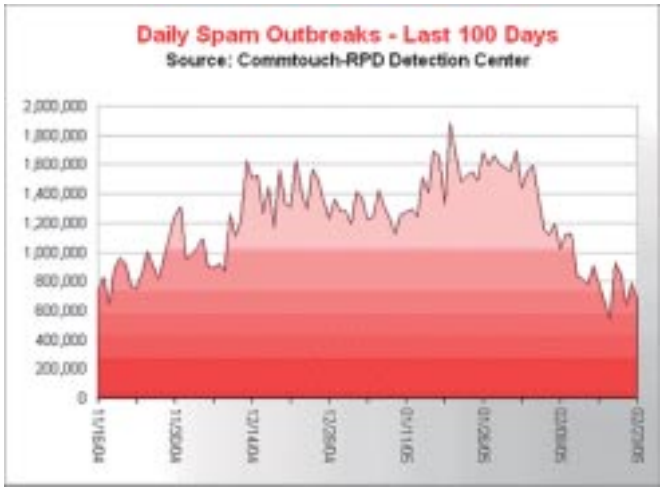
C'est cette technique qui oblige à tenir compte de l'authentification dans le paramétrage des comptes sur le logiciel de messagerie (MS Outlook par exemple). En effet, le serveur de messagerie du fournisseur d'accès autorise uniquement la connexion d'utilisateurs authentifiés par lui-même.

L'utilisation de cette authentification pose des problèmes lorsque l'accès à la messagerie se fait au travers d'un autre fournisseur d'accès (roaming) ne supportant l'authentification lors de l'envoi d'e-mail et peut entraîner de ce fait l'impossibilité d'envoyer des messages. La réception n'étant pas affectée par le mécanisme d'open relay, elle reste possible.

# 6 Le spam en quelques chiffres

## 6.1 Pays de provenance des spam en 2005

| Rang | Pays | Pourcentage |
|---|---|---|
| 1 | États-Unis | 56.7 % |
| 2 | Canada | 6.8 % |
| 3 | Chine | 6.2 % |
| 4 | Corée du Sud | 5.8 % |
| 5 | Pays-Bas | 2.1 % |
| 6 | Brésil | 2.0 % |
| 7 | Allemagne | 1.8 % |
| 8 | France | 1.5 % |




**Liens utiles :**

- http://spambayes.sourceforge.net/
  SpamBayes - plug-in anti-spam pour Microsoft Outlook 2000/XP sous Windows, mais aussi pour Linux et Mac OS
- http://prdownloads.sourceforge.net/mmm3/magic-2.94b10.zip?use_mirror=ovh
  Magic Mail Monitor - permet d'examiner le contenu de vos boîtes aux lettres directement sur le serveur et d'y supprimer d'éventuels messages parasites.
- http://spam.abuse.net/
  Fight Spam- excellent site sur le Spam
- http://www.spampal.org/
  SpamPal - logiciel qui s'installe sur le poste de travail qui permet de filtrer les messages reçus à l'aide de DNSBL. Les spams reçus ne sont pas supprimés mais taggés en ajoutant dans leur sujet la balise [SPAM] pour permettre de les classer facilement via Outlook.