

A photograph of two young boys playing under a large, leafy tree. The boy on the right is lifting the boy on the left. They are standing on a dirt ground in front of a bright yellow wall. The scene is brightly lit, suggesting a sunny day.

LUTTE CONTRE LES SPAMS

Présentateur : Pacôme ARCHER

Cordonnateur de l'activité Internet

Côte d'Ivoire Télécom

AGENDA

INTRODUCTION

LE SPAM

- HISTORIQUE
- Généralités
- La qualification
- Les impacts
- Les types de Spam

LA LUTTE CONTRE LE SPAM

- Les listes
- Les techniques
- Les filtres
- L'analyse des images
- L'aspect juridique

LES RECOMMANDATIONS

CONCLUSION



INTRODUCTION

Le courrier électronique ("e-mail) est devenu un mode de communication incontournable aussi bien dans les relations professionnelles qu'interpersonnelles. Cependant, le courrier électronique présente de nombreuses faiblesses du point de vue de la sécurité des données. En effet, nul n'est à l'abri d'interception, de piratage, de virus ou encore de pourriels (spams).

La prolifération du spam ces dernières années n'est plus à démontrer. Alors qu'en 2003, la part du spam était évaluée à 50% du trafic email mondial, les estimations pour les années 2008 et 2009, avoisinaient les 80%



LE SPAM



COTE D'IVOIRE TELECOM



HISTORIQUE

Le mot **Spam** est l'acronyme de Shoulder of Pork and hAM (épaule de porc et jambon).

Ce terme provient d'un sketch d'un groupe comique anglais qui faisant la pub d'un jambon en boîte de basse qualité répétait de façon réccurente (des centaines de fois) le nom du produit : SPAM

Le Spam est né en 1994 lorsque deux juristes Américains effectuent le premier e-mailing de masse vers quelques milliers de destinataires en vue de promouvoir leur société de conseil.

Le tournant décisif du Spam a pour origine l'épisode de l'anthrax, en 2001



GENERALITE

Le Spam est un message, généralement a caractère publicitaire que l'on reçoit de manière abondante sans avoir sollicité l'expéditeur. Actuellement le Spam par courrier électronique est le type de Spam le plus répandu et le plus gênant.

Il en existe d'autres types :

- par message de forum de discussion,
- par des fenêtres pop up,
- par SMS,
- par lettre postale.
- ...



LA QUALIFICATION

Voici les critères proposés pour qualifier le Spam :

1. **Nombre** : Défini par un envoi en masse.
 2. **Méthode de collecte** : Collecte illégale ou automatisée d'adresses emails.
 3. **Contenu** : Contenu a caractère offensant.
 4. **Enveloppe** : Falsification des entêtes, usurpation d'adresse.
- Pour un internaute, le critère principal est le contenu, dont il est seul juge (choquant, pornographique, dérangeant).
 - Pour les FAI et Opérateur Telecom, le nombre est le premier critère, puisque l'envoi massif peut endommager son infrastructure de service.



Il existe deux types de spam : avec du texte et avec des images
COTE D'IVOIRE TELECOM



LE COÛT LIÉ AU SPAM

Les coûts directs

- Les coûts liés à la réception et au stockage des courriers électroniques indésirables
- Les coûts liés au niveau de la largeur de la bande passante Internet (la messagerie utilise plus de 50% du trafic sur le réseau et que 72% de ce courrier s'avère être du spam)
- cas d'interruption de service, notamment de la messagerie, lié à la réception de spam (plus de réception des messages des fournisseurs et des clients)
- impossibilité d'envoyer les mails car le domaine et adresses IP de l'entreprise dans les blacklists



Les Coûts indirects

Les coûts liés à la baisse de productivité d'une entreprise

–Pour supprimer un spam: 10 secondes par message. Avec une moyenne d'environ 10 spams par jour (donnée minimaliste), le coût indirect lié au spam représente alors : $10 \text{ secondes} * 10 \text{ messages} * 20 \text{ jours} * 12 \text{ mois} = 24000 \text{ secondes}$ soit l'équivalent d'un jour plein sur l'année.

–la surcharge du service d'assistance de l'entreprise (help-desk) liée aux appels générés à cause de la réception de spams, qui peut être estimée à environ 1 heure par an et par utilisateur.

Les moyennes de **coûts globaux liés à la réception de spams** autour de **2,5 jours / homme par an**



LES IMPACTS

– Perte de l'information essentielle

Les Spams noient les messages importants au risque que ces derniers soient effacés par l'utilisateur ou par l'Antispam.

Dans certains cas, vos correspondants peuvent être dans l'impossibilité de vous adresser des e-mails dû à des blacklist intempestives ou un format de mail non conforme.

– Risque sécuritaire

Les Spams véhiculent en plus de la publicité pharmaceutique et pornographique, des tentatives d'intrusions, de détournements et de destructions (Virus, Backdoor, Fishing et etc)



LA LUTTE CONTRE LE SPAM



COTE D'IVOIRE TELECOM



LES LISTES : L'ANTISPAM

- **La liste noire** : contient les emails et adresses IP des spammeurs
- **La liste blanche** : on ne reçoit seulement les emails qui sont envoyés par les personnes incluses dans cette liste blanche.
- **La liste grise** : attente de validation avec un message de réponse automatique contenant un lien permettant de valider l'envoi ok : liste blanche Nok : liste noire



LES TECHNIQUES : L'ANTISPAM

– Les RBL:

RBL signifie Realtime Blackhole List et c'est une liste noire centralisée. Les listes RBL sont disponibles sur l'Internet via des serveurs qui collectent les adresses noires et les ajoutent dans leurs listes qu'ils partagent.

– L'enregistrement DNS PTR:

Tout serveur de messagerie doit posséder cet enregistrement ; requête DNS inverse (in-addr.arpa).

– L'authentification sur SMTP:

Pas efficace : Spam envoyés par des serveurs SMTP, des relais ouvert ou par des zombies.



LES FILTRES : L'ANTISPAM

Les messages mail se composent de deux sections principales:

- **L'entête** : Structuré dans des champs tels que le sommaire, l'expéditeur, le destinataire, et d'autres informations sur l'email.
- **Le contenu** : Le message lui-même en tant que texte non structuré; Il peut contenir parfois un bloc de signature à l'extrémité

Le filtre basé sur les entêtes

- Le taux d'efficacité de ce type de filtre est d'environ 50%.
- Cette technique présente l'avantage de pouvoir bloquer les mails avant même que leur contenu ne soit envoyé : diminuer grandement le trafic sur le relais SMTP



LES FILTRES : L'ANTISPAM

–Le filtre basé sur les mots clés

–Le filtre Bayésien

–Méthode probabiliste de filtrage des courriers électroniques fonctionnant par apprentissage et se basant sur la distribution statistique de mots clés dans les mails.

–Ce type d'algorithme utilise une base la plus hétérogène possible de spams et de hams (messages légitimes) afin d'être capable par la suite de reconnaître le type de message reçu

L'ANALYSE DES IMAGES pour la prise en compte des spams contenant des images.



EXEMPLE DE MISE EN QUARANTE

McAfee Email and Web Security Appliance

Récapitulatif des e-mails en quarantaine pour

exemple@aviso.ci

E-mails en quarantaine

Quarantaine de spam

Les e-mails ci-dessous ne figurent pas dans le dernier récapitulatif de contenus indésirables. Placés dans votre zone de quarantaine de contenus indésirables, ils seront supprimés après 2 jours. Sélectionnez tous les e-mails que vous voulez débloquer ou supprimer, puis cliquez sur Appliquer.

Action	Score	De	Objet	Date
	10	<moustyfof1@yahoo.fr>	Hello . l--%	ven 02 jui 2010 23:56:39 WET

Supprimer ▾

Appliquer



AU NIVEAU JURIDIQUE

- Pas de dispositions juridiques clairement définies en Côte d'Ivoire existant pour la lutte spécifique contre les spams (mise en place récemment d'une entité pour la lutte contre la cybercriminalité qui prend en compte certains aspects des spams)
- Le Parlement Européen a adopté une directive spécifique concernant le spam et l'envoi de courriers électroniques non sollicités, en faveur de l'opt-in (consentement préalable des internautes), **en juillet 2002**
- Comme exemple : en Hollande En octobre 2009, la mise en place d'une loi anti-spam a entraîné une chute de **85% dans les spams semi-légaux envoyés**. 39 entreprises ont reçu un avertissement officiel



LES RECOMMANDATIONS



COTE D'IVOIRE TELECOM



- **Pour les PARTICULIERS**

- Sécurisation des accès WIFI par des codes de sécurité
- Sécurisation de son poste de travail par les logiciels de sécurité (Anti-virus, firewall, Anti spyware, antisпам (pour éviter d'être un rebond : relayage SMPT et logiciel cheval de troie))

- **Pour les PROFESSIONNELS**

- Contrôler tout le trafic SMTP afin d'autoriser que les serveurs de messagerie relais identifiés pour l'envoi des mails
- Définir une politique de sécurité pour les différents services liés à la messagerie avec une mise à jour constante des procédures.
- Informer les utilisateurs sur les risques encourus par le non respect des différentes mesures de sécurité.
- Renforcer les aspects juridiques des contrats de souscription



- **8 conseils pratiques pour éviter les spams en entreprise**
- 1. Ne JAMAIS répondre à un spam, ne cliquez jamais sur un lien fourni par mail pour se désinscrire (validation de votre adresse)
- 2. N'achetez jamais le produit ou le service proposé par un spammeur (en vous inscrivant sans retenue sur des sites WEB)
- 3. Détenir au minimum 2 adresses emails. (utilisation privée et une autre pour inscriptions aux forums, salles de discussion, listes de mailing (yahoo, hotmail, gmail ...))
- 4. Ne jamais indiquer votre adresse mail privée sur des ressources accessibles par le grand public



5. Votre adresse privée doit être difficile à usurper (revoir la politique de nomenclature des e-mails en entreprise: [prenom.nom@entreprise.ci](#). Utilisation de nom générique commercial, technique ...)
6. Eviter de considérer votre adresse publique comme acquise. Considérez la plutôt comme temporaire
7. Dans le cas où votre adresse privée est découverte, n'hésitez pas à changer immédiatement
8. Assurez-vous que votre adresse électronique est [filtrée par une solution anti-spam](#). ou installer une solution [anti-spam](#) localement sur votre PC



CONCLUSION



COTE D'IVOIRE TELECOM



Ainsi, bien qu'il existe un arsenal juridique dans le monde interdisant le *spam*, la réalité témoigne de son insuffisance. Croire en l'éradication de cette pratique illégale paraît illusoire.

En revanche, les moyens de la limiter existent. Ils passent à la fois par l'exploitation des instruments juridiques (via l'utilisation de Signal Spam), l'utilisation des moyens techniques (tels que les filtres ...) mais aussi par un certain nombre de précautions que l'internaute doit prendre.



Devant les différentes conséquences engendrées par le développement des spams dans le monde la Côte d'Ivoire doit prendre des mesures urgentes au risque de se retrouver isolé du monde internet.

Reste à savoir quelle arme employer face au développement des *blue spams* qui sont des messages électroniques envoyés à travers le réseau bluetooth, et qui peuvent être reçus sur le téléphone portable en passant à côté d'un émetteur...





Merci !