Le spamming en question

Exemples illustrés et conseils pratiques

Novembre 2006

economie
SPF Economie, P.M.E., Classes moyennes et Energie

.be

Le spamming en question

Exemples illustrés et conseils pratiques

Novembre 2006

economie
SPF Economie, P.M.E., Classes moyennes et Energie

Consultation en ligne

Cette brochure peut être téléchargée gratuitement (au format pdf) sur le site Internet du Service public fédéral Economie, PME, Classes moyennes et Energie :

Version en français :
http://economie.fgov.be/information_society/spamming/home_fr.htm

Version en néerlandais :
http://economie.fgov.be/information_society/spamming/home_nl.htm

Version en allemand :
http://economie.fgov.be/information_society/spamming/home_de.htm

Version en anglais :
http://economie.fgov.be/information_society/spamming/home_en.htm

Service public fédéral Economie, P.M.E., Classes moyennes et Energie
Rue du Progrès, 50
B - 1210 BRUXELLES
N° d'entreprise : 0314.595.348
http://economie.fgov.be

tél. (02) 277 51 11

Pour les appels en provenance de l'étranger :
tél. + 32 2 277 51 11

Editeur responsable : Lambert VERJUS
Président du Comité de Direction
Rue du Progrès, 50
B-1210 BRUXELLES

Dépôt légal : D/2006/2295/107

0954-06

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

TABLE DES MATIERES

economie
SPF Economie, P.M.E., Classes moyennes et Energie

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

AVANT-PROPOS

Cette brochure présente les exemples de spam les plus fréquents qui relèvent notamment de l'arnaque, de l'escroquerie ou de la criminalité informatique, parfois bien organisée.

Il s'agit de ces spam qui peuvent vous causer de sérieux ennuis, vous faire perdre beaucoup d'argent voire présenter un danger pour votre santé, si vous avez la naïveté d'y répondre.

Une partie de cette brochure est également consacrée à certaines techniques d'envoi de courriers électroniques non sollicités qui présentent, certes, un degré de dangerosité largement inférieur aux spam les plus classiques mais qui peuvent, dans certaines hypothèses, poser des difficultés au regard de l'application de la loi.

La liste d'exemples n'est pas exhaustive mais elle essaye de présenter les techniques les plus fréquentes, de les illustrer et de donner des conseils pratiques, afin que vous ne tombiez pas dans le piège à votre tour.

Cette brochure a été rédigée par Didier GOBERT dans le cadre des travaux de lutte contre le spam menés par le SPF Economie, PME, Classes moyennes et Energie ainsi que dans le cadre de la collaboration au sein du groupe de réflexion informel SpamSquad (www.spamsquad.be). Je tiens à le remercier ainsi que les collègues de la Direction générale de la Régulation et de l'Organisation du marché, de la Direction générale du Contrôle et de la Médiation, de la Direction générale du Potentiel économique du SPF Economie, les collaborateurs de la Direction générale Médicaments du SPF Santé publique et enfin les membres du groupe SpamSquad pour leur relecture attentive et leurs remarques constructives.

J'espère que grâce à cette brochure, vous ne vous ferez pas (plus) attraper.

Une personne avertie en vaut deux !

Robert GEURTS

Directeur général de la Direction générale de la Régulation et de l'Organisation du marché

economie
SPF Economie, P.M.E., Classes moyennes et Energie

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

LE SPAMMING EN QUESTION : EXEMPLES ILLUSTRÉS ET CONSEILS PRATIQUES

Introduction

Le terme spamming est plus souvent utilisé qu'il n'est défini. Il existe d'ailleurs une grande variété de « spam », qui peuvent tomber sous le coup de législations différentes (loi sur le commerce électronique, loi relative à la vie privée, loi relative à la criminalité informatique, code pénal, lois relatives à la protection du consommateur, loi relative à la publicité pour les médicaments, etc.).

Au sens large, ce terme désigne l'envoi de messages électroniques non sollicités. Bien que ce ne soit pas systématiquement le cas, les caractéristiques du spamming sont globalement les suivantes :

- les messages non sollicités sont envoyés de manière massive et parfois répétée ;
- le message poursuit parfois un objectif commercial (la promotion d'un produit ou d'un service) ;
- les adresses sont souvent obtenues à l'insu du propriétaire (en violation des règles relatives à la vie privée) ;
- il est en outre assez fréquent que, d'une part, le message ait un contenu illégal, trompeur et/ou préjudiciable et, d'autre part, l'expéditeur masque son identité ou utilise une fausse identité.

Si le courrier électronique classique est le véhicule le plus utilisé par les spammeurs, on constate que ce phénomène se répand de plus en plus sur d'autres canaux, tels la messagerie instantanée (on parle alors de « spim »), les blogs, les sms, etc.

Le but de cette brochure est double.

Premièrement, la brochure vise avant tout à présenter les exemples de spam les plus fréquents qui relèvent notamment de l'arnaque, de l'escroquerie ou de la criminalité informatique, parfois bien organisée.

Il s'agit de ces spam qui peuvent vous causer de sérieux ennuis, vous faire perdre beaucoup d'argent voire présenter un danger pour votre santé, si vous aviez la naïveté d'y répondre.

La liste d'exemples n'est pas exhaustive. En effet, de nouvelles formes de spam apparaissent régulièrement. Mais cette liste essaye de présenter les différentes

techniques utilisées, de les illustrer et de donner des conseils pratiques. L'objectif consiste à ce que vous ne tombiez pas dans le piège à votre tour.

Nous nous sommes limités aux cas suivants :

1. La lettre nigériane ou « scam africain » ;
2. Le « phishing » ou hameçonnage ;
3. Les messages électroniques qui vous garantissent... de perdre de l'argent ;
4. Les messages électroniques spécialisés dans.... les faux produits et les produits contrefaits ;
5. Les messages électroniques peu soucieux de votre santé ;
6. Les messages électroniques qui répandent des virus informatiques ;
7. Les messages électroniques qui véhiculent des arnaques classiques.

On peut sans difficulté dire que ces spam présentent un **degré de dangerosité élevé**. Ils font l'objet de la première partie de cette brochure.

Le second objectif de cette brochure vise à illustrer deux pratiques d'envoi de courriers électroniques non sollicités, qui présentent **un degré de dangerosité largement inférieur** aux spam les plus classiques (visés ci-dessus). Mais elles peuvent, dans certaines hypothèses, poser des difficultés au regard de l'application de la loi ou présenter certains risques. Il s'agit des deux pratiques suivantes :

1. Les « hoax », canulars ou rumeurs ;
2. Les messages électroniques qui vous associent – bien malgré vous – à une campagne publicitaire de marketing viral.

A ces deux catégories, on pourrait en ajouter une troisième : il s'agit des messages électroniques publicitaires envoyés par des entreprises réputées sérieuses, qui n'auraient néanmoins pas respecté les règles en matière de consentement préalable, d'identification du caractère publicitaire du message ou d'informations relatives au droit d'opposition.

Certes, il s'agit d'infractions à la loi, et l'autorité publique veille à réduire au maximum celles-ci en entamant les poursuites si nécessaire. Mais il faut ici aussi reconnaître que ces infractions constituent davantage une nuisance que des dangers comme celles qui sont présentées dans la première partie de cette brochure.

Cette troisième catégorie n'est pas abordée dans la présente brochure car elle fait déjà l'objet de la brochure « Le spamming en 24 questions et réponses » disponible

en ligne : www.economie.fgov.be/information_society/spamming/home_fr.htm, à laquelle nous renvoyons le lecteur.

Ces trois catégories de pratiques présentent un **degré de dangerosité limité**. Ils font l'objet de la seconde partie de cette brochure.

Notre intention n'est certainement pas de donner une image négative de l'Internet et du courrier électronique. Il ne faut d'ailleurs pas généraliser le phénomène.

Il est évident que le courrier électronique apparaît de plus en plus comme le moyen de communication privilégié, tant en raison de son coût modique, de sa rapidité et de sa facilité d'utilisation. En outre, Internet s'impose de plus en plus comme une nouvelle plate-forme sur laquelle de nombreuses sociétés sérieuses font du commerce de façon identique au monde réel, c'est-à-dire de manière totalement correcte et honnête.

Mais il est vrai aussi que, sur Internet comme ailleurs, des escrocs sévissent et sont à la recherche de personnes mal informées ou naïves afin de les « plumer ». Nous espérons que grâce à cette brochure, vous n'en ferez pas ou plus partie...

Une personne avertie en vaut deux !

Préliminaire : rappel de quelques principes de prudence !

Avant d'aborder les exemples concrets, il nous semble bon de rappeler quelques conseils élémentaires de prudence pour éviter ou, à tout le moins, limiter la réception de spam :

- soyez vigilant(e) lorsque vous communiquez votre adresse électronique et évitez de la communiquer sans raison à n'importe qui ;
- évitez d'afficher votre adresse électronique sur un site web, car celle-ci sera systématiquement copiée par un logiciel de « capture automatique d'adresses » utilisé par les spammeurs ;
- si vous voulez éviter que du « spam » arrive sur votre adresse électronique principale (que vous utilisez avec vos proches ou dans vos relations professionnelles), créez une seconde adresse auprès d'un fournisseur gratuit. Vous pourrez alors utiliser celle-ci dans le cadre d'applications plus risquées au regard du « spam » (inscription à des newsletters, participation à des forums, commande sur des sites web commerciaux, affichage sur votre page web, etc.) ;
- si l'origine du message ou l'identité de l'émetteur vous paraissent clairement douteuses, évitez de répondre à ce « spam », même si on vous donne la pos-

sibilité d'exercer votre droit d'opposition ! Evitez aussi de cliquer sur les liens hypertextes insérés dans le corps du message car les spammeurs malintentionnés utilisent ces techniques pour vérifier si votre adresse e-mail est encore active et... pour vous envoyer encore plus de « spam » !

- ne rendez pas visibles les adresses e-mails de vos correspondants lorsque vous créez un groupe ou une liste de diffusion, ou que vous transférez un e-mail. Il est donc nécessaire de masquer les adresses de l'ensemble des destinataires dans le cas de l'envoi simultané d'un même message à plusieurs personnes. Pour cela, utilisez lors de l'envoi d'un message la fonctionnalité "copie cachée" de votre logiciel de messagerie, le plus souvent symbolisée par « Cci » ou « BCC » ou « CCC » ;
- ne communiquez pas à des tiers des adresses e-mail d'autres personnes (proches, connaissances professionnelles, etc.) sans le consentement de ces dernières ;
- lorsque l'émetteur du message n'est pas clairement identifié et connu par vous, évitez d'ouvrir un fichier joint au message (surtout s'il porte l'extension .src, .exe, .scr) car il peut s'agir d'un virus ;
- ne participez pas à une chaîne d'e-mails ;
- installez un bon pare-feu et anti-virus, mettez les régulièrement à jour et scanner régulièrement votre (vos) disque(s) dur(s) ;
- sensibilisez vos enfants aux règles précédentes et à l'utilisation qu'ils peuvent faire de leur adresse électronique (idéalement différente de la vôtre !).

Pour des sources d'informations très complètes sur la question du spam et des arnaques véhiculées par ce biais, nous renvoyons le lecteur à quelques sites web de référence :

- Le site web du SPF Economie (www.economie.fgov.be), et particulièrement la page relative à la prévention des arnaques (www.economie.fgov.be/protection_consumer/fraud_prevention/home_fr.htm) ainsi que celle relative au spam (www.economie.fgov.be/information_society/spamming/home_fr.htm) ;
- Le site web de la « Federal Computer Crime Unit » de la Police fédérale (www.fccu.be/crim/crim_fccu_fr.php) ;
- Le site web « SpamSquad » (www.spamsquad.be) ;
- Le site web « Arnaques » du Centre de Recherches et d'Information des Organisations de Consommateurs (www.arnaques.be)
- Le site web « Hoaxbuster » (www.hoaxbuster.com).

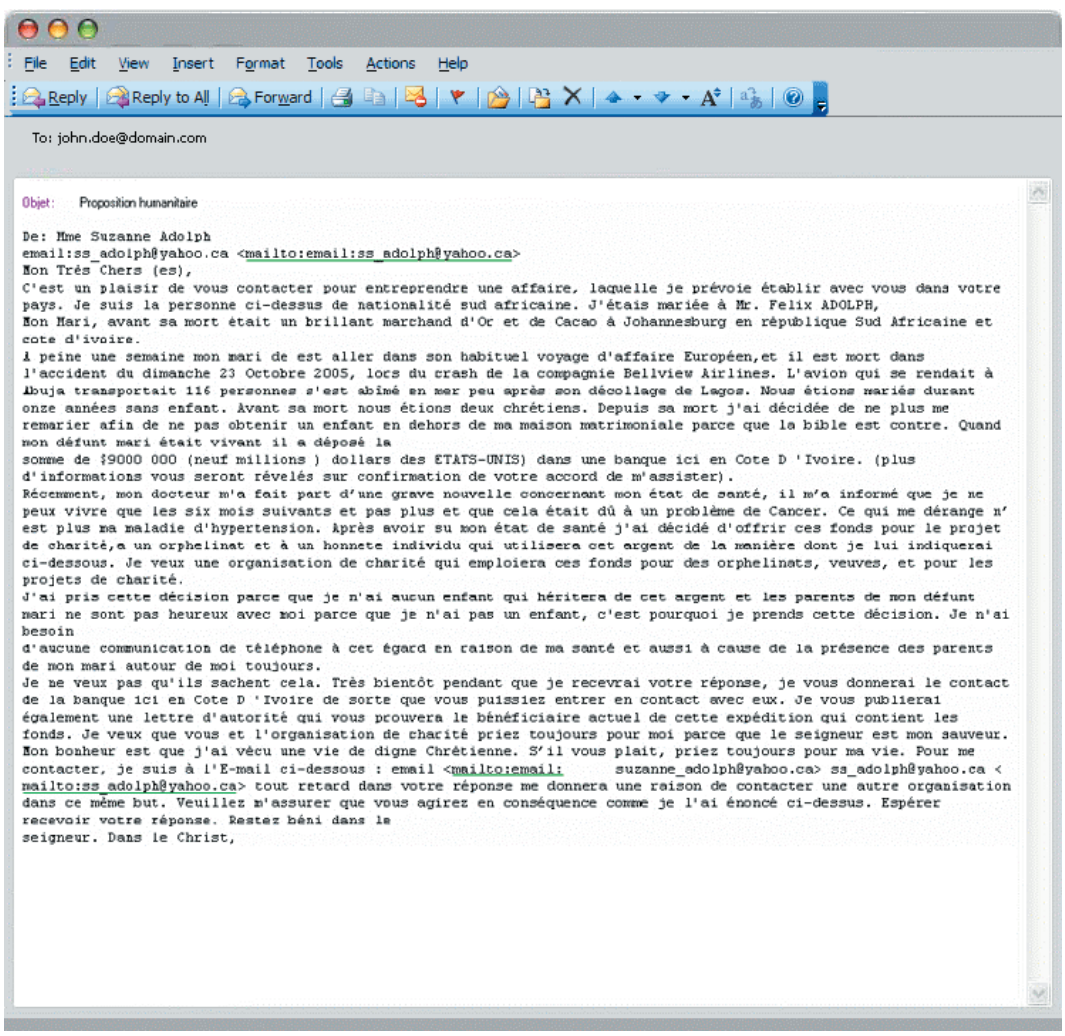
« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

PARTIE 1 : LES SPAM À DEGRÉ DE DANGEROSITÉ ÉLEVÉ

1. La lettre nigériane ou « scam africain »

Illustrations

Exemple 1 de lettre nigériane


File Edit View Insert Format Tools Actions Help

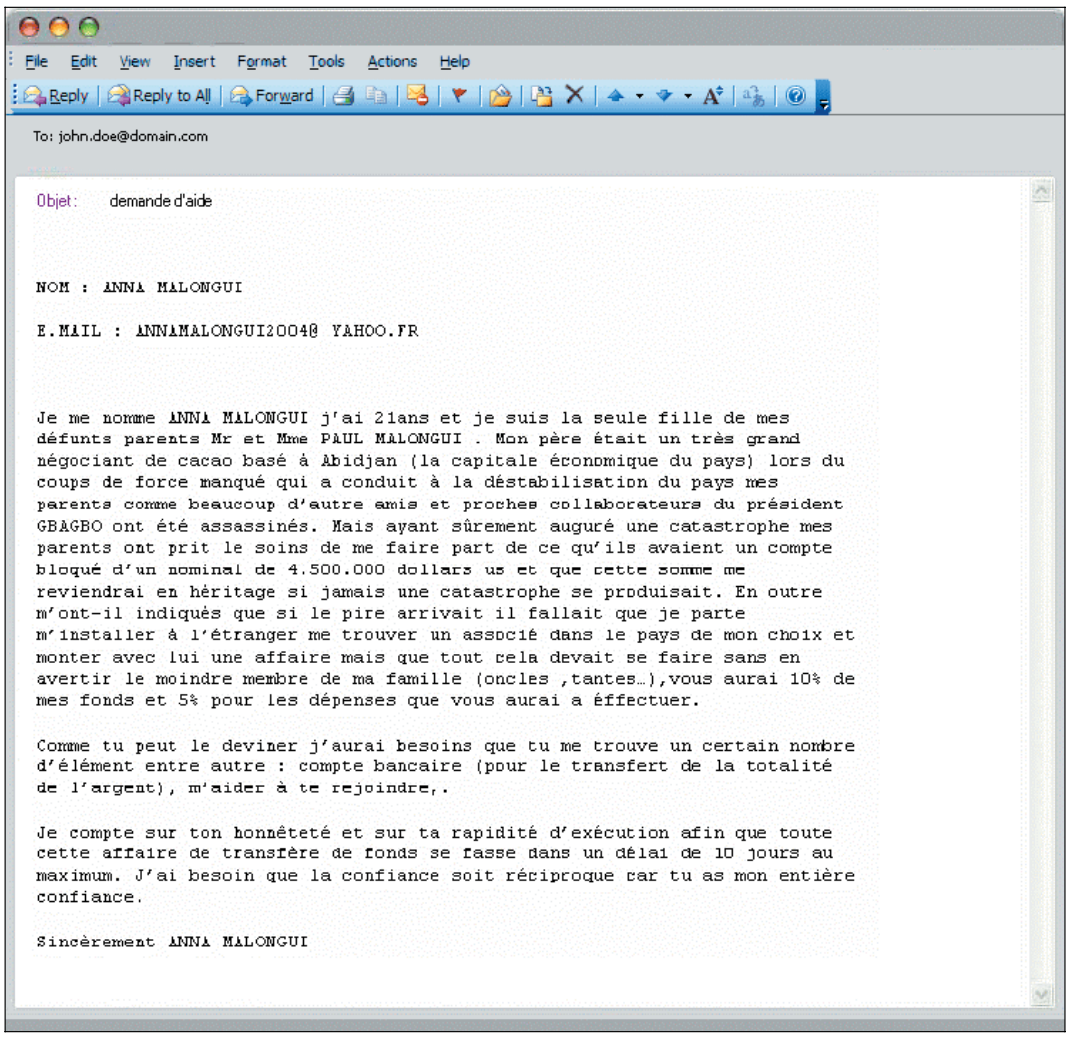
Reply | Reply to All | Forward

To: john.doe@domain.com

Objet: Proposition humanitaire

De: Mme Suzanne Adolph
email:ss_adolph@yahoo.ca <mailto:email:ss_adolph@yahoo.ca>
Mon Très Chers (es),
C'est un plaisir de vous contacter pour entreprendre une affaire, laquelle je prévoie établir avec vous dans votre pays. Je suis la personne ci-dessus de nationalité sud africaine. J'étais mariée à Mr. Felix ADOLPH, Mon Mari, avant sa mort était un brillant marchand d'Or et de Cacao à Johannesburg en république Sud Africaine et cote d'ivoire.
A peine une semaine mon mari de est aller dans son habituel voyage d'affaire Européen,et il est mort dans l'accident du dimanche 23 Octobre 2005, lors du crash de la compagnie Bellview Airlines. L'avion qui se rendait à Abuja transportait 116 personnes s'est abîmé en mer peu après son décollage de Lagos. Nous étions mariés durant onze années sans enfant. Avant sa mort nous étions deux chrétiens. Depuis sa mort j'ai décidée de ne plus me remarier afin de ne pas obtenir un enfant en dehors de ma maison matrimoniale parce que la bible est contre. Quand mon défunt mari était vivant il a déposé la
somme de $9000 000 (neuf millions) dollars des ETATS-UNIS) dans une banque ici en Cote D 'Ivoire. (plus d'informations vous seront révelés sur confirmation de votre accord de m'assister).
Récemment, mon docteur m'a fait part d'une grave nouvelle concernant mon état de santé, il m'a informé que je ne peux vivre que les six mois suivants et pas plus et que cela était dû à un problème de Cancer. Ce qui me dérange n' est plus ma maladie d'hypertension. Après avoir su mon état de santé j'ai décidé d'offrir ces fonds pour le projet de charité,a un orphelinat et à un honnete individu qui utilisera cet argent de la manière dont je lui indiquerai ci-dessous. Je veux une organisation de charité qui emploiera ces fonds pour des orphelinats, veuves, et pour les projets de charité.
J'ai pris cette décision parce que je n'ai aucun enfant qui héritera de cet argent et les parents de mon défunt mari ne sont pas heureux avec moi parce que je n'ai pas un enfant, c'est pourquoi je prends cette décision. Je n'ai besoin
d'aucune communication de téléphone à cet égard en raison de ma santé et aussi à cause de la présence des parents de mon mari autour de moi toujours.
Je ne veux pas qu'ils sachent cela. Très bientôt pendant que je recevrai votre réponse, je vous donnerai le contact de la banque ici en Cote D 'Ivoire de sorte que vous puissiez entrer en contact avec eux. Je vous publierai également une lettre d'autorité qui vous prouvera le bénéficiaire actuel de cette expédition qui contient les fonds. Je veux que vous et l'organisation de charité priez toujours pour moi parce que le seigneur est mon sauveur. Mon bonheur est que j'ai vécu une vie de digne Chrétienne. S'il vous plait, priez toujours pour ma vie. Pour me contacter, je suis à l'E-mail ci-dessous : email <mailto:email: suzanne_adolph@yahoo.ca> ss_adolph@yahoo.ca <mailto:ss_adolph@yahoo.ca> tout retard dans votre réponse me donnera une raison de contacter une autre organisation dans ce même but. Veuillez m'assurer que vous agirez en conséquence comme je l'ai énoncé ci-dessus. Espérer recevoir votre réponse. Restez béni dans le
seigneur. Dans le Christ,

Exemple 2 de lettre nigériane



File Edit View Insert Format Tools Actions Help

Reply | Reply to All | Forward

To: john.doe@domain.com

Objet : demande d'aide

NOM : ANNA MALONGUI

E.MAIL : ANNAMALONGUI2004@ YAHOO.FR

Je me nomme ANNA MALONGUI j'ai 21ans et je suis la seule fille de mes défunts parents Mr et Mme PAUL MALONGUI . Mon père était un très grand négociant de cacao basé à Abidjan (la capitale économique du pays) lors du coups de force manqué qui a conduit à la déstabilisation du pays mes parents comme beaucoup d'autre amis et proches collaborateurs du président GBAGBO ont été assassinés. Mais ayant sûrement auguré une catastrophe mes parents ont prit le soins de me faire part de ce qu'ils avaient un compte bloqué d'un nominal de 4.500.000 dollars us et que cette somme me reviendrai en héritage si jamais une catastrophe se produisait. En outre m'ont-il indiqués que si le pire arrivait il fallait que je parte m'installer à l'étranger me trouver un associé dans le pays de mon choix et monter avec lui une affaire mais que tout cela devait se faire sans en avertir le moindre membre de ma famille (oncles ,tantes…),vous aurai 10% de mes fonds et 5% pour les dépenses que vous aurai a éffectuer.

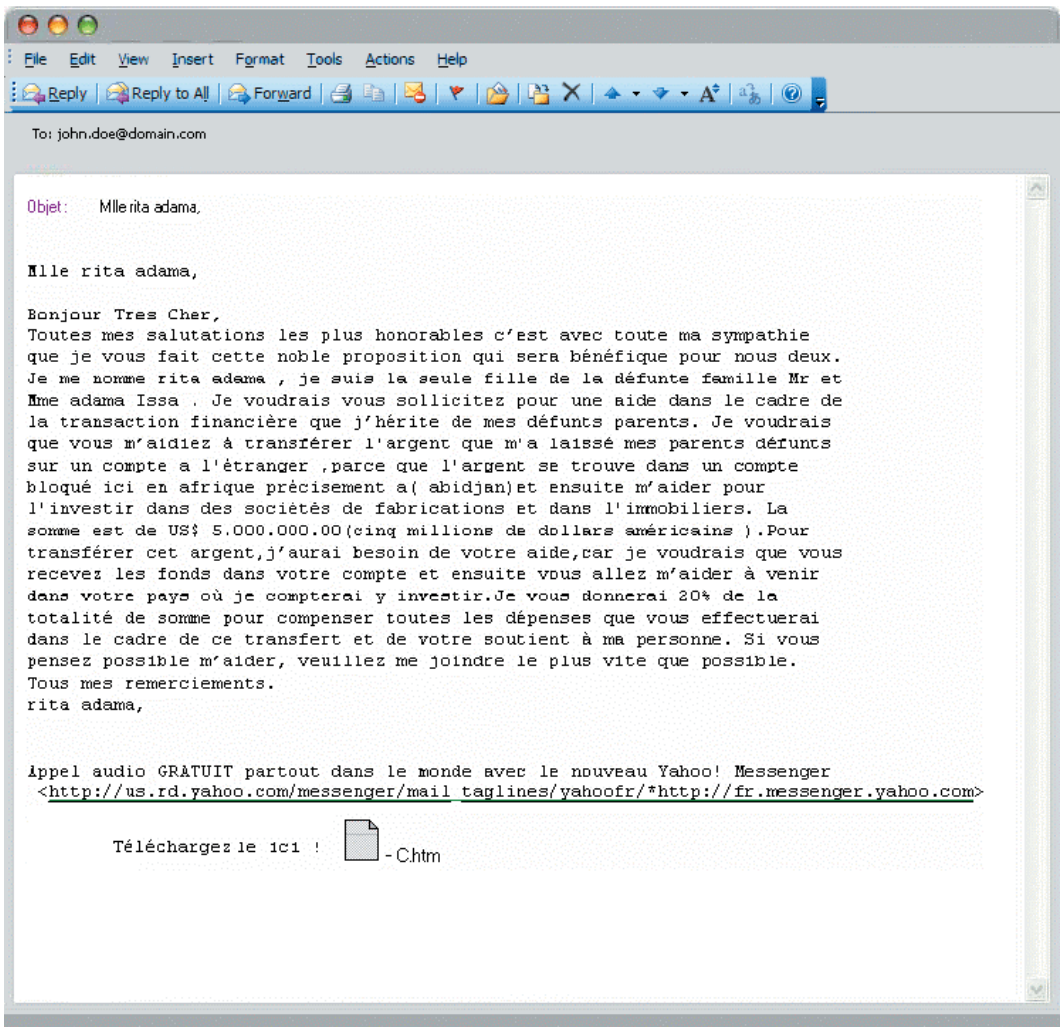
Comme tu peut le deviner j'aurai besoins que tu me trouve un certain nombre d'élément entre autre : compte bancaire (pour le transfert de la totalité de l'argent), m'aider à te rejoindre,.

Je compte sur ton honnêteté et sur ta rapidité d'exécution afin que toute cette affaire de transfère de fonds se fasse dans un délai de 10 jours au maximum. J'ai besoin que la confiance soit réciproque car tu as mon entière confiance.

Sincèrement ANNA MALONGUI

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

Exemple 3 de lettre nigériane



File Edit View Insert Format Tools Actions Help

Reply | Reply to All | Forward

To: john.doe@domain.com

Objet : Mlle rita adama,

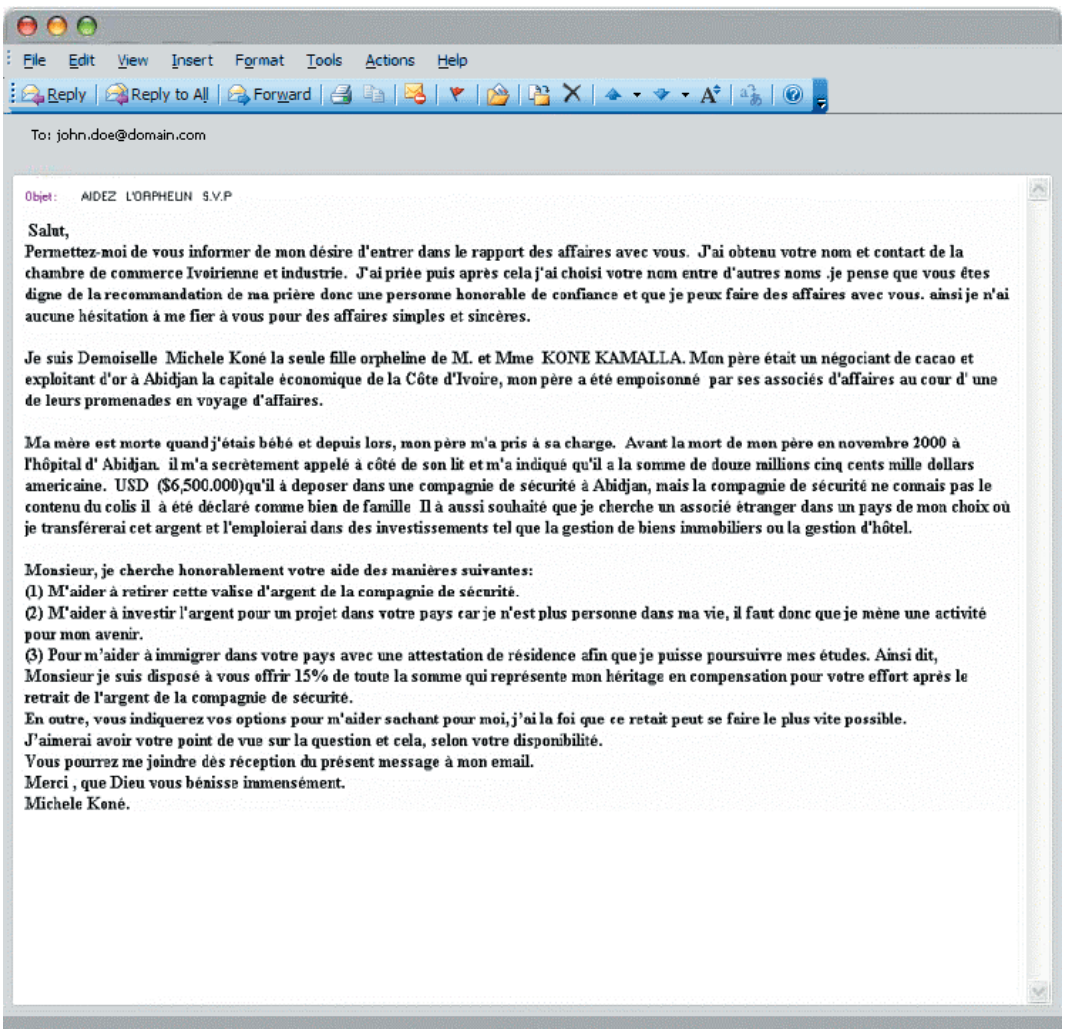
Mlle rita adama,

Bonjour Tres Cher,
Toutes mes salutations les plus honorables c'est avec toute ma sympathie
que je vous fait cette noble proposition qui sera bénéfique pour nous deux.
Je me nomme rita adama , je suis la seule fille de la défunte famille Mr et
Mme adama Issa . Je voudrais vous sollicitez pour une aide dans le cadre de
la transaction financière que j'hérite de mes défunts parents. Je voudrais
que vous m'aidiez à transférer l'argent que m'a laissé mes parents défunts
sur un compte a l'étranger ,parce que l'argent se trouve dans un compte
bloqué ici en afrique précisement a(abidjan)et ensuite m'aider pour
l'investir dans des sociétés de fabrications et dans l'immobiliers. La
somme est de US$ 5.000.000.00(cinq millions de dollars américains).Pour
transférer cet argent,j'aurai besoin de votre aide,car je voudrais que vous
recevez les fonds dans votre compte et ensuite vous allez m'aider à venir
dans votre pays où je compterai y investir.Je vous donnerai 20% de la
totalité de somme pour compenser toutes les dépenses que vous effectuerai
dans le cadre de ce transfert et de votre soutient à ma personne. Si vous
pensez possible m'aider, veuillez me joindre le plus vite que possible.
Tous mes remerciements.
rita adama,

Appel audio GRATUIT partout dans le monde avec le nouveau Yahoo! Messenger
<http://us.rd.yahoo.com/messenger/mail_taglines/yahoofr/*http://fr.messenger.yahoo.com>

Téléchargez le ici ! - C.htm

Exemple 4 de lettre nigériane



File Edit View Insert Format Tools Actions Help

Reply | Reply to All | Forward

To: john.doe@domain.com

Objet : AIDEZ L'ORPHELIN S.V.P

Salut,
Permettez-moi de vous informer de mon désire d'entrer dans le rapport des affaires avec vous. J'ai obtenu votre nom et contact de la chambre de commerce Ivoirienne et industrie. J'ai priée puis après cela j'ai choisi votre nom entre d'autres noms .je pense que vous êtes digne de la recommandation de ma prière donc une personne honorable de confiance et que je peux faire des affaires avec vous. ainsi je n'ai aucune hésitation à me fier à vous pour des affaires simples et sincères.

Je suis Demoiselle Michele Koné la seule fille orpheline de M. et Mme KONE KAMALLA. Mon père était un négociant de cacao et exploitant d'or à Abidjan la capitale économique de la Côte d'Ivoire, mon père a été empoisonné par ses associés d'affaires au cour d' une de leurs promenades en voyage d'affaires.

Ma mère est morte quand j'étais bébé et depuis lors, mon père m'a pris à sa charge. Avant la mort de mon père en novembre 2000 à l'hôpital d' Abidjan. il m'a secrètement appelé à côté de son lit et m'a indiqué qu'il a la somme de douze millions cinq cents mille dollars americaine. USD ($6,500.000)qu'il à deposer dans une compagnie de sécurité à Abidjan, mais la compagnie de sécurité ne connais pas le contenu du colis il à été déclaré comme bien de famille Il à aussi souhaité que je cherche un associé étranger dans un pays de mon choix où je transférerai cet argent et l'emploierai dans des investissements tel que la gestion de biens immobiliers ou la gestion d'hôtel.

Monsieur, je cherche honorablement votre aide des manières suivantes:
(1) M'aider à retirer cette valise d'argent de la compagnie de sécurité.
(2) M'aider à investir l'argent pour un projet dans votre pays car je n'est plus personne dans ma vie, il faut donc que je mène une activité pour mon avenir.
(3) Pour m'aider à immigrer dans votre pays avec une attestation de résidence afin que je puisse poursuivre mes études. Ainsi dit, Monsieur je suis disposé à vous offrir 15% de toute la somme qui représente mon héritage en compensation pour votre effort après le retrait de l'argent de la compagnie de sécurité.
En outre, vous indiquerez vos options pour m'aider sachant pour moi, j'ai la foi que ce retait peut se faire le plus vite possible.
J'aimerai avoir votre point de vue sur la question et cela, selon votre disponibilité.
Vous pourrez me joindre dès réception du présent message à mon email.
Merci , que Dieu vous bénisse immensément.
Michele Koné.

Explication

La lettre nigériane ou « scam africain » est une des arnaques les plus anciennes reçue sur l'adresse de courrier électronique. Et pourtant, cela n'empêche pas ce type de message de diminuer. Il ne nous est évidemment pas possible de tous les répertorier dans cette brochure (il y en aurait plus de 150 variantes répertoriées à ce jour !). Toutefois, il nous semblait utile d'en présenter les principales caractéristiques.

Que ce soit en anglais, en français ou dans d'autres langues, les messages ont de nombreux points communs :

- Ils se présentent tous à l'identique (l'ex femme de; le fils de; le colonel de; le frère de; etc... d'une personne soit disant fortunée qui vient de mourir, de disparaître ou est en prison) ;
- Les personnes qui vous contactent sont toutes en possession d'une importante somme d'argent (ou des diamants, ou de l'or, etc...) qui est stockée quelque part et qui n'attend que vous pour effectuer un transfert de fonds ou le déblocage du « trésor » ;
- Ils vous demandent votre aide et en échange promettent de vous rétribuer largement pour ce service rendu.

Et pourtant, ils ont tous le même but : vous extorquer de l'argent !

Si vous décidez de réagir à ce message, vous recevez rapidement tous les détails de l'affaire et une sollicitation à vous engager un peu plus loin. Seulement attention, plus vous rentrerez dans le jeu, plus il vous sera difficile d'en sortir et une fois repéré(e) vous risquez gros, très gros.

En effet, les émetteurs du message vont par exemple vous demander d'ouvrir un compte dans une banque étrangère (compte qui devra être approvisionné d'une somme relativement importante) voire dans votre pays (le compte ouvert à votre nom pourrait alors être utilisé en transit pour blanchir de l'argent sale !).

Il est également possible que vous deviez avancer de l'argent pour payer « certains » frais d'avocats, droits de transactions, taxes ou encore divers pots-de-vin, pour surmonter tous les obstacles qui ne manqueront pas de se dresser entre la grosse somme d'argent promise et vous.

Les escrocs pourraient encore se servir de votre numéro de compte et de vos coordonnées bancaires pour émettre de faux virements ou de faux chèques à votre nom.

Il est évident qu'après avoir ouvert ce compte en banque et/ou payé ces sommes d'argent, vous n'aurez plus aucune nouvelle des émetteurs et ne verrez plus jamais la couleur tant de votre argent que de la somme promise ! Il est en outre possible que vous soyez poursuivi(e) pour complicité relative à une opération de blanchiment d'argent.

Comment réagir ?

Le conseil est simple mais impératif : surtout, ne répondez jamais à ce courrier électronique très facilement reconnaissable et détruisez le directement.

Si vous avez malheureusement réagi à ce mail, pris un premier contact voire été plus loin, prenez immédiatement contact avec la Federal Computer Crime Unit de la Police fédérale pour expliquer la situation à l'adresse : contact@fccu.be.

Pour en savoir plus

Le site web : www.hoaxbuster.com ;

Le site web : http://onguardonline.gov/spam.html ;

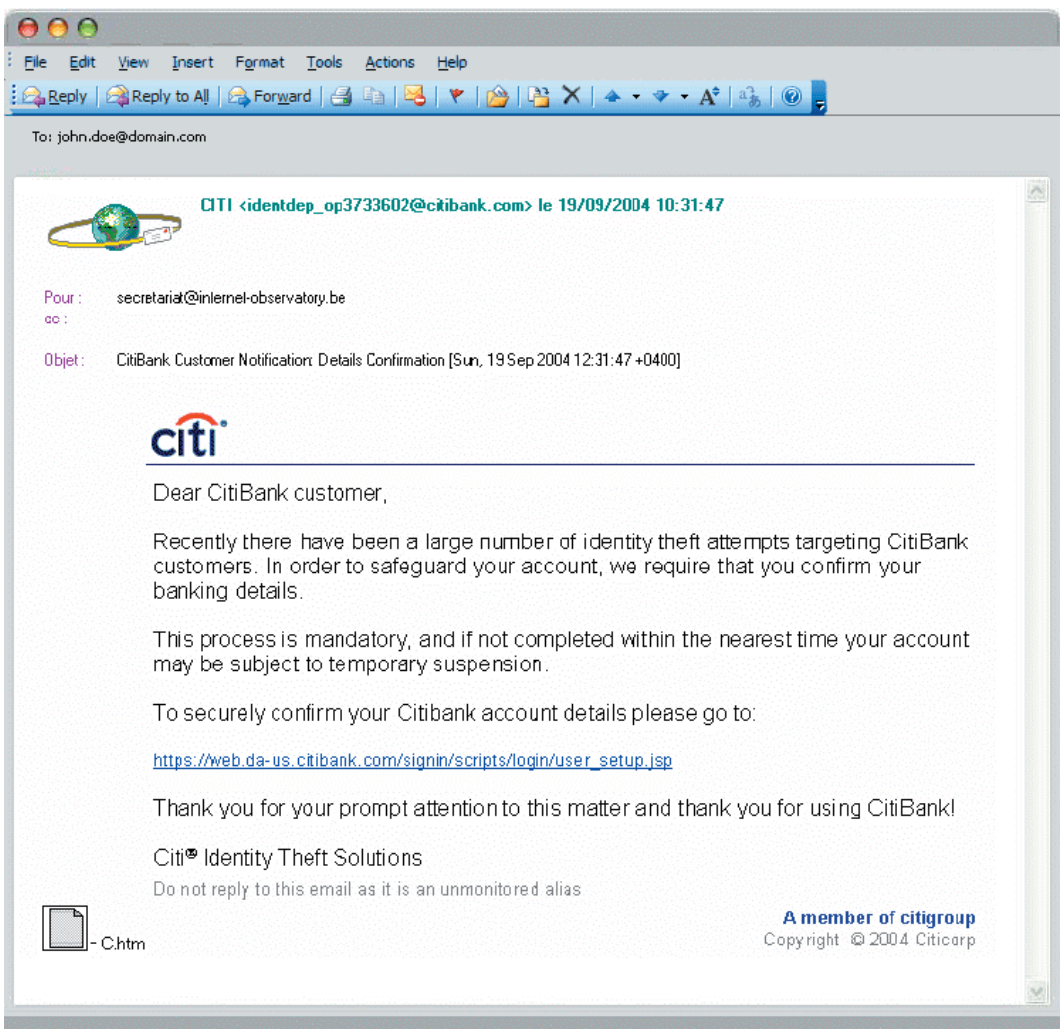
Le site web de la FCCU (Police fédérale) : www.fccu.be/crim/crim_fccu_fr.php .

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

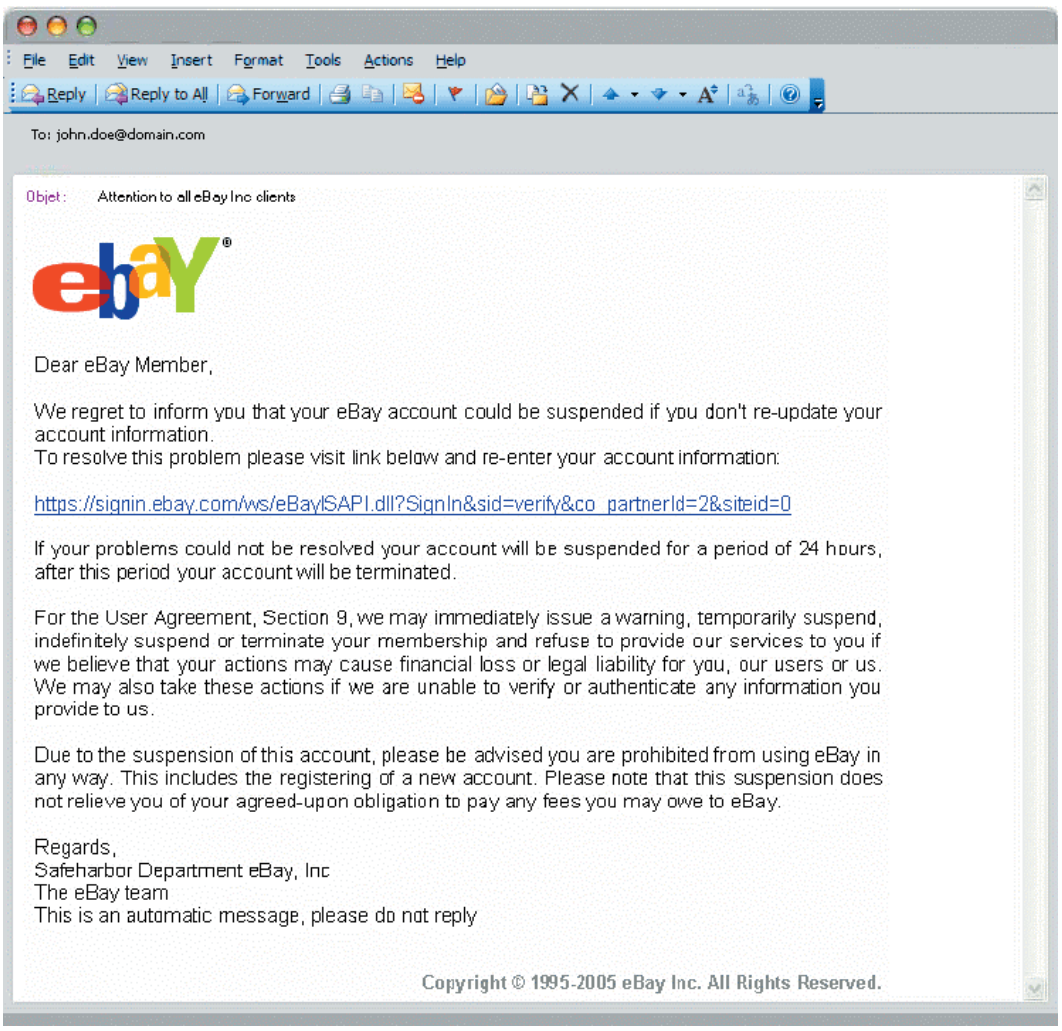
2. Le « phishing » ou hameçonnage

Illustrations

Exemple 1 de « phishing »



Exemple 2 de « phishing »



Explication

Le "phishing", aussi appelé "hameçonnage", est une escroquerie qui circule de plus en plus via le courrier électronique. Le mot « phishing » est en fait la contraction des mots anglais "fishing", en français pêche, et "phreaking", désignant le piratage de lignes téléphoniques.

Il s'agit d'une technique utilisée par les pirates informatiques pour récupérer des informations personnelles (telles que le nom d'utilisateur et le mot de passe voire des données bancaires) auprès d'internautes afin de les utiliser frauduleusement, et cela en usurpant l'identité d'un tiers et en invoquant un faux prétexte.

Qu'il s'agisse de prétexter la mise à jour des données personnelles sur eBay, de vérifier que le compte du consommateur chez Citibank ou son fournisseur d'accès n'a pas été piraté, de s'assurer que le numéro de carte de crédit Visa n'a pas été utilisé frauduleusement ou d'autres scénarios farfelus de ce genre, le but des escrocs est toujours le même : se faire passer pour un organisme ou une entreprise de confiance possédant lesdites données, inviter le consommateur à se connecter en ligne par le biais d'un lien hypertexte et, pour une raison ou pour une autre, le faire réintroduire ses données dans un formulaire qui se trouve sur une page web factice, copie conforme du site original. Par ailleurs, les adresses web mentionnées dans ces e-mails ressemblent parfois fortement aux adresses officielles.

Dans ce contexte, l'extrême urgence généralement invoquée et la facilité d'amener rapidement l'internaute sur le site contrefait font tomber certaines personnes dans le panneau.

Une fois que les informations personnelles sont dans les mains de l'escroc, ce dernier pourra les utiliser frauduleusement, notamment pour sortir de l'argent du compte en banque de l'internaute piégé ou faire des achats à l'aide de son numéro de carte de crédit.

Comment réagir ?

Le simple fait de recevoir un courrier électronique vous demandant de mettre à jour vos données personnelles doit vous inciter à la méfiance.

Il est possible que ce genre de messages soit légitime, mais c'est pratiquement jamais le cas en ce qui concerne des données aussi sensibles que le nom d'utilisateur et le mot de passe ou des données bancaires, tel le numéro de carte de crédit. Les banques sérieuses ne demandent d'ailleurs jamais les données confidentielles d'un client par courrier électronique.

Si l'internaute reçoit un courrier électronique qui demande ses données personnelles, la meilleure solution est de ne pas réagir et de l'effacer. S'il a néanmoins un doute, nous lui conseillons de contacter directement son prestataire (banquier, fournisseur d'accès, vendeur en ligne, etc) – dont l'identité pourrait avoir été usurpée – afin de vérifier la véracité de la demande. Dans ce cas, il ne faut évidemment

pas utiliser les éventuelles coordonnées de contact indiquées dans le courrier électronique mais veiller à obtenir des coordonnées fiables par d'autres voies.

Si l'internaute se rend compte – mais trop tard – qu'il a divulgué ses données bancaires, la première chose à faire est de bloquer son compte et sa carte le plus rapidement possible afin que l'escroc ne puisse pas s'en servir. Il suffit d'appeler le numéro 070/344.344 (Card Stop). Ce service est disponible pour toutes les cartes bancaires belges, qu'il s'agisse de cartes Bancontact/Mistercash ou de cartes de crédit. Nous conseillons également de dénoncer les faits à la FCCU à l'adresse suivante : contact@fccu.be.

Pour éviter de tomber dans le piège, voici quelques vérifications à faire pour déceler le caractère douteux de ce type de message :

- ai-je communiqué à cette entreprise mon adresse de messagerie ? Si ce n'est pas le cas, comment la connaît-elle et se fait-il qu'elle me contacte par ce biais ?
- le message en question est-il nominatif ? Le courrier reçu possède-t-il des éléments personnalisés permettant d'identifier sa véracité (numéro de client, nom de l'agence, etc.) ? Si ce n'est pas le cas, méfiance !
- l'expéditeur a-t-il une adresse électronique officielle ? Si c'est une adresse yahoo ou hotmail, vous devez clairement considérer ce courrier électronique comme douteux. Par ailleurs, il ne faut pas se fier totalement à l'adresse de l'expéditeur, qui est falsifiable et peut parfois porter un nom proche d'une entreprise connue ;
- il ne faut pas non plus se fier à l'apparence du site vers lequel on est dirigé : un site web peut être copié au pixel près !
- le lien inclus au message pointe-t-il directement vers l'adresse classique : [www.votrebanque.be], [www.votreprestataire.be], etc. ? Attention, les sites falsifiés ont parfois une adresse qui ressemble de près à l'adresse officielle, mais pas totalement (bien vérifier l'orthographe du nom de domaine) !
- éviter de cliquer directement sur le lien contenu dans l'e-mail, mais plutôt vous connecter à votre service en ligne par la barre d'adresse de votre navigateur, en tapant manuellement l'adresse ;
- vérifier que le site contenant des données sensibles est protégé (ce qui se concrétise par l'utilisation du protocole https et l'affichage d'un petit cadenas dans la barre d'état au bas du navigateur) ;
- dernier conseil : ne jamais divulguer de codes ou identifiants par courrier électronique.

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

Ces quelques règles de précaution devraient éviter bien des mauvaises surprises. Ces petites précautions prises, il convient toutefois de ne pas sombrer dans la paranoïa et de garder à l'esprit qu'Internet n'est pas plus dangereux que le monde réel dans lequel chacun de nous évolue chaque jour...

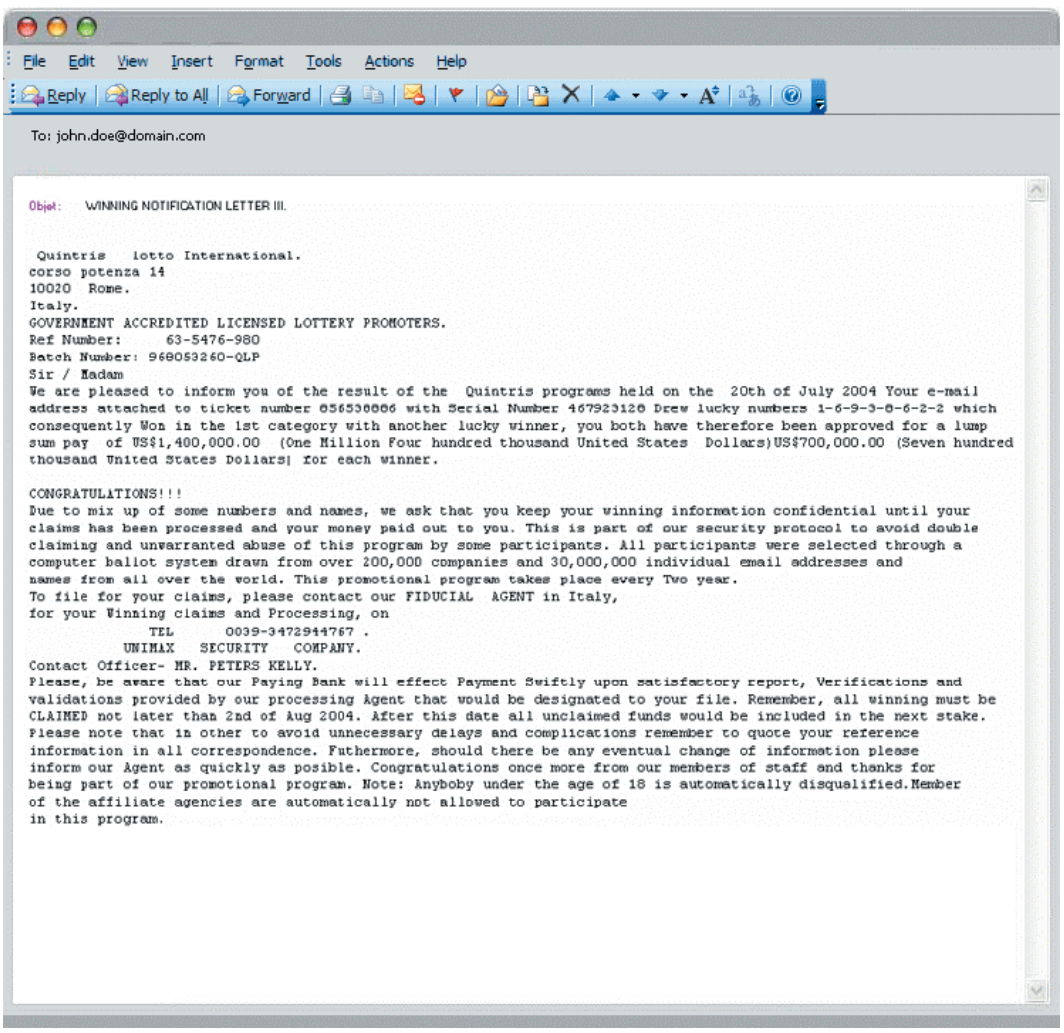
Pour en savoir plus

Le site web « Arnaques » du CRIOC : www.arnaques.be ;

Les sites web : www.hoaxbuster.com ; http://onguardonline.gov/phishing.html .

3. Les messages électroniques qui vous garantissent... de perdre de l'argent

Illustration


File Edit View Insert Format Tools Actions Help
Reply | Reply to All | Forward

To: john.doe@domain.com

Objet: WINNING NOTIFICATION LETTER III.

Quintris lotto International.
corso potenza 14
10020 Rome.
Italy.
GOVERNMENT ACCREDITED LICENSED LOTTERY PROMOTERS.
Ref Number: 63-5476-980
Batch Number: 968053260-QLP
Sir / Madam
We are pleased to inform you of the result of the Quintris programs held on the 20th of July 2004 Your e-mail address attached to ticket number 656530006 with Serial Number 467923120 Drew lucky numbers 1-6-9-3-8-6-2-2 which consequently Won in the 1st category with another lucky winner, you both have therefore been approved for a lump sum pay of US$1,400,000.00 (One Million Four hundred thousand United States Dollars)US$700,000.00 (Seven hundred thousand United States Dollars) for each winner.

CONGRATULATIONS!!!
Due to mix up of some numbers and names, we ask that you keep your winning information confidential until your claims has been processed and your money paid out to you. This is part of our security protocol to avoid double claiming and unwarranted abuse of this program by some participants. All participants were selected through a computer ballot system drawn from over 200,000 companies and 30,000,000 individual email addresses and names from all over the world. This promotional program takes place every Two year.
To file for your claims, please contact our FIDUCIAL AGENT in Italy,
for your Winning claims and Processing, on
TEL 0039-3472944767 .
UNIMAX SECURITY COMPANY.
Contact Officer- MR. PETERS KELLY.
Please, be aware that our Paying Bank will effect Payment Swiftly upon satisfactory report, Verifications and validations provided by our processing Agent that would be designated to your file. Remember, all winning must be CLAIMED not later than 2nd of Aug 2004. After this date all unclaimed funds would be included in the next stake. Please note that in other to avoid unnecessary delays and complications remember to quote your reference information in all correspondence. Futhermore, should there be any eventual change of information please inform our Agent as quickly as posible. Congratulations once more from our members of staff and thanks for being part of our promotional program. Note: Anyboby under the age of 18 is automatically disqualified.Member of the affiliate agencies are automatically not allowed to participate in this program.

Explication

Internet a souvent accéléré le développement ou la reprise d'arnaques qui sont de nature à extorquer de l'argent à l'internaute. Les variantes de ces arnaques sont nombreuses. Nous nous limiterons à traiter des plus fréquentes sur Internet, à savoir des fausses loteries, des faux héritages et des demandes de dons détournées.

Pour les autres, nous renvoyons le lecteur à la page arnaques du SPF Economie (www.economie.fgov.be/protection_consumer/fraud_prevention/home_fr.htm) et à l'excellent site web : www.arnaques.be.

Les fausses loteries

Il n'est pas rare de recevoir un message indiquant que vous avez gagné dans le cadre d'une loterie internationale une certaine somme, parfois proche du million d'euros. Pour obtenir le gain, on vous indique qu'il vous suffit de communiquer votre numéro de compte bancaire à une personne désignée dans le mail. Il arrive même qu'un numéro de téléphone soit indiqué et qu'une personne au bout du fil confirme le contenu du mail !

Dans tous les cas, on vous informe que pour récupérer le gain, vous êtes tenus de payer des frais administratifs et/ou des taxes (qui peuvent s'élever à plusieurs dizaines voire centaines d'euros).

Dans la grande majorité des cas, il s'agit ni plus ni moins d'une tentative d'escroquerie :

- soit le lot ne sera jamais obtenu mais l'escroc quant à lui aura disparu dans la nature avec les sommes que vous avez versées au titre de frais de dossiers ou de taxes ;
- soit vous allez obtenir un lot d'une valeur tout à fait ridicule et, en tous les cas, toujours inférieure au montant versé à titre de frais.

Parfois, les escrocs ont même le culot de relancer l'internaute.

En effet, quelques semaines après son versement pour payer les frais administratifs, il est contacté par téléphone ou par mail par un prétendu responsable de la police judiciaire. Celui-ci lui annonce que le montant des prix de la loterie a été saisi et que les fichiers montrent que cette loterie lui est redevable d'un prix (correspondant à la somme annoncée au départ à l'internaute). Ce prétendu responsable de la police lui propose de recouvrer le prix saisi moyennant le versement d'une petite commission...

Si l'internaute s'est fait prendre une première fois, les escrocs estiment que la probabilité est grande qu'il accepte à nouveau la même argumentation. Le consommateur sera alors abusé une seconde fois, mais il est clair qu'il ne verra jamais la couleur de la somme promise !

Une autre variante de cette escroquerie est la suivante : vous recevez un courrier électronique prometteur. Une bonne nouvelle vous est annoncée : c'est votre fête

! Votre adresse de courrier électronique a été sélectionnée pour participer à un concours! Pour ce faire, il vous suffit de choisir un lot entre 25 et 400 euros et vous précipiter sur votre téléphone pour composer le 0909 99 XXX.

Espérant gagner quelque chose - on ne sait jamais! -, vous appelez le numéro de téléphone. Comme par hasard, vous ne gagnez rien mais l'appel vous a coûté 25 euros ! Il s'agit tout simplement d'escroquerie réalisée par le biais de numéro surtaxé.

Les pratiques de ces sociétés sont tout simplement illégales. La loi du 21 juillet 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur (LPC) interdit expressément toute publicité qui éveille chez le consommateur l'espoir ou la certitude d'avoir gagné ou de pouvoir gagner un produit, un service ou un avantage quelconque par l'effet du hasard.

Les faux héritages

N'avez-vous jamais reçu un courrier électronique vous informant que votre oncle d'Amérique – dont vous n'avez jamais entendu parler – vient de décéder. La personne qui vous contacte est un prétendu officier public chargé de sa succession vous apprenant que vous êtes l'unique héritier d'une fortune colossale. Toutefois, pour disposer de l'héritage, la personne vous indique que certains devoirs administratifs doivent être accomplis à l'étranger, ce qui nécessite le paiement préalable des frais de dossier.

Même sur Internet, l'oncle d'Amérique fait encore recette. Les escrocs relancent ainsi l'arnaque au faux héritage. Comme le montant des frais demandés est dérisoire (plusieurs centaines d'euros) par rapport à la fortune colossale dont va disposer l'héritier, il entre tête baissée dans le piège et se fait délester du montant des frais de dossier.

Les demandes détournées de dons

Le Federal Computer Crime Unit – section spéciale de la police fédérale – reçoit régulièrement des avis concernant des risques potentiels de malversation liés à Internet.

Parmi ces avis, figurent pour partie de fausses demandes de dons, particulièrement dans les semaines qui suivent des évènements majeurs tels le Tsunami en Asie ou l'ouragan Katrina aux Etats-Unis. C'est ainsi que des courriers électroniques émis au nom d'organisations non gouvernementales bien connues incitaient à faire des dons via Internet.

Le problème est qu'au lieu de transiter sur les comptes de l'ONG, l'argent était envoyé sur un compte dans un pays exotique et les courriers électroniques étaient envoyés d'un autre pays tout aussi exotique.

Derrière ces e-mails de solidarité se cachent malheureusement des escrocs plus soucieux de leur portefeuille que de celui de leurs victimes.

Comment réagir ?

Toute proposition suspecte de gain d'argent facile ou appel à la générosité doivent faire l'objet d'une analyse attentive de l'internaute. Si les arnaques précitées se déroulaient dans la rue et qu'un inconnu faisait la même proposition au citoyen, celui-ci soupçonnerait immédiatement l'entourloupe. Pourquoi faire confiance aux inconnus sur Internet ?

Rappelons par ailleurs que l'usurpation de l'identité de tiers (entreprises ou organisations exemptent de tout soupçon) ou la falsification de courrier électronique est aisée sur Internet : autant donc adopter systématiquement le principe de précaution.

En tout état de cause, l'internaute ne doit jamais payer le moindre frais administratif que l'on lui réclame pour obtenir un soi-disant lot obtenu sans participer au jeu.

S'il est sollicité pour faire un don d'argent, il a intérêt à s'adresser à des organisations nationales ou internationales reconnues et vérifier que le numéro de compte indiqué correspond à celui de l'ONG en question. Ce numéro de compte peut facilement être obtenue via les autres médias ou sur le site web (officiel) de l'ONG.

Si vous vous êtes malheureusement fait prendre au piège, nous vous conseillons de dénoncer les faits à la FCCU à l'adresse suivante : contact@fccu.be.

Pour en savoir plus

Le site web du SPF Economie : http://economie.fgov.be/protection_consumer/fraud_prevention/home_fr.htm ;

Le site web « Arnaques » du CRIOC : www.arnaques.be ;

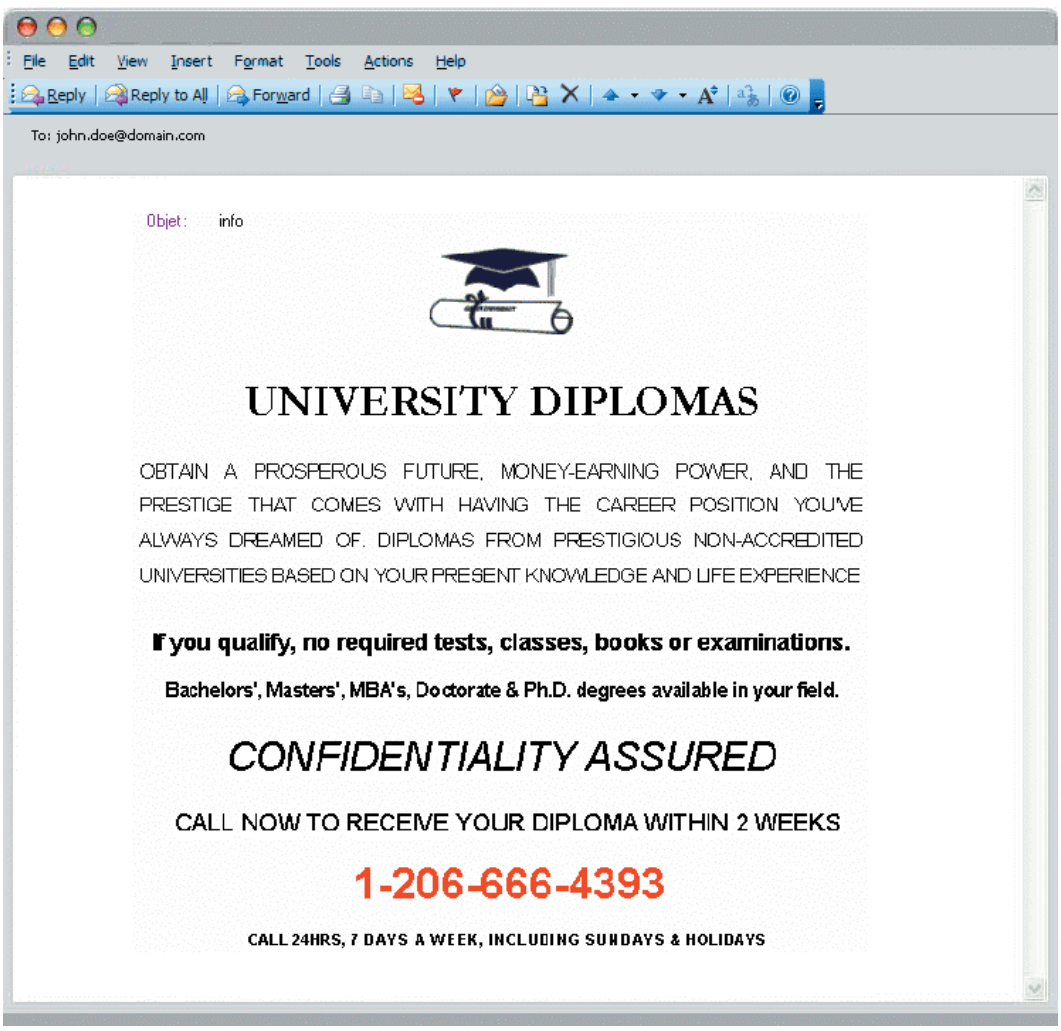
Le site web : www.hoaxbuster.com ;

Le site web : http://onguardonline.gov/spam.html .

4. Les messages électroniques spécialisés dans... les faux produits et les produits contrefaits

Illustrations

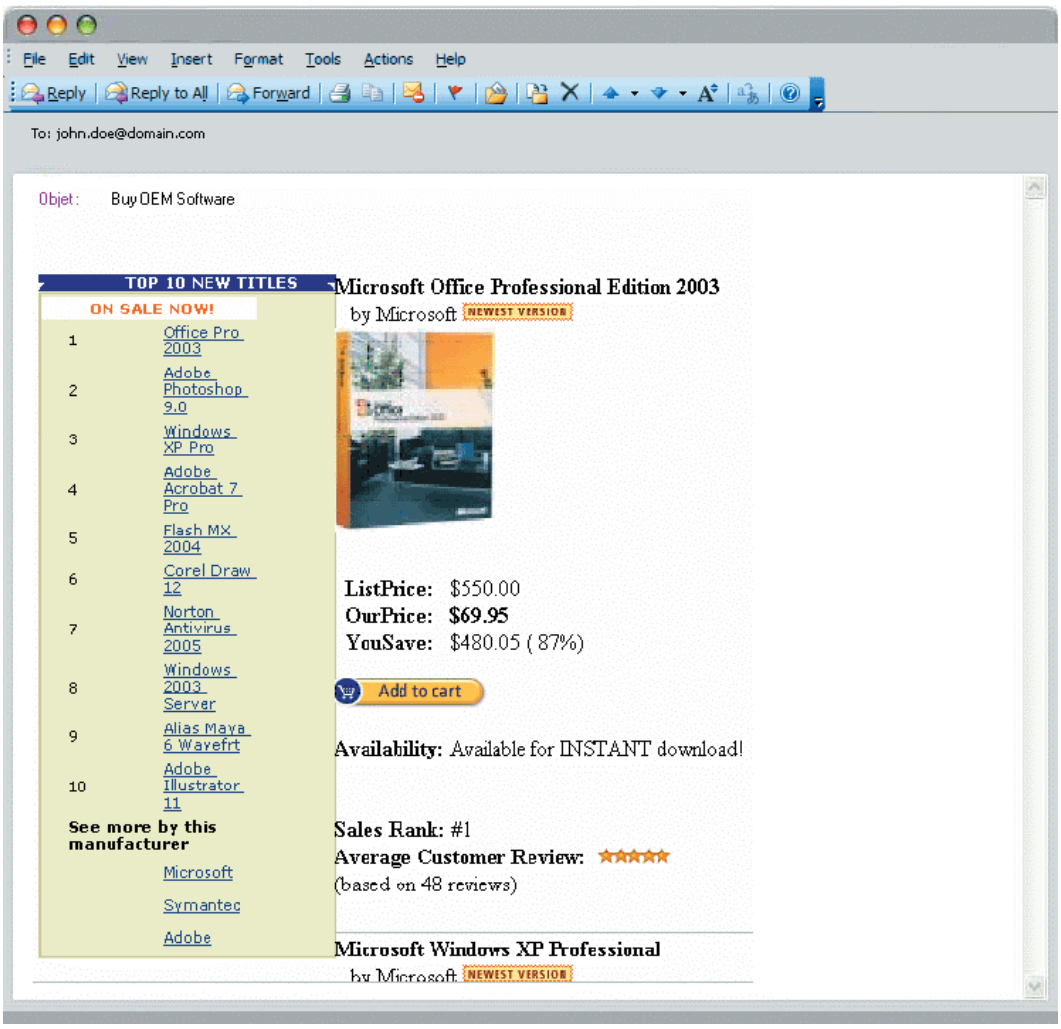
Exemple 1 : faux diplômes



« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

Exemple 2 : montres contrefaites

Exemple 3 : logiciels contrefaits



Explication

Sur le marché, les produits contrefaits sont nombreux et touchent tous les secteurs de l'activité économique : cosmétique, joaillerie, informatique, vidéo, parfum, alcool, textile, maroquinerie et même le secteur pharmaceutique.

Le terme de contrefaçon désigne, dans sons sens le plus général, toute atteinte à un droit de propriété intellectuelle.

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

La contrefaçon étant devenue un phénomène international, les contrefacteurs ont vite compris l'intérêt d'Internet à cet égard pour proposer à la vente des produits contrefaits ou de faux produits.

Qui n'a en effet jamais reçu un message électronique proposant l'achat d'une montre, d'un logiciel, d'un diplôme, ou de matériel hi-fi pour un prix défiant toute concurrence ? Il arrive même que l'émetteur indique dans son message que le produit est tout simplement un faux !

Les spécialistes de la lutte contre la fraude sur Internet estiment que les spam proposant des produits contrefaits représentent aujourd'hui une bonne partie du spam mondial. Même si 0,001 % des consommateurs répondent à ces mails et commandent, les escrocs deviennent vite millionnaires (les spammeurs prennent parfois un bénéficie de 900 à 1000 % sur le produit vendu, qu'ils ont acheté au départ à tout petit prix dans l'un ou l'autre pays réputé pour la contrefaçon).

Pour le consommateur, l'achat sur Internet d'un produit contrefait pose divers problèmes. Le produit peut ne pas correspondre à ce qui lui a été présenté, il est peu fiable et tombe rapidement en panne... sans garantie aucune bien entendu ! Par ailleurs, le consommateur n'a droit à aucun service après-vente, le vendeur sur le net n'étant bien souvent pas identifiable.

De plus, il se peut que le produit contrefait soit saisi par la douane. Le règlement européen n°1383/2003 organise à cet effet une procédure qui permet aux autorités douanières, lorsqu'il existe des motifs suffisants de soupçonner que l'on se trouve en présence de marchandises portant atteinte à un droit de propriété intellectuelle, de procéder à la retenue de la marchandise, afin de permettre au titulaire du droit d'introduire une demande d'intervention.

De nombreux colis postaux arrivent via les aéroports belges et sont confisqués par les douanes qui traquent – et c'est bien légitime – les produits contrefaits. Le consommateur pourrait être accusé de recel et il est très probable qu'il ne reverra jamais les sommes versées au départ ! En effet, le vendeur est souvent très difficile à identifier et est localisé dans un pays lointain, ce qui rend illusoire une poursuite efficace...

Pour ce qui concerne l'achat de logiciel contrefait, le titulaire des droits pourra à tout moment vous attaquer pour contrefaçon, et ainsi vous interdire d'utiliser le logiciel – que vous avez payé à l'escroc !

Il pourra obtenir d'un juge, sur requête unilatérale, l'autorisation de faire procéder, par un ou plusieurs experts (désignés par le juge) à une saisie-contrefaçon. Le titulaire des droits pourra ainsi obtenir la description de tous les objets et procédés

prétendus contrefaits, vous faire condamner au paiement d'une amende pouvant aller de 100 à 100.000 euros (montant à majorer par les décimes additionnels, ce qui concrètement abouti à multiplier ce montant par 5,5) si vous mettez en circulation ou que, à des fins commerciales, vous détenez une copie d'un programme d'ordinateur en sachant qu'elle est illicite ou en ayant des raisons de le croire. En cas de récidive, l'amende de même montant peut être accompagnée d'une peine de prison de trois mois à deux ans. Le titulaire des droits pourra également obtenir la confiscation du logiciel (objet de l'infraction) et vous réclamer d'éventuels dommages et intérêts.

Pour ce qui concerne la vente de faux diplômes, la confection de ceux-ci est généralement réalisée dans des pays lointains, ce qui ne rend pas les poursuites faciles, d'autant qu'ici aussi l'expéditeur sera souvent difficile à identifier ou à localiser. Toutefois, si un consommateur utilise ces documents dans le but de tromper un employeur potentiel, il commet une infraction (faux et/ou usage de faux) punissable pénalement.

Comment réagir ?

Les offres trop bon marché cachent très souvent des produits contrefaits voire des arnaques.

Plusieurs indices doivent attirer l'attention du consommateur sur le risque d'achat de ce type de produits :

- Le prix : un prix anormalement bas, voire trop intéressant, doit inciter à la prudence et éveiller les soupçons quant au caractère contrefait du produit ;
- L'origine de l'achat : certains pays sensibles sont connus pour la contrefaçon des produits de luxe ;
- La garantie d'authenticité : le certificat livré avec le produit peut aussi être falsifié et ne présente donc aucune garantie quant à la légitimité du produit ;
- Le vendeur : l'absence d'identification précise du vendeur demeure suspecte (aucune coordonnée particulière, si ce n'est une adresse e-mail qui ne garantit pas grand chose) ;
- La description du produit : certains termes employés dans la description du produit – tels que copie, réplique, imitation,... - peuvent suggérer le faux.

En cas de doute, il est conseillé de ne jamais répondre à ces messages et à ne pas acheter les produits proposés... sauf si vous avez de l'argent à perdre et que vous ne craignez pas les poursuites judiciaires !

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

Pour en savoir plus

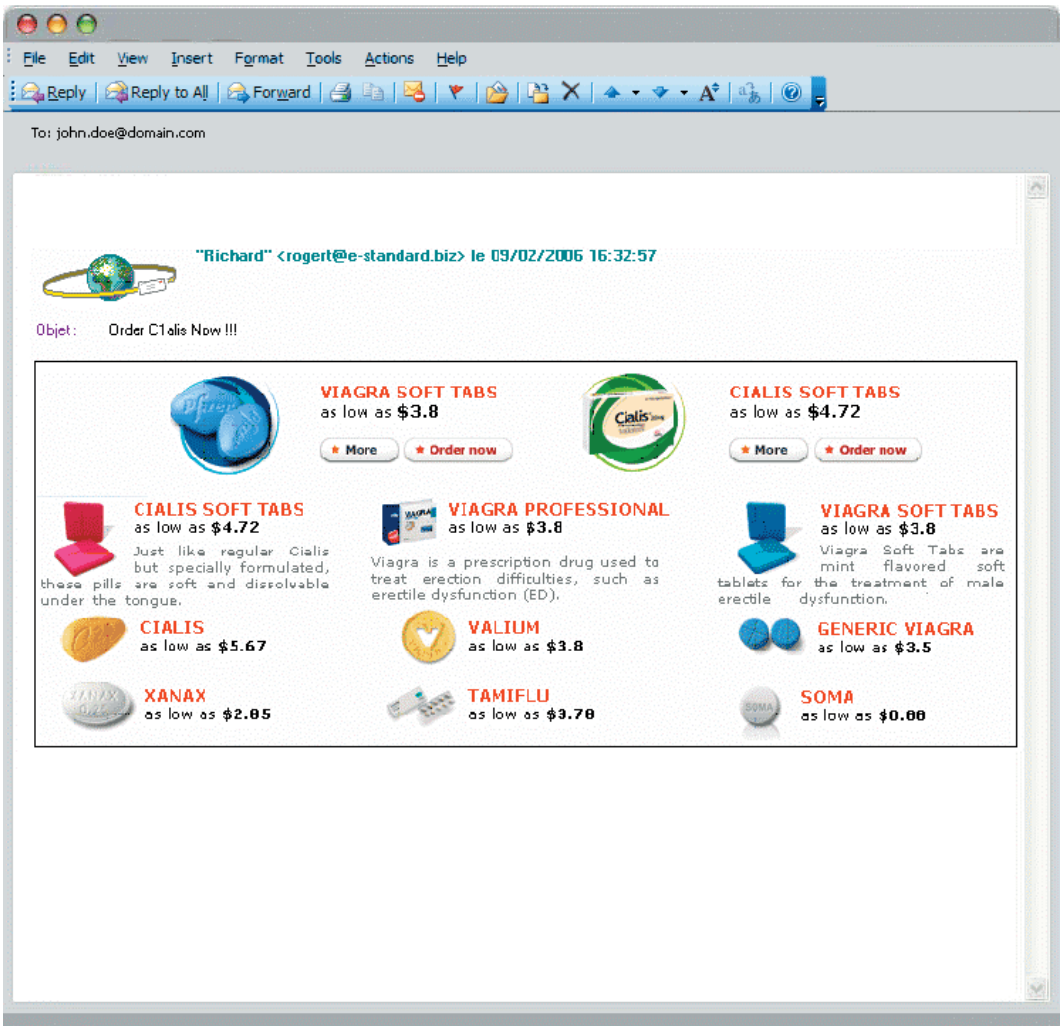
Le site web Arnaques : www.arnaques.be ;

Le site web du SPF Economie, PME, Classes moyennes et Energie : www.economie.fgov.be, et particulièrement la rubrique relative à la propriété intellectuelle : http://economie.fgov.be/intellectual_property/home_fr.htm ;

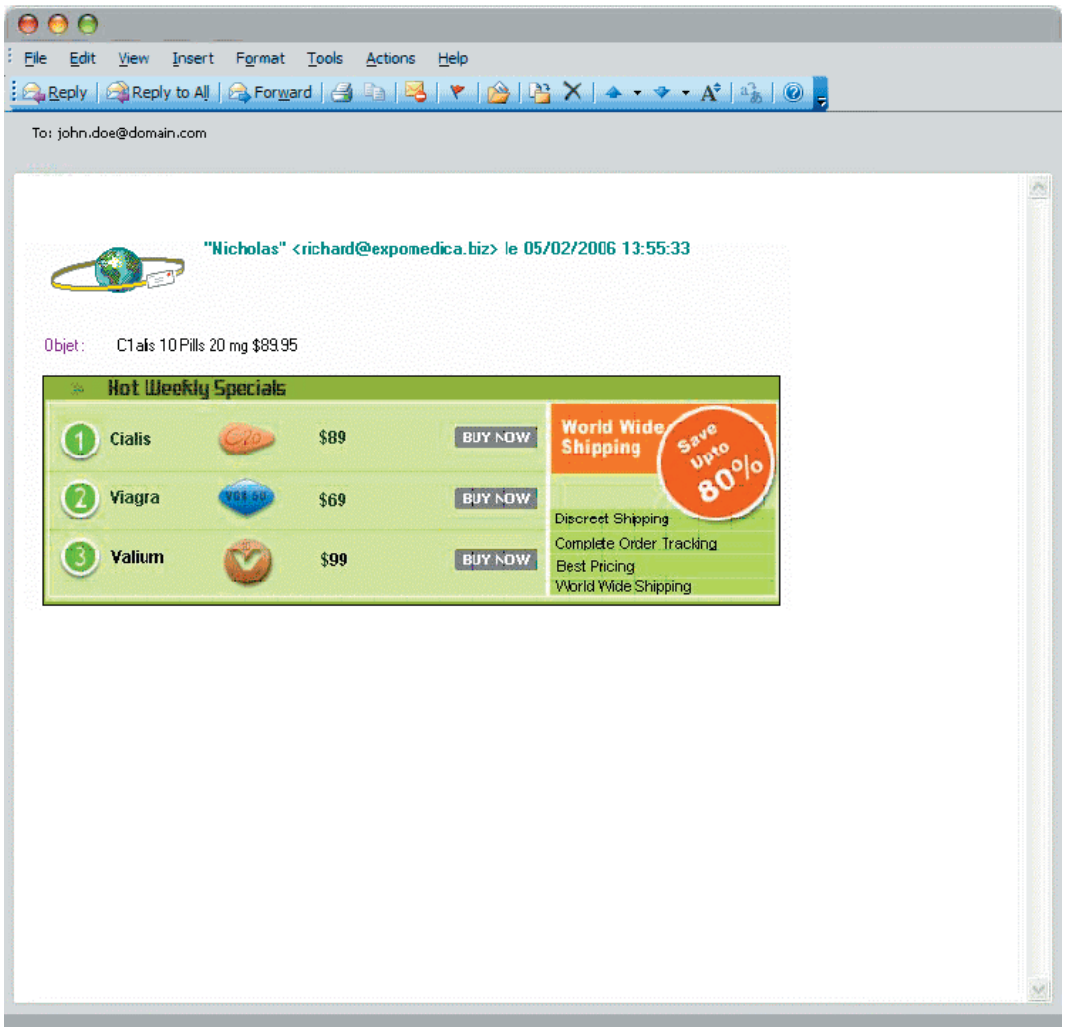
Le site web de l'Administration des douanes et accises : www.fiscus.fgov.be/interfdafr/default.htm .

5. Les messages électroniques peu soucieux de votre santé

Illustrations



« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »



Explication

On reçoit régulièrement des messages électroniques publicitaires pour des produits relatifs à la santé (stimulant sexuel, produit amaigrissant, anti-dépresseur, etc.). Par ailleurs, de nombreux produits de santé sont offerts en vente sur Internet.

Face à ces messages publicitaires qui peuvent être illégaux, mensongers voire constituer de véritables arnaques pouvant se révéler dangereuses pour la santé, il convient d'adopter la plus grande prudence.

En effet, il existe de nombreuses raisons qui font que l'achat de produits de santé via Internet peut présenter un danger pour votre santé ou, à tout le moins, constituer un inconvénient ou une perte d'argent :

- Les instructions d'utilisation peuvent être inexistantes, incorrectes ou incompréhensibles (par exemple dans une langue que vous ne connaissez pas) ;
- Les canaux de distribution utilisés pour la vente des produits de santé sur l'Internet ne sont généralement pas les circuits légaux contrôlés par les autorités compétentes. Dans ces conditions, la qualité des produits, leurs conditions de conservation, leur efficacité et leur sécurité ne peuvent être garanties. L'achat sur l'Internet de ces produits favorise le risque de mauvais usage car ceux-ci ne sont pas forcément adaptés ou peuvent être contre-indiqués ;
- Le remboursement peut poser problème ;
- Il est fréquent que l'on ne dispose d'aucune information sur le vendeur et/ou producteur, ce qui vous posera de grosses difficultés si vous voulez obtenir des précisions sur les qualifications du vendeur ou souhaitez, pour une raison ou une autre, intenter un recours à l'encontre de celui-ci ;
- Certains produits achetés à l'étranger peuvent être interdits dans notre pays. En cas d'illégalité, vos produits commandés peuvent être saisis, confisqués voire détruits par la douane, sans compter l'éventuelle amende dont vous seriez redevable !

Le plus paradoxal est de constater que les médicaments mis en vente sur Internet le sont parfois à des prix (largement) supérieurs à ceux pratiqués dans votre pharmacie ! Rappelons que le prix des médicaments est réglementé en Belgique et que le système de remboursement mis en place dans notre pays est souvent intéressant pour le patient.

Comment réagir ?

La prudence est de rigueur lorsque l'on décide d'acheter des produits relatifs à la santé via Internet. Dans de nombreux pays, la procédure d'achat de médicaments par Internet peut même être illégale. Nous ne pouvons que recommander d'acquérir les médicaments et autres produits de santé via les canaux légaux de distribution, comme les pharmacies en ce qui concerne les médicaments.

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

Ne jouez pas à l'apprenti sorcier ! En commandant vos produits de santé via Internet, vous pouvez prendre des risques pour votre santé et votre portefeuille et, surtout, vous vous privez parfois de la possibilité de bénéficier des avis éclairés et des conseils avisés de votre médecin, pharmacien ou autre professionnel de la santé.

La Direction Générale Médicaments du SPF Santé publique publie régulièrement des mises en garde contre la vente de produits de santé sur Internet à l'adresse suivante : www.health.fgov.be (consulter la rubrique « Médicament »). **Nous vous invitons à visiter régulièrement ce site web**.

Cette même Direction Générale combat la publicité et la vente illégales des médicaments et des dispositifs médicaux sur Internet, notamment en collaborant avec le SPF Economie et d'autres instances nationales et internationales.

Les utilisateurs d'Internet peuvent signaler à la DG Médicaments les cas d'activités soupçonnées d'être illégales et les cas à problème concernant les produits de santé, à l'adresse suivante :

SPF Santé publique, Sécurité de la Chaîne alimentaire et Environnement
Direction générale Médicaments
Boulevard Bischoffsheim, 33
B-1000 Bruxelles
Tél : + 32 (0)2 227 55 25
Fax : + 32 (0)2 227 56 46
E-mail : info.dgm@health.fgov.be

Pour en savoir plus

Nous conseillons la consultation du **« Guide Médicaments et Internet »** rédigé à l'initiative de l'Organisation Mondiale de la Santé (OMS) et disponible sur le site web du Service Public Fédéral Santé publique, Sécurité de la Chaîne alimentaire et Environnement : www.health.fgov.be (consulter la rubrique « Médicament », sous-rubrique « Médicaments et Internet »).

Les communiqués de mise en garde de la DG Médicaments contre la vente de produits de santé sur Internet sont diffusés sur le site www.health.fgov.be (consulter la rubrique « Médicaments). **Nous vous invitons à visiter régulièrement ce site web.**

Pour un complément d'information sur les arnaques liées à la santé, nous renvoyons aussi le lecteur vers la rubrique **« Les arnaques de santé »** disponible sur le site web www.arnaques.be du CRIOC (Centre de Recherche et d'Information des Organisations de Consommateurs).

6. Les messages électroniques qui répandent des virus informatiques

Illustration

Vu la grande variété de virus qui peuvent être envoyés par courrier électronique, il est difficile d'illustrer ce phénomène. En pratique, il est très fréquent que ces virus soient véhiculés par les fichiers attachés au courrier électronique. Prudence donc avant d'ouvrir ces fichiers ! Vous trouvez sur les sites spécialisés (voir « Pour en savoir plus » ci-dessous) les différents virus envoyés par courrier électronique, leur effet, leur nocivité et la manière de prévenir ou de se débarrasser de ces virus.

Explication

L'objectif de cette brochure n'est pas de faire un inventaire des différentes formes de virus informatiques, de leur dangerosité et des solutions pour les éviter ou les contrer. Sur ces différentes questions, nous renvoyons le lecteur à la lecture des « Fiches pratiques de sécurisation » disponibles à l'adresse suivante : www.spamsquad.be.

Dans un souci de clarté, limitons-nous à fournir les informations suivantes.

Vous devez prendre conscience que le courrier électronique est fréquemment utilisé par des escrocs ou des pirates pour faire circuler des virus informatiques. Il s'agit de programmes d'ordinateur plus ou moins nocifs capables d'infecter votre système informatique.

De la sorte, les pirates essayent notamment de prendre le contrôle et de piloter à distance votre ordinateur ou de vous envoyer des modules informatiques qui ont soit pour objet de limiter l'utilisation du service, soit de paralyser le réseau ou l'ordinateur voire de l'endommager (par exemple, en détruisant des données).

Il existe une grande variété de virus, sans compter que de nouveaux apparaissent tous les jours. Les spécialistes les classent selon leur mode de propagation et d'infection :

- Les **vers** sont des virus capables de se propager à travers un réseau ;
- Les **chevaux de Troie** (malwares, spywares, dialer, etc.) sont des virus permettant de créer une faille dans un système informatique. Ils sont généralement installés de manière insidieuse par un pirate informatique afin de lui permettre

de contrôler un ordinateur à distance, d'accéder à son contenu ou de prendre connaissance d'informations secrètes fournies lors d'une transaction (mot de passe, numéro de carte de crédit, etc.) ou encore de prendre la connexion du modem de l'internaute afin d'établir un dialogue avec un site souvent étranger à taux de facturation élevé ;

- **Les bombes logiques** sont des virus capables de se déclencher suite à un événement particulier (date système, activation distante,...) ;
- **Les hoax** annoncent un canular en précisant de faire suivre la nouvelle à tous les contacts, ce qui conduit à l'engorgement des réseaux ainsi qu'à la désinformation (cfr. infra).

Dans le même ordre d'idée, sans toutefois que l'on puisse considérer ce logiciel comme un virus, les escrocs utilisent parfois un "scanner de sécurité". Il s'agit d'un utilitaire permettant de réaliser un audit de sécurité d'un réseau en analysant les ports ouverts sur une machine donnée afin de déterminer les risques en matière de sécurité.

Cet outil est bien entendu très utile pour les administrateurs système et réseau afin de surveiller la sécurité du parc informatique dont ils ont la charge. Le revers de la médaille est que cet outil est parfois utilisé par des pirates informatiques afin de déterminer les brèches d'un système et de repérer les ports de l'ordinateur qui sont ouverts et non protégés.

Comment réagir ?

Indiquons d'emblée que le (la) lecteur (lectrice) trouvera de nombreux conseils détaillés sur la manière de sécuriser le plus adéquatement son système informatique, et ainsi éviter virus et autres attaques nuisibles, dans les « Fiches pratiques de sécurisation » disponibles à l'adresse suivante : www.spamsquad.be.

Rappelons néanmoins quelques mesures préventives élémentaires à prendre, qui devraient réduire le risque d'attaque et d'infection par des virus.

1. Installez un pare-feu (ou firewall, logiciel qui permet de protéger votre ordinateur des intrusions provenant de l'Internet) et un programme antivirus (mais aussi anti-spyware/mal-ware), mettez les à jour le plus souvent possible et effectuez régulièrement une analyse complète de votre(vos) disque(s) dur(s). **ATTENTION** : un pare-feu est inutile sans l'installation d'un antivirus et vice-versa !

2. Mettez régulièrement à jour les différents logiciels installés sur votre ordinateur (système d'exploitation, messagerie, etc), et installez les éventuelles solu-

tions réparatrices (patches) des bogues ou failles relatives à la version de votre logiciel ;

3. Evitez d'ouvrir un fichier attaché, particulièrement s'il est exécutable (.exe), ou un hyperlien reçu par courrier électronique si vous n'êtes pas certain(e) de son authenticité, surtout si ce courrier vous indique qu'il contient une solution pour protéger votre ordinateur ;

4. Effectuez régulièrement une sauvegarde (back-up) de vos données.

Pour être informé(e) au quotidien des nouveaux virus qui apparaissent sur Internet, l'internaute peut s'abonner à une liste de diffusion qui diffuse les alertes de l'Institut Belge des Postes et des Télécommunications (IBPT) et/ou consulter les sites web spécialisés en la matière.

Pour en savoir plus

« Fiches pratiques de sécurisation » disponibles à l'adresse suivante : www.spamsquad.be.

Rubrique « Les arnaques, l'informatique et les réseaux » du site web : www.arnaques.be

La rubrique « virus info » de l'IBPT : www.bipt.be/virus/viruswarning.htm

La rubrique « virus » du site web : www.hoaxbuster.com

Site spécialisé sur les virus : www.secuser.com (en français) ; www.insecure.org (en anglais) ; www.securityfocus.com (en anglais)

Site web gouvernemental américain : http://onguardonline.gov/spyware.html (en anglais)

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

7. Les messages électroniques qui véhiculent des arnaques classiques

Illustration

Malheureusement, nous – les arnaques – sommes trop nombreuses pour que nous puissions être illustrées dans ce document. Venez donc nous rendre visite et apprendre à nous reconnaître sur les sites web spécialisés indiqués ci-dessous (voir « Pour en savoir plus »).

Explication

Qui n'a jamais été attiré par les belles promesses d'une publicité vantant la beauté, la performance, la fortune ? Aujourd'hui, l'arnaque est plus que jamais un phénomène international. Les escrocs utilisent les nouvelles technologies avec un professionnalisme impressionnant.

Certes, ces escrocs n'ont pas attendu l'arrivée d'Internet pour commettre leurs méfaits.

Toutefois, l'utilisation du courrier électronique (ainsi que, comme on le voit de plus en plus, l'utilisation de la messagerie instantanée ou l'intervention dans les blogs) présente des atouts indéniables par rapport aux arnaques commises dans la rue, par téléphone, par téléfax ou par courrier postal : le coût, la rapidité et le nombre de victimes potentielles qui peut être touché (des milliers en quelques secondes !).

Dans ce contexte, nul doute que le courrier électronique est devenu le média par excellence pour commettre ces délits !

Par le biais du courrier électronique, les escrocs essayent de soutirer des sommes – parfois considérables – avant de s'évaporer dans la nature sans laisser de traces. La Direction générale du Contrôle et de la Médiation du SPF Economie et la Police fédérale sont confrontées chaque jour à des victimes ayant subi des dommages qui peuvent être importants.

Ces arnaques qui sont très nombreuses peuvent présenter des variantes et se développer tant dans un contexte électronique que non électronique. L'objectif de cette brochure n'est pas de présenter un inventaire complet de ces multiples arnaques. Nous renvoyons le lecteur à certains sites web de référence très complets et régulièrement mis à jour (voir la rubrique « Pour en savoir plus » ci-dessous).

Pour illustrer la variété, limitons-nous à citer le nom de quelques arnaques répertoriées et fréquentes :

- La fraude à l'identité ;
- Les propositions qui sont trop belles pour être vraies (lettres nigérianes, fausses loteries, revente de timesharing, vente en pyramide, vente de couverts, publicité pour travail à domicile, produits miracles, voyages à prix super réduit,...) ;
- Téléchargement forcé d'un logiciel de connexion vers un numéro surtaxé (« dialer ») ou offre de faux services via un numéro de téléphone surtaxé ;
- Les fausses allégations relatives à la santé ;
- Les arnaques liées au mariage et aux rencontres ;
- L'offre de faux services ou services farfelus (voyance, médium, etc.) ;
- Fausse vente ou achat à l'aide de chèques falsifiés ;
- Demande de dons illégitime (souvent suite à des évènements majeurs tels le tsunami en Asie ou Katrina) ;
- Etc.

Comment réagir ?

Le meilleur conseil que l'on puisse vous donner afin de réagir adéquatement face à ces tentatives d'arnaques et d'éviter de vous faire prendre au piège est le suivant : informez-vous !

Prenez le temps de décoder la proposition qui vous est faite. Apprenez à reconnaître les divers types d'arnaques et les moyens simples d'y faire face, avant qu'il ne soit trop tard.

Pour ce faire, nous ne pouvons que vous inviter à consulter les sites spécialisés et mis à jour qui recensent et expliquent de nombreuses arnaques afin de vérifier que la proposition ne tombe pas dans un des cas de figure. Nous conseillons particulièrement les sites web officiels suivants :

- Le SPF Economie :www.economie.fgov.be/protection_consumer/fraud_prevention/home_fr.htm ;

- La « Federal Computer Crime Unit » de la Police fédérale : www.fccu.be/crim/crim_fccu_fr.php ;
- Le site web « Arnaques » du Centre de recherche et d'information des organisations de consommateurs (CRIOC) : www.arnaques.be.

Si le doute se confirme après avoir consulté ces sources d'informations, abstenez-vous de réagir et supprimez le courrier électronique. Si un doute subsiste, prenez contact avec la Direction générale du Contrôle et de la Médiation du SPF Economie (eco.inspec@economie.fgov.be) ou une organisation de consommateurs pour obtenir des conseils judicieux.

Une personne prévenue en vaut deux !

Pour en savoir plus

Le site web du SPF Economie : http://economie.fgov.be/protection_consumer/fraud_prevention/home_fr.htm ;

Le site web de la FCCU (Police fédérale) : www.fccu.be/crim/crim_fccu_fr.php ;

Le site web « Arnaques » du CRIOC : www.arnaques.be ;

Le cyberconsommateur averti : www.clcv.org ;

Le site web : www.hoaxbuster.com ;

Autres sites web sur les arnaques : www.lesarnaques.com, www.scambusters.org

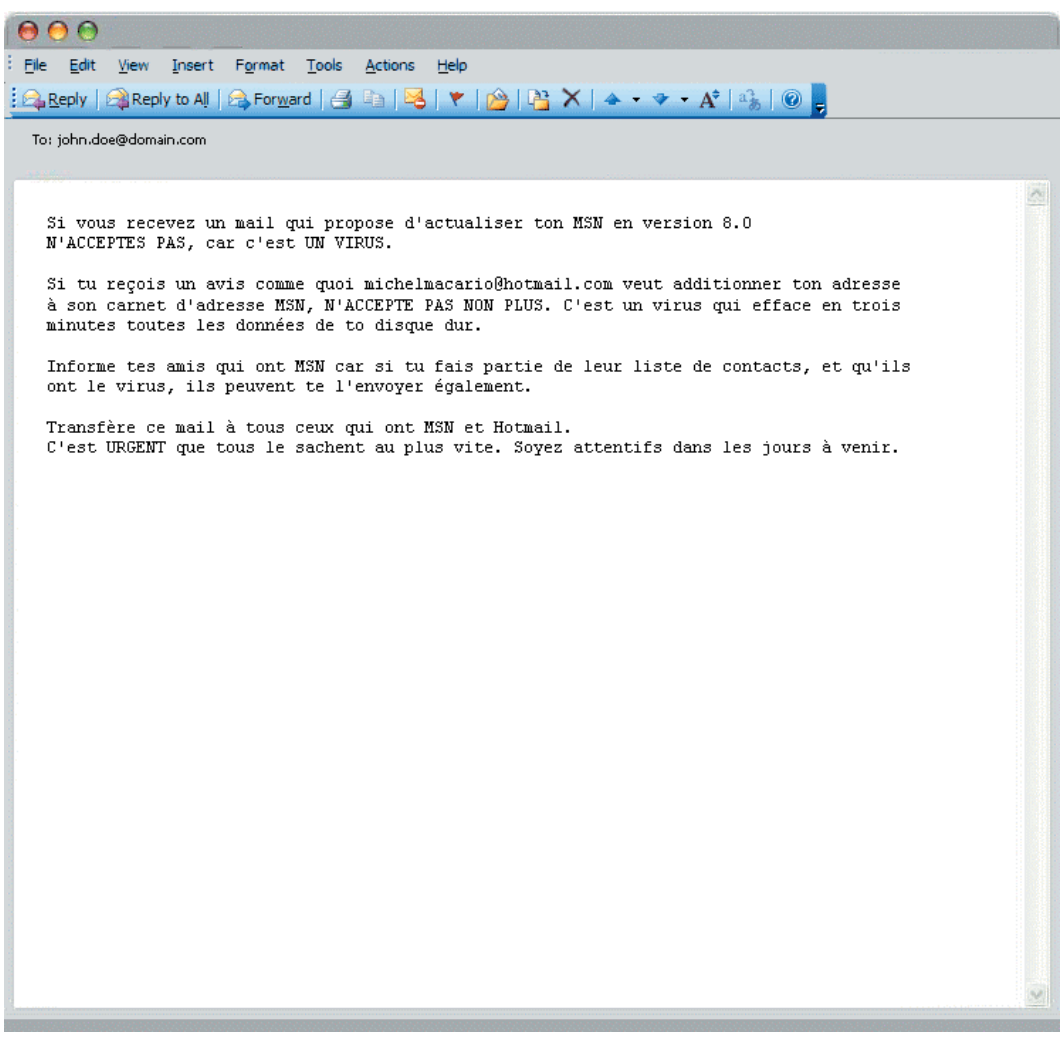
« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

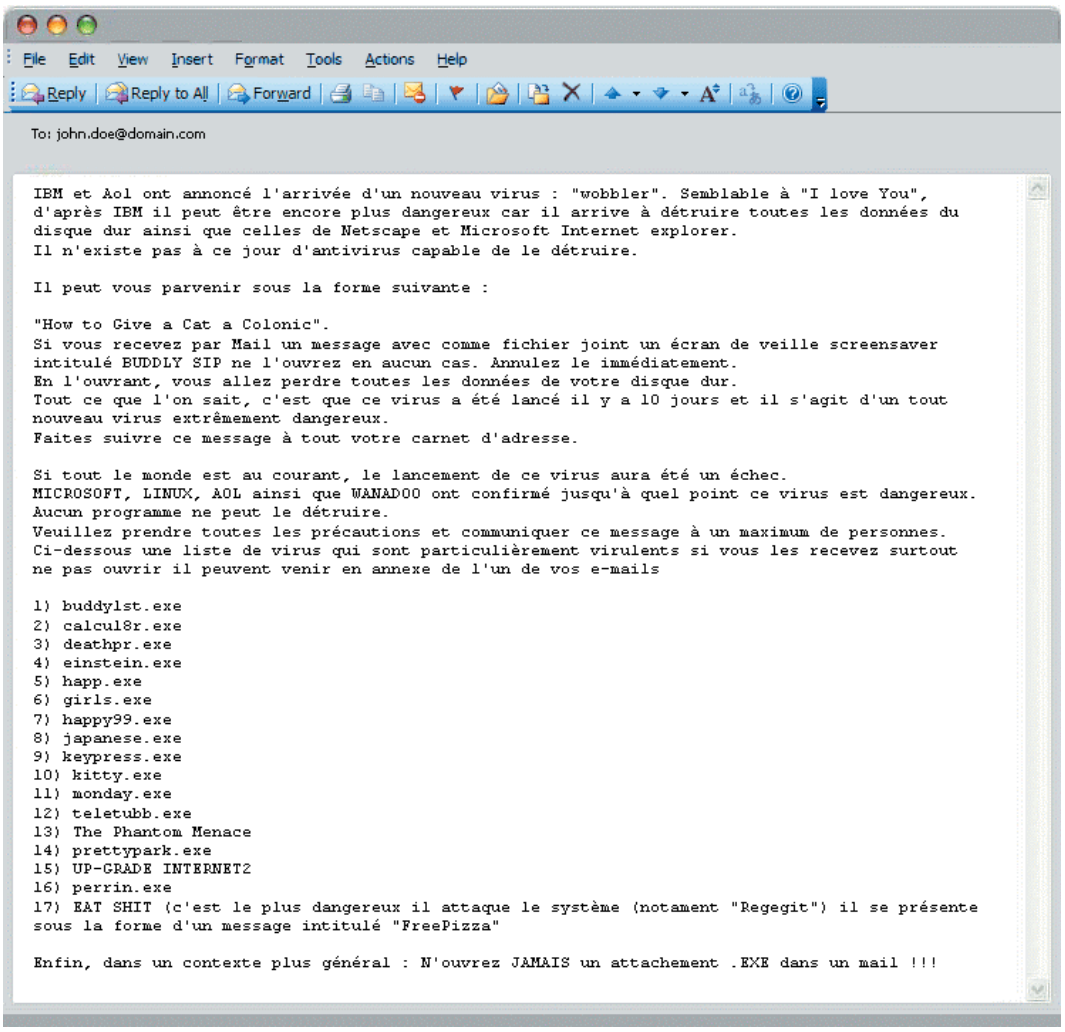
PARTIE 2 : LES COURRIERS ÉLECTRONIQUES NON SOLLICITÉS À DEGRÉ DE DANGEROSITÉ LIMITÉ

1. Les « hoax », canulars ou rumeurs

Illustrations

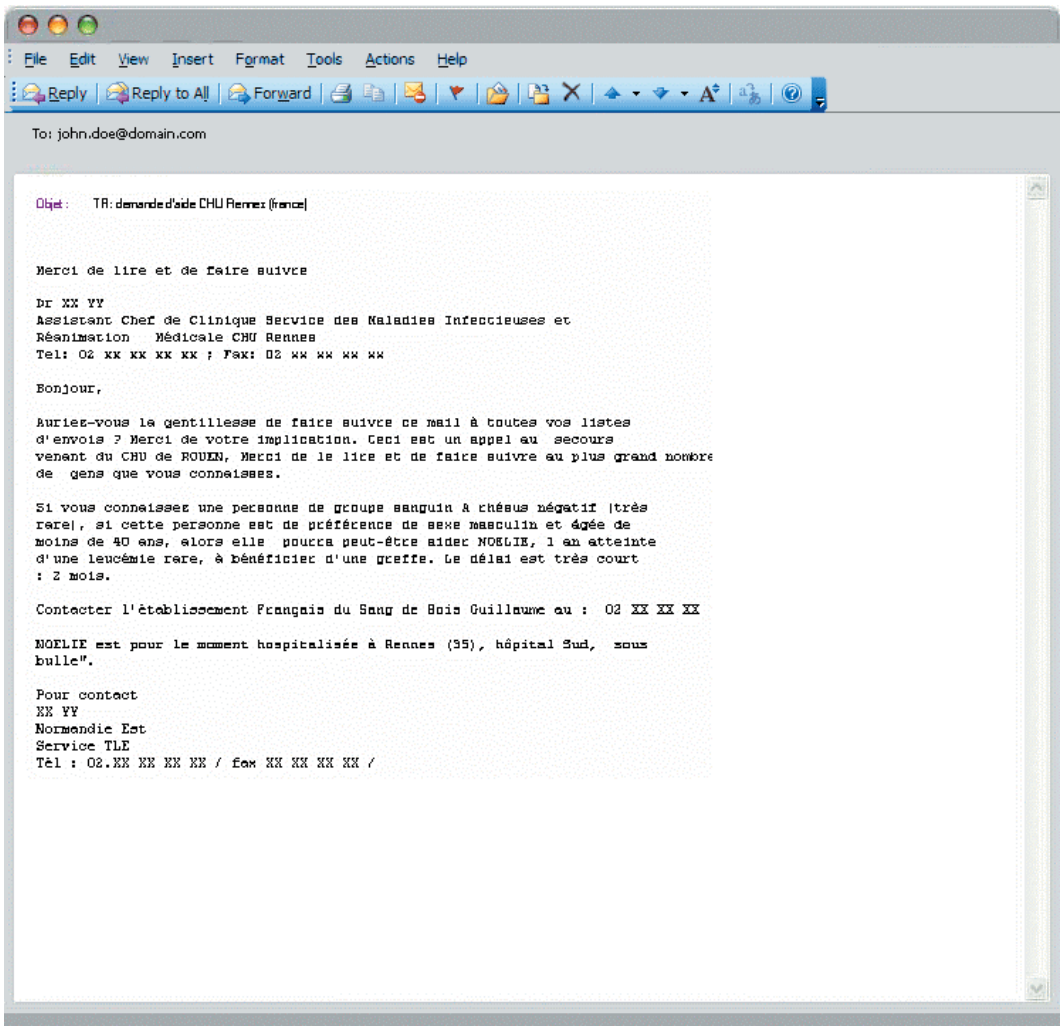
Exemple 1 : le faux virus




File Edit View Insert Format Tools Actions Help
Reply Reply to All Forward
To: john.doe@domain.com
IBM et Aol ont annoncé l'arrivée d'un nouveau virus : "wobbler". Semblable à "I love You",
d'après IBM il peut être encore plus dangereux car il arrive à détruire toutes les données du
disque dur ainsi que celles de Netscape et Microsoft Internet explorer.
Il n'existe pas à ce jour d'antivirus capable de le détruire.
Il peut vous parvenir sous la forme suivante :
"How to Give a Cat a Colonic".
Si vous recevez par Mail un message avec comme fichier joint un écran de veille screensaver
intitulé BUDDLY SIP ne l'ouvrez en aucun cas. Annulez le immédiatement.
En l'ouvrant, vous allez perdre toutes les données de votre disque dur.
Tout ce que l'on sait, c'est que ce virus a été lancé il y a 10 jours et il s'agit d'un tout
nouveau virus extrêmement dangereux.
Faites suivre ce message à tout votre carnet d'adresse.
Si tout le monde est au courant, le lancement de ce virus aura été un échec.
MICROSOFT, LINUX, AOL ainsi que WANADOO ont confirmé jusqu'à quel point ce virus est dangereux.
Aucun programme ne peut le détruire.
Veuillez prendre toutes les précautions et communiquer ce message à un maximum de personnes.
Ci-dessous une liste de virus qui sont particulièrement virulents si vous les recevez surtout
ne pas ouvrir il peuvent venir en annexe de l'un de vos e-mails
1) buddy1st.exe
2) calcul8r.exe
3) deathpr.exe
4) einstein.exe
5) happ.exe
6) girls.exe
7) happy99.exe
8) japanese.exe
9) keypress.exe
10) kitty.exe
11) monday.exe
12) teletubb.exe
13) The Phantom Menace
14) prettypark.exe
15) UP-GRADE INTERNET2
16) perrin.exe
17) EAT SHIT (c'est le plus dangereux il attaque le système (notament "Regegit") il se présente
sous la forme d'un message intitulé "FreePizza"
Enfin, dans un contexte plus général : N'ouvrez JAMAIS un attachement .EXE dans un mail !!!

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

Exemple 2 : la chaîne de solidarité



File Edit View Insert Format Tools Actions Help

Reply | Reply to All | Forward

To: john.doe@domain.com

Objet : TR: demande d'aide CHU Rennes (france)

Merci de lire et de faire suivre

Dr XX YY
Assistant Chef de Clinique Service des Maladies Infectieuses et
Réanimation Médicale CHU Rennes
Tel: 02 xx xx xx xx ; Fax: 02 xx xx xx xx

Bonjour,

Auriez-vous la gentillesse de faire suivre ce mail à toutes vos listes
d'envois ? Merci de votre implication. Ceci est un appel au secours
venant du CHU de ROUEN, Merci de le lire et de faire suivre au plus grand nombre
de gens que vous connaisses.

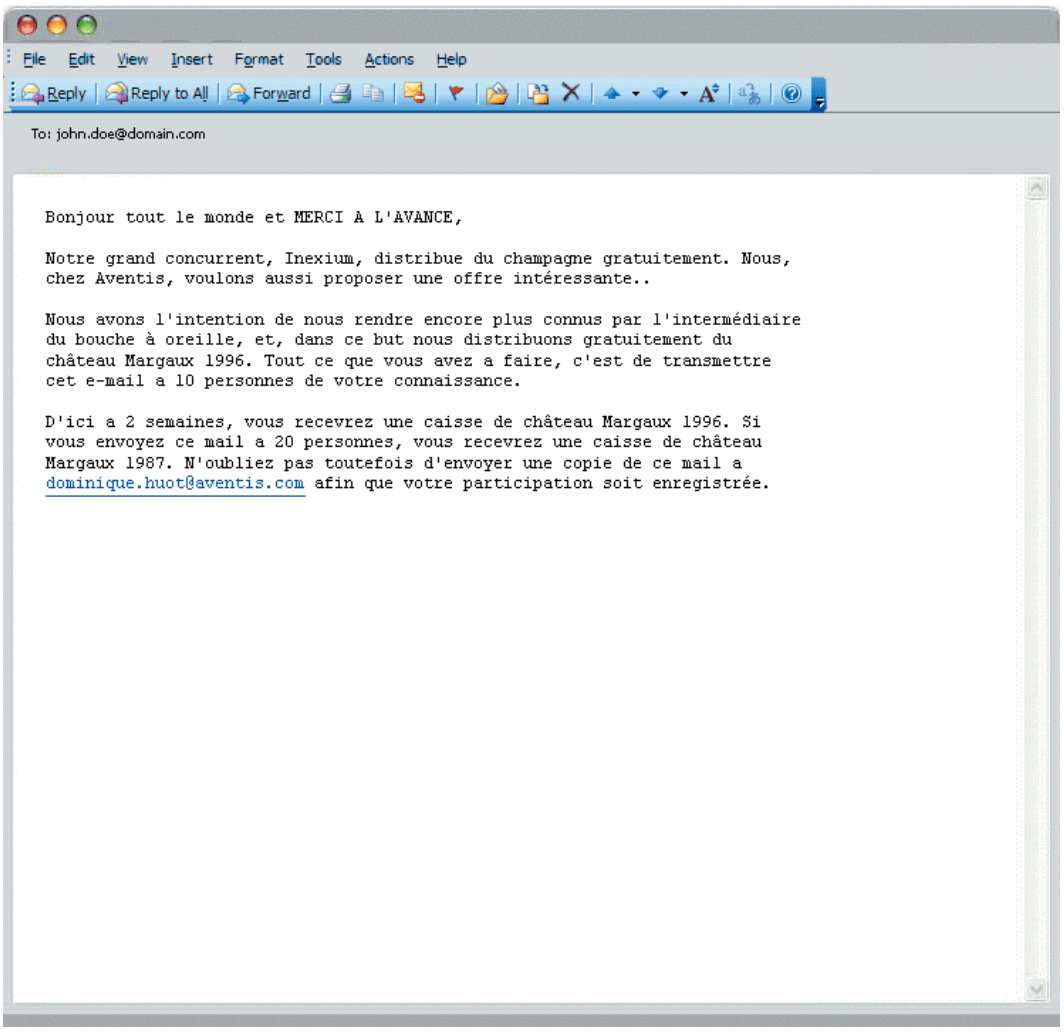
Si vous connaisser une personne de groupe sanguin A rhésus négatif (très
rare), si cette personne est de préférence de sexe masculin et âgée de
moins de 40 ans, alors elle pourra peut-être aider NOELIE, l an atteinte
d'une leucémie rare, à bénéficier d'une greffe. Le délai est très court
: 2 mois.

Contacter l'établissement Français du Sang de Bois Guillaume au : 02 XX XX XX

NOELIE est pour le moment hospitalisée à Rennes (35), hôpital Sud, sous
bulle".

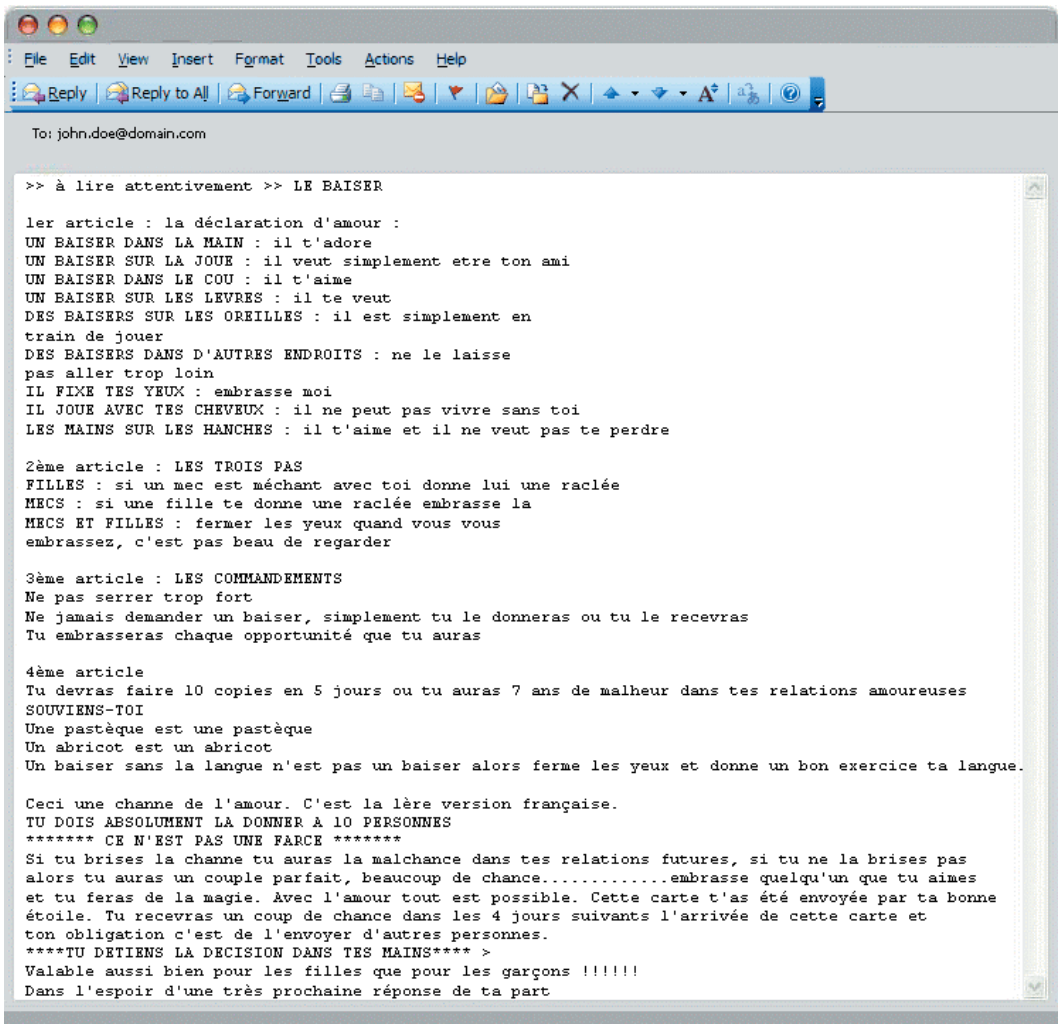
Pour contact
XX YY
Normandie Est
Service TLE
Tél : 02.XX XX XX XX / fax XX XX XX XX /

Exemple 3 : la promesse de « gains » ou produits gratuits



« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

Exemple 4 : bonne fortune ou mauvaise fortune



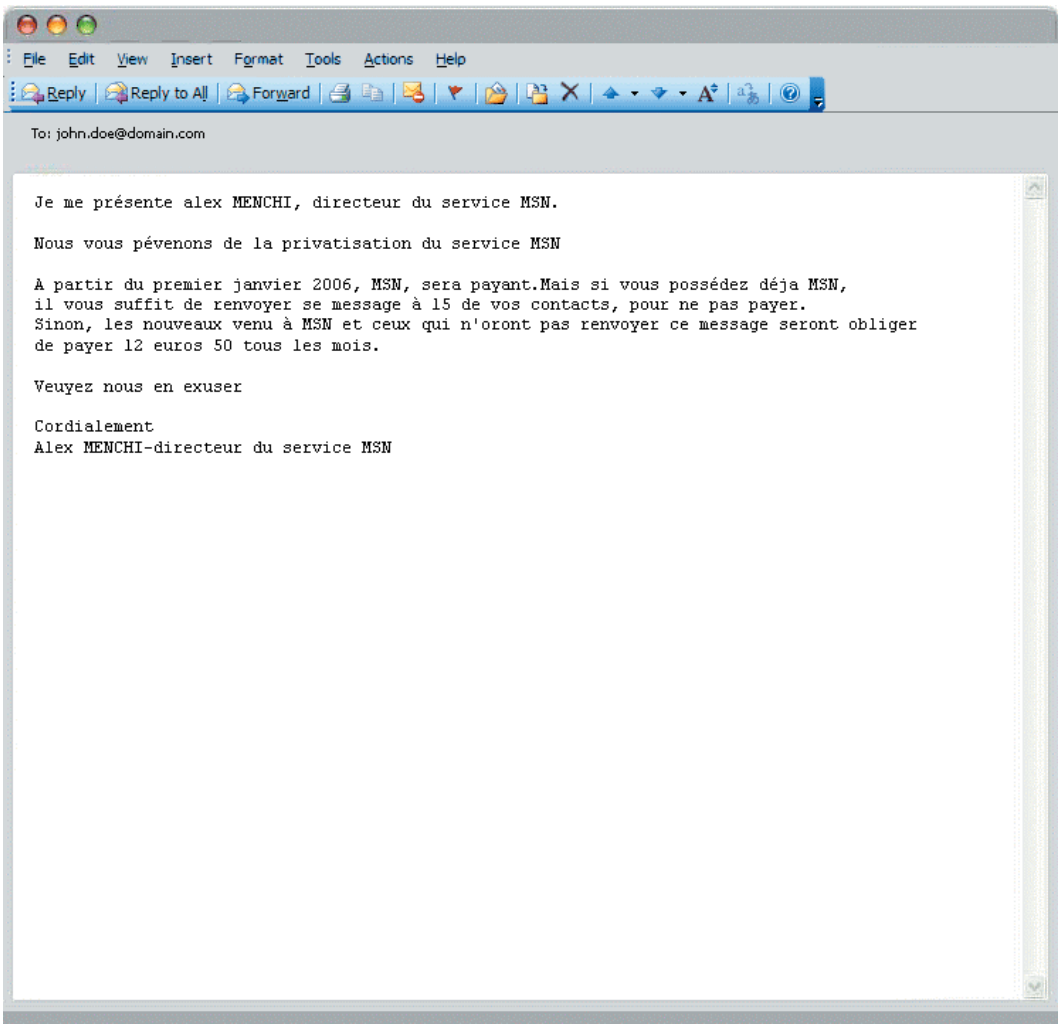
File Edit View Insert Format Tools Actions Help

Reply | Reply to All | Forward

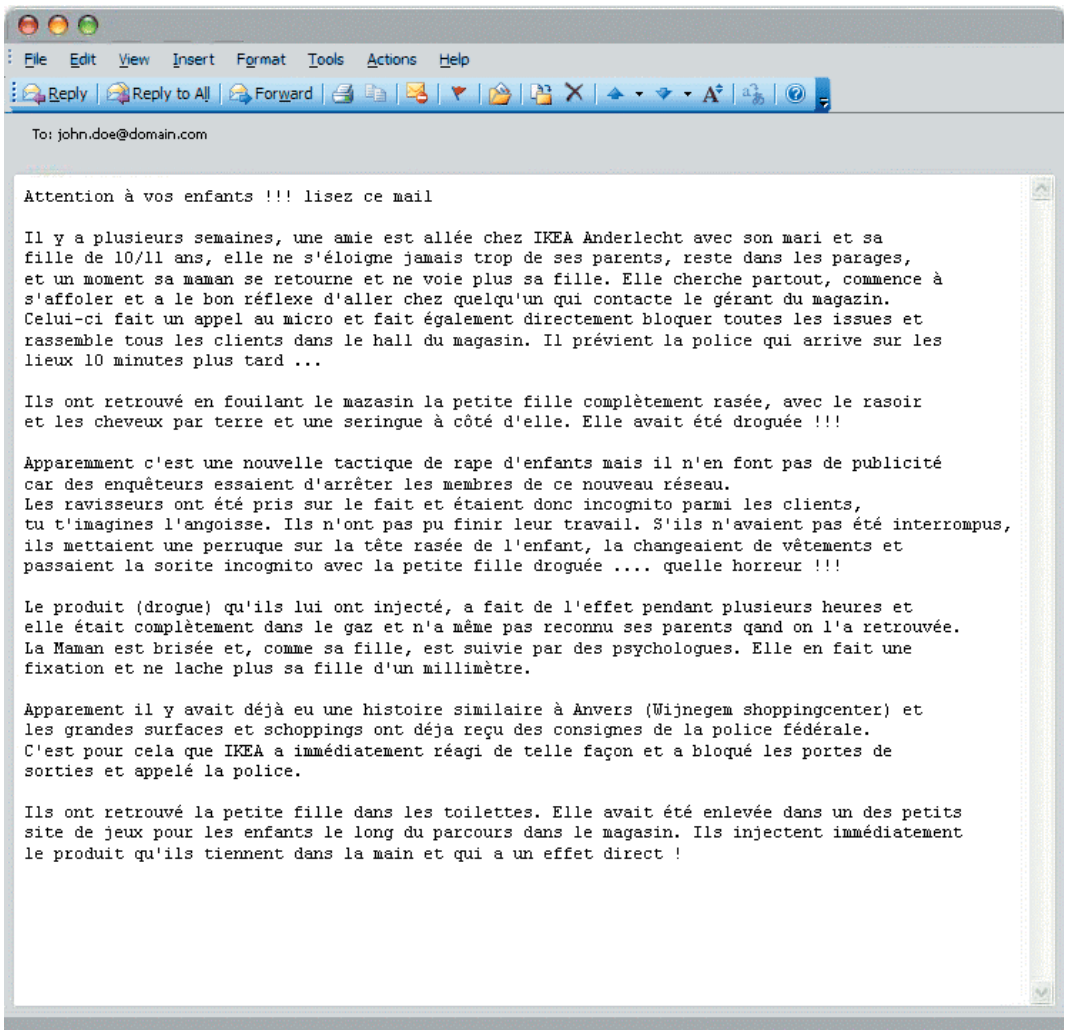
To: john.doe@domain.com

```
>> à lire attentivement >> LE BAISER

ler article : la déclaration d'amour :
UN BAISER DANS LA MAIN : il t'adore
UN BAISER SUR LA JOUE : il veut simplement etre ton ami
UN BAISER DANS LE COU : il t'aime
UN BAISER SUR LES LEVRES : il te veut
DES BAISERS SUR LES OREILLES : il est simplement en
train de jouer
DES BAISERS DANS D'AUTRES ENDROITS : ne le laisse
pas aller trop loin
IL FIXE TES YEUX : embrasse moi
IL JOUE AVEC TES CHEVEUX : il ne peut pas vivre sans toi
LES MAINS SUR LES HANCHES : il t'aime et il ne veut pas te perdre

2ème article : LES TROIS PAS
FILLES : si un mec est méchant avec toi donne lui une raclée
MECS : si une fille te donne une raclée embrasse la
MECS ET FILLES : fermer les yeux quand vous vous
embrassez, c'est pas beau de regarder

3ème article : LES COMMANDEMENTS
Ne pas serrer trop fort
Ne jamais demander un baiser, simplement tu le donneras ou tu le recevras
Tu embrasseras chaque opportunité que tu auras

4ème article
Tu devras faire 10 copies en 5 jours ou tu auras 7 ans de malheur dans tes relations amoureuses
SOUVIENS-TOI
Une pastèque est une pastèque
Un abricot est un abricot
Un baiser sans la langue n'est pas un baiser alors ferme les yeux et donne un bon exercice ta langue.

Ceci une channe de l'amour. C'est la lère version française.
TU DOIS ABSOLUMENT LA DONNER A 10 PERSONNES
******* CE N'EST PAS UNE FARCE *******
Si tu brises la channe tu auras la malchance dans tes relations futures, si tu ne la brises pas
alors tu auras un couple parfait, beaucoup de chance.............embrasse quelqu'un que tu aimes
et tu feras de la magie. Avec l'amour tout est possible. Cette carte t'as été envoyée par ta bonne
étoile. Tu recevras un coup de chance dans les 4 jours suivants l'arrivée de cette carte et
ton obligation c'est de l'envoyer d'autres personnes.
****TU DETIENS LA DECISION DANS TES MAINS**** >
Valable aussi bien pour les filles que pour les garçons !!!!!!
Dans l'espoir d'une très prochaine réponse de ta part
```

Exemple 5 : désinformation ou fausse rumeur

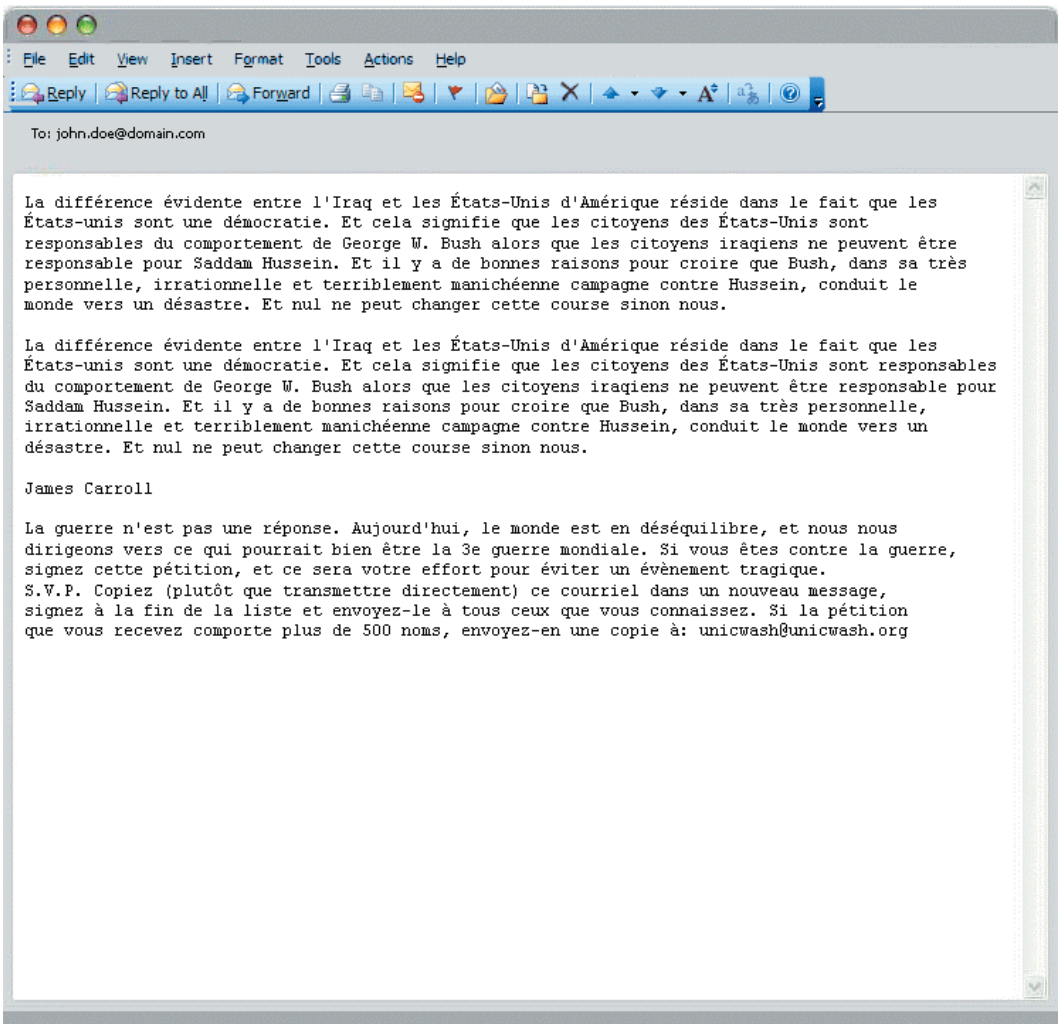


« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »



Suite à la circulation de ce courrier électronique, IKEA (et plus précisément le magasin belge d'Anderlecht) a rapidement réagi et fait circuler un communiqué démentant l'information de manière très claire.

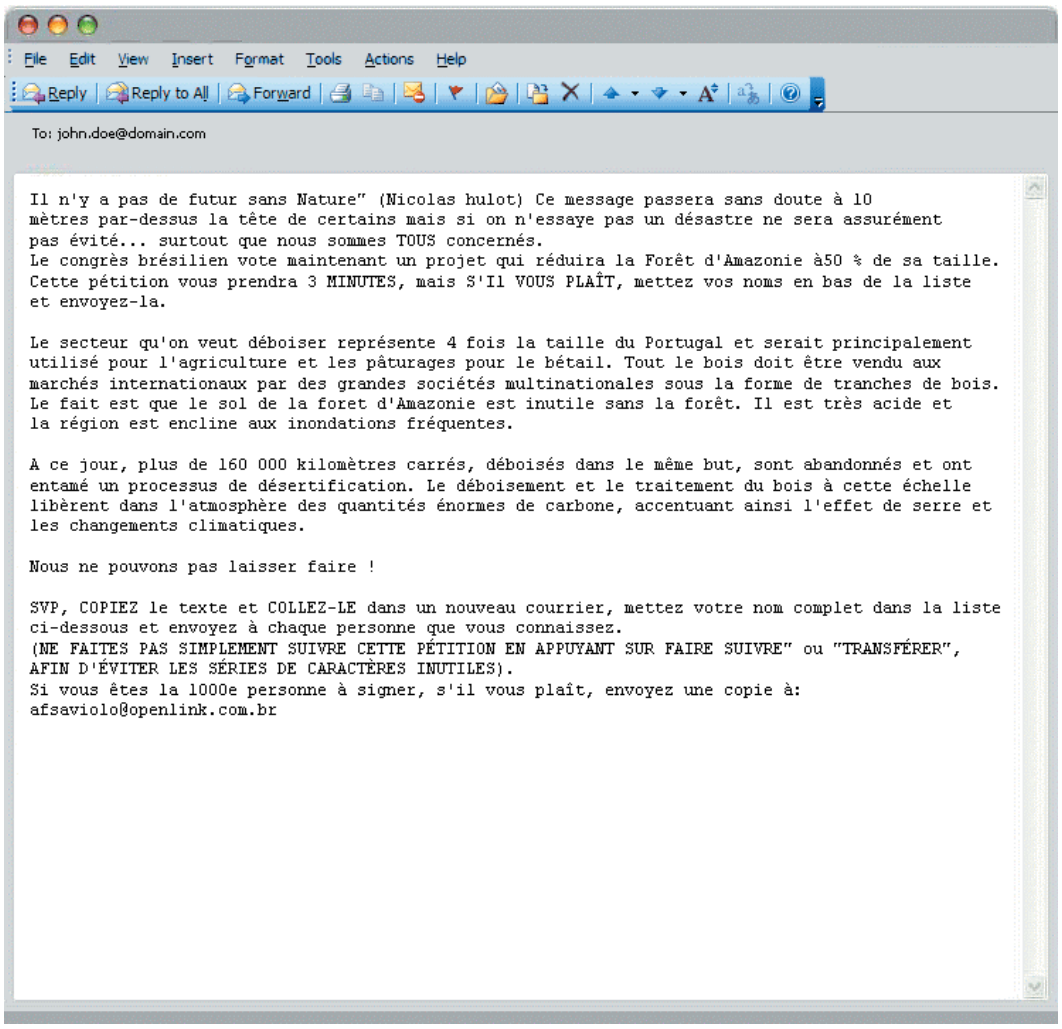
Exemple 6 : la fausse pétition contre la guerre conduite en Irak



Cette pétition est un canular, et le centre d'information des Nations Unies ("the United Nations Information Centre") situé à Washington (http://unicwash.org), n'a rien à voir dans cette affaire. Lui écrire ne sert donc à rien.

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

Exemple 7 : la fausse pétition de Nicolas HULOT transmise par courrier électronique


File Edit View Insert Format Tools Actions Help

Reply | Reply to All | Forward

To: john.doe@domain.com

Il n'y a pas de futur sans Nature" (Nicolas hulot) Ce message passera sans doute à 10 mètres par-dessus la tête de certains mais si on n'essaye pas un désastre ne sera assurément pas évité... surtout que nous sommes TOUS concernés.
Le congrès brésilien vote maintenant un projet qui réduira la Forêt d'Amazonie à50 % de sa taille. Cette pétition vous prendra 3 MINUTES, mais S'Il VOUS PLAÎT, mettez vos noms en bas de la liste et envoyez-la.

Le secteur qu'on veut déboiser représente 4 fois la taille du Portugal et serait principalement utilisé pour l'agriculture et les pâturages pour le bétail. Tout le bois doit être vendu aux marchés internationaux par des grandes sociétés multinationales sous la forme de tranches de bois. Le fait est que le sol de la foret d'Amazonie est inutile sans la forêt. Il est très acide et la région est encline aux inondations fréquentes.

A ce jour, plus de 160 000 kilomètres carrés, déboisés dans le même but, sont abandonnés et ont entamé un processus de désertification. Le déboisement et le traitement du bois à cette échelle libèrent dans l'atmosphère des quantités énormes de carbone, accentuant ainsi l'effet de serre et les changements climatiques.

Nous ne pouvons pas laisser faire !

SVP, COPIEZ le texte et COLLEZ-LE dans un nouveau courrier, mettez votre nom complet dans la liste ci-dessous et envoyez à chaque personne que vous connaissez.
(NE FAITES PAS SIMPLEMENT SUIVRE CETTE PÉTITION EN APPUYANT SUR FAIRE SUIVRE" ou "TRANSFÉRER", AFIN D'ÉVITER LES SÉRIES DE CARACTÈRES INUTILES).
Si vous êtes la 1000e personne à signer, s'il vous plaît, envoyez une copie à:
afsaviolo@openlink.com.br

La fondation Nicolas Hulot existe réellement et propose des actions concrètes concernant l'environnement. Toutefois, les responsables de cette fondation précisent que « bien entendu, cette pétition n'émane ni de Nicolas Hulot, ni de la Fondation Nicolas Hulot ».

Explication

Qui n'a jamais reçu un « hoax », appelé aussi canular, sur son adresse de courrier électronique ?

Depuis des lustres, les canulars font la joie des consommateurs. D'abord par courrier postal ou appel téléphonique, ils ont désormais pris une dimension mondiale avec Internet et le courrier électronique. Ils se jouent alors des frontières, de la distance, du temps et des coûts pour parvenir directement et facilement sur vos messageries électroniques.

Ils peuvent en outre prendre diverses formes, telles que notamment les fausses alertes aux virus, les fausses chaînes de solidarité, les fausses pétitions, les fausses promesses, les fausses informations, les blagues d'un goût douteux, ...

Généralement envoyé par un ami, le message est souvent frappé du sceau de l'urgence. Le réflexe premier est de relayer cette alerte et donc de renvoyer au plus vite le message à toutes ses connaissances. Ces dernières feront alors exactement la même chose et ainsi de suite jusqu'à ce que, par un effet « boule de neige », le message fasse plusieurs fois le tour du monde !

Le problème est que ces « hoax » font appel à votre naïveté et peuvent présenter des dangers. Pour cette raison, nous voulons ici attirer votre attention sur les caractéristiques qui permettent de reconnaître un « hoax » d'un message légitime, les types de « hoax » les plus fréquents et enfin les dangers que présentent ces messages.

Caractéristiques des « hoax »

Les canulars ou hoax présentent généralement les caractéristiques suivantes, facilement reconnaissables :

- Le message est adressé à une liste de correspondants et non à un destinataire unique ;
- Le message est de nature intrigante, inquiétante voire choquante ;
- Comme le message ne laisse pas insensible, il suscite la réaction du lecteur ;
- L'information est cautionnée par des références dignes de foi mais qui ne sont jamais prouvées ;
- L'internaute est invité à faire suivre le message à tous ses contacts ;
- Le message contient souvent des fautes de syntaxe ou d'orthographe.

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

Les types de hoax les plus fréquents

Les types de hoax les plus fréquents sont les suivants (cette liste est reprise du site web www.hoaxbuster.com) :

1/ Les faux-virus

Le message – censé provenir de grandes sociétés (IBM, AOL, Microsoft,...) – vous alerte de la propagation fulgurante d'un virus via le courrier électronique. Le message vous encourage à prévenir le maximum de personnes vu l'urgence de la situation et la dangerosité du virus. Le message est parfois signé par de hauts responsables informatiques ou des agences de presse renommées.

En réalité, de nombreux messages de ce style sont tout simplement faux. En cas de doute, l'internaute a intérêt à vérifier l'information sur les sites web spécialisés tels www.secuser.com ou www.hoaxbuster.com.

2/ Les chaînes de solidarité

Ce type de message fait appel à la générosité des internautes. Le message vous encourage à sauver une ou plusieurs personnes (atteinte(s) d'une maladie grave, etc.). On vous indique que les fournisseurs d'accès à Internet sont censés comptabiliser tous vos messages et reverser une somme au(x) malheureux. Bref, on vous incite à envoyer un maximum de messages car plus le message est envoyé, plus on récoltera de l'argent pour le prétendu malheureux.

Vous constaterez toutefois qu'aucun sponsor ne soutient l'opération, que le message ne contient aucun lien de partenariat avec une quelconque organisation officielle et enfin que les adresses e-mail, lorsqu'elles sont présentent, sont toujours fausses. Et pour cause : la prétendue maladie n'existe pas, et la personne atteinte encore moins !

3/ La promesse de « gains » ou de produits gratuits

Le message vous promet de gagner un maximum d'argent en un rien de temps. Il suffit pour cela d'envoyer le message au plus grand nombre de personnes. Un programme est censé se charger de compter vos envois. Il arrive même que le message soit étayé d'un exemple (ahurissant) qui vous démontre que vous pouvez gagner ainsi plusieurs milliers de dollars !

Il arrive aussi que des messages sont émis au nom d'une entreprise connue et indiquent que l'on peut recevoir un produit gratuit si on envoie le message à un nombre X de personnes ainsi qu'à un responsable de l'entreprise en question, dont l'adresse de courrier électronique est indiquée.

Un simple transfert d'e-mail n'a jamais rapporté de l'argent à personne. La bonne preuve, c'est que personne n'a jamais connu l'heureux gagnant de cette action... Et puis, si c'était vrai, ça se saurait !

4/ Bonne fortune ou mauvaise fortune

Tout le monde a déjà reçu une lettre postale du même genre. Le message vous désigne comme heureux destinataire de la bonne fortune ou du malheur le plus terrible selon que vous faites suivre ou pas le message (parfois un nombre de personnes est indiqué).

Pour renforcer le message, on cite l'exemple d'une personne qui n'a pas renvoyé le message et qui a eu tous les malheurs du monde jusqu'à ce qu'elle se décide enfin, suite à quoi tous ses problèmes se sont résolus d'un coup.

Il est vrai que la superstition pousse parfois certaines personnes à faire suivre ce message. Mais la raison ne doit-elle pas toujours l'emporter sur la superstition ? Effacez le message et surtout ne prolongez pas la chaîne.

5/ Désinformation

Le message "informe" l'internaute de tel ou tel fait. Le fait en question peut être scandaleux (telle société réputée collabore avec un parti d'extrême droite par exemple). Il peut aussi être inquiétant (un enfant est enlevé de manière rocambolesque dans une grande surface connue par exemple). Il peut enfin être urgent (renouvellement du permis de conduire dans un certain délai en vue de bénéficier de la gratuité par exemple).

Le fait invoqué est généralement de nature à faire réagir l'internaute, ce qui est le but recherché. Il implique en général des sociétés très connues et réclame une diffusion à grande échelle du scandale, de l'information inquiétante ou urgente.

Outre le fait que l'information est fausse, le signataire du message est bien entendu inconnu. Par contre, il est fréquent que les personnes mises en cause existent réellement. Le cas échéant, le canular se transforme en véritable diffamation.

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

6/ Les pétitions douteuses

De par sa rapidité, l'e-mail est un outil de pétition très utilisé, mais pas toujours sans danger. Conformément à notre devise belge « l'union fait la force », ce genre de message propose aux internautes de s'unir contre l'injustice. On l'invite ainsi à inscrire son nom au bas d'une liste à la suite des autres signataires pour protester contre cette injustice.

Cependant, l'absence d'identification de l'association commanditaire, de personne à l'origine de la pétition doit attirer l'attention. Car, signer un e-mail et le renvoyer à ses connaissances revient à lancer une bouteille à la mer sans aucune garantie.

En effet, la pétition se limitera à faire le tour du monde si personne n'est chargé de la transmettre au destinataire (il est même possible que l'adresse donnée comme destinataire n'est plus active depuis longtemps). Sans compter qu'à tout moment, n'importe quel internaute peut changer le contenu du texte original et véhiculer d'autres idées avec le soutien "involontaire" du précédent co-signataire.

La signature d'une pétition est un acte qui engage le citoyen. A ce titre, mieux vaut vérifier la qualité du contenu proposé, la légitimité de son émetteur et utiliser des pétitions à signer sur un site où l'initiateur et le destinataire sont identifiés, et où l'information peut être vérifiée.

7/ Humour

Souvent reçu au hasard du courriel, le message humoristique ne laisse jamais insensible. Il se caractérise par son absence de signature et concerne de manière universelle tous les internautes. Soucieux de détente, l'internaute s'en empare et contamine illico d'autres internautes en espérant leur faire plaisir.

C'est bien entendu le moins dangereux des « hoax » quant à son contenu. De par sa nature, son degré de contamination est toutefois très élevé. Veillez donc à rester raisonnable et à sélectionner les courriers humoristiques que vous envoyez ainsi que les destinataires de ceux-ci. Ceci étant dit, ne vous privez pas de partager une bonne blague avec vos proches car l'humour est le meilleur conservateur du corps et de l'esprit de l'homme et de la femme ...

Les dangers que présentent les « hoax »

Il est vrai qu'a priori les hoax ne semblent pas présenter de risques particuliers. Mais à y regarder de plus près, on constate souvent qu'il est conseillé de les éviter car ils peuvent présenter les dangers suivants :

- Ils véhiculent de fausses allégations qui peuvent porter atteinte à l'image d'une personne ou d'une société voire constituer de la diffamation ;
- Ils propagent des rumeurs pas toujours anodines qui décrédibilisent les informations vraies disponibles sur Internet : comment dans ce contexte encore distinguer le vrai du faux ? Il faut donc toujours se poser la question de savoir si c'est de l'info ou de l'intox, pour ne pas dire de « l'inthoax » ! ;
- Ils occupent inutilement la bande passante, ralentissent la circulation sur les réseaux informatiques et peuvent, par un effet boule de neige, saturer les serveurs de mails. Tout cela a un coût qui, in fine, est payé par l'internaute ;
- Ils véhiculent de fausses alertes (virus, action urgente à entreprendre, ...) et créent la lassitude au point que quand des messages sont réels, ils ne sont plus considérés comme crédibles ;
- Ils peuvent être modifiés par des pirates et servir de support à des virus qui transforment le canular en véritable épidémie.

Comment réagir ?

Vous l'avez compris, de nombreux canulars ou « hoax » peuvent causer des problèmes voire constituer de véritables dangers. Nous vous conseillons donc de :

- réfléchir à deux fois avant de faire suivre « bêtement » et mécaniquement le message à tout ou partie de votre carnet d'adresses ;
- vérifier si le message est ou non un « hoax » sur le site web www.hoaxbuster.com ;
- s'il s'agit d'un prétendu virus, vérifier l'existence de ce nouveau virus sur les sites web spécialisés, dont www.secuser.com.

Si, suite ou malgré ces vérifications, vous souhaitez néanmoins envoyer le message à vos connaissances, **nous vous conseillons fermement d'inclure les adresses e-mail dans le champ « ccc » (Copie Conforme Cachée) ou « cci » (Copie Conforme Invisible) ou « bcc » (Blind Carbon Copy) de votre messagerie électronique** : de la sorte, chaque destinataire reçoit le message sans que ne soient mentionnées les adresses des autres destinataires. Cela permet d'éviter que les adresses de

courrier électronique de vos relations soient visibles par tous les destinataires du courrier électronique transmis et, ainsi, limiter le risque de collecte et d'utilisation à des fins de spamming.

Pour en savoir plus

Le site par excellence sur la question des hoax : www.hoaxbuster.com ;

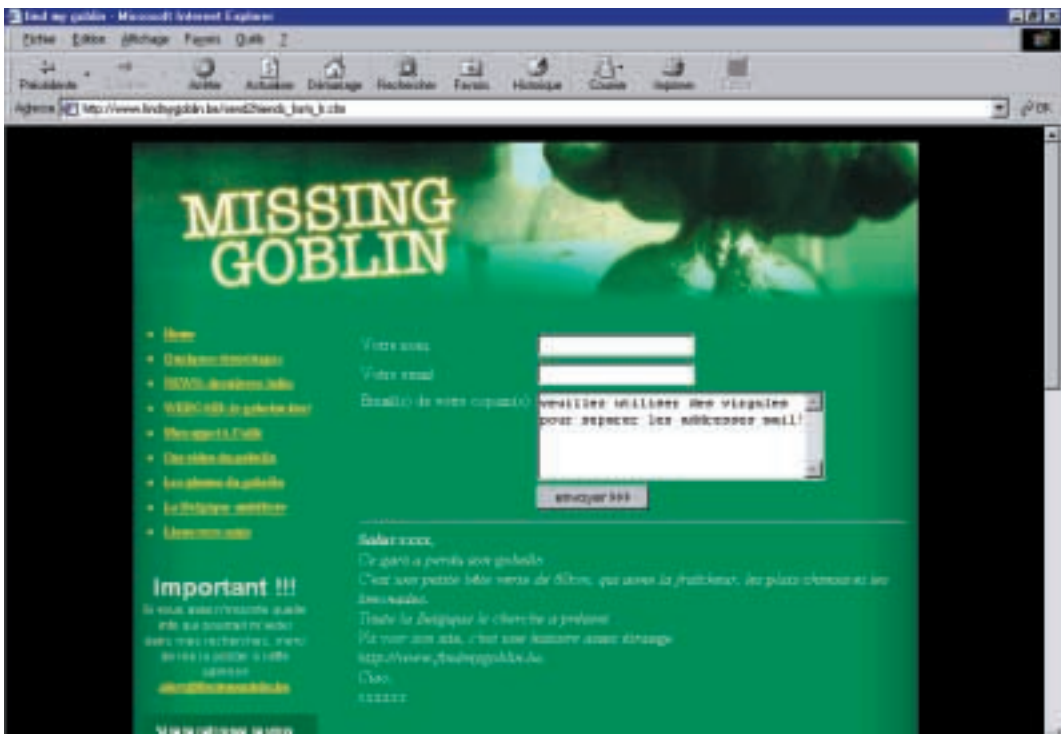
De nombreux exemples sont également donnés sur le site web : www.arnaques.be ;

Sur la question des virus : www.secuser.com.

2. Les messages électroniques qui vous associent – bien malgré vous – à une campagne publicitaire de marketing viral

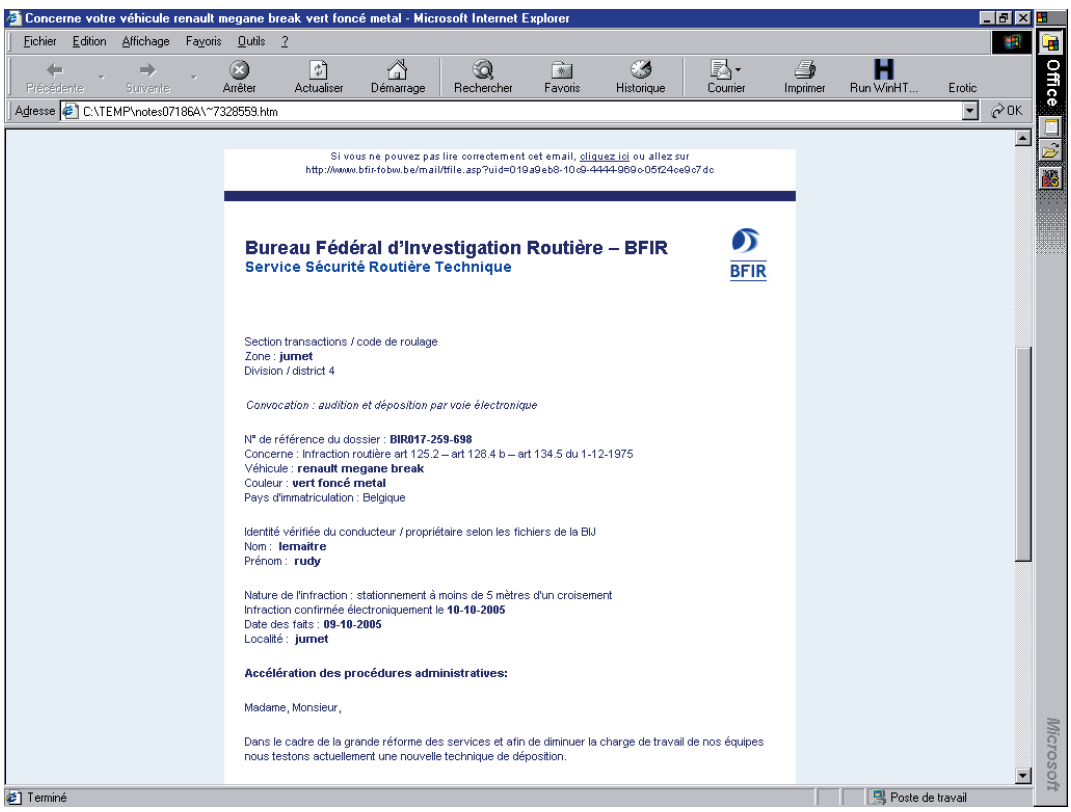
Illustrations

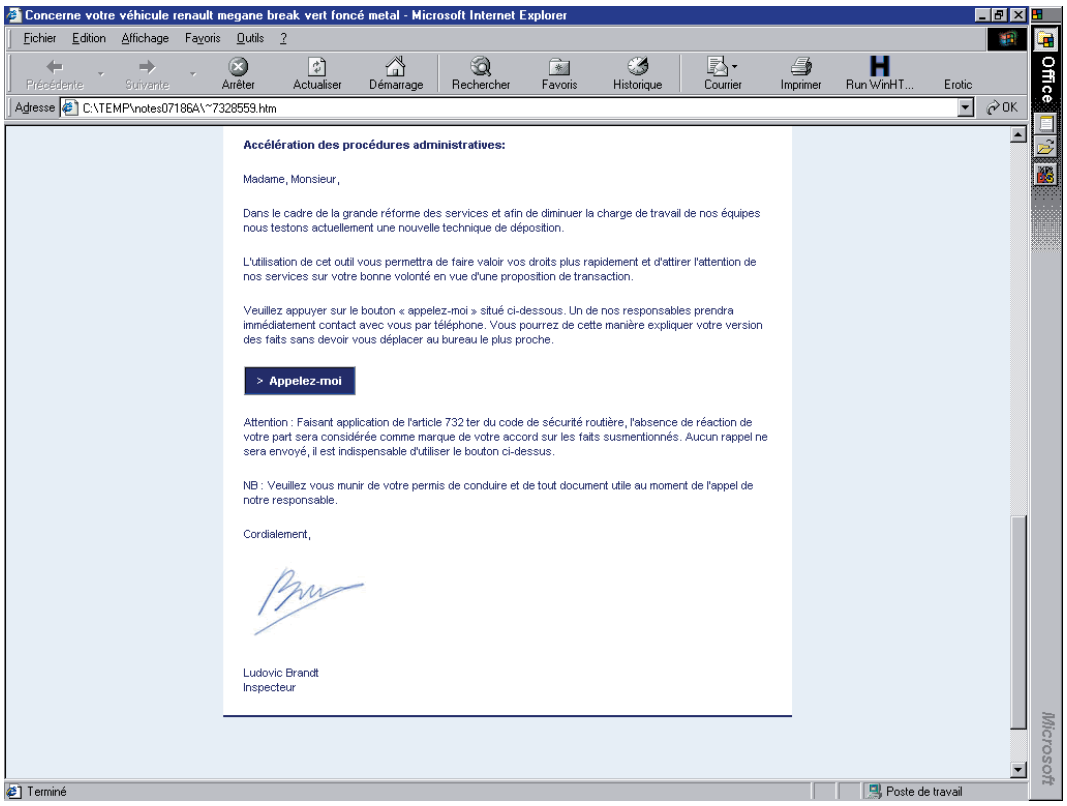
Exemple 1



« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

Exemple 2





Explication

On est régulièrement confronté à des campagnes publicitaires - dites de « marketing viral » - qui sont menées tant sur internet que dans le monde traditionnel. C'est le rêve caché de toutes les marques : transformer le consommateur-internaute lui-même en vecteur de promotion.

Le concept est simple : il consiste à exploiter le principe du bouche à oreille dans l'environnement électronique (éventuellement combiné à l'environnement traditionnel), en diffusant un message qui donne l'envie de le colporter. La philosophie du message relevant du marketing viral est d'entrer en contact avec des personnes, non pas sous le couvert d'une marque, mais sous le couvert d'une relation, d'un ami ou d'un collègue.

Le marketing viral est par nature dynamique : le message provoque l'action d'initiative chez la personne touchée, il donne l'envie de cliquer, de répondre, de transférer, d'en parler...

De plus, il n'est pas rare que l'annonceur invite clairement l'internaute à colporter ce message, voire même, mette à disposition de ce dernier les outils pour augmenter la diffusion du message (par exemple, un site web proposant un formulaire de collecte d'adresses e-mails et d'envoi automatique du message).

Pour assurer une diffusion la plus large possible, ce type de message peut adopter différentes approches.

Cette approche peut être humoristique, par exemple en envoyant des images ou une séquence vidéo drôles, en faisant connaître un site humoristique, en lançant un canular,...

Cette approche peut également être ludique, par exemple en diffusant une information intrigante en vue de démarrer un jeu de recherches, en diffusant une information (parfois fausse !) choquante (parfois à l'extrême !) dans le seul but d'interpeller ou de faire réagir le lecteur, en lançant un jeu en ligne,...

Le message peut aussi viser à mettre en place un service (cartes électroniques, fonds d'écran, distribution d'échantillons, coupons de réduction...) voire reposer sur un système de parrainage.

Dans le premier exemple visé ci-dessus : la campagne se limite à diffuser de faux avis de recherche (sous forme d'affiches et par le biais d'un site web et de courriers électroniques) d'une créature qui adore les limonades et à lancer un jeu sous forme d'intrigue en invitant les lecteurs à laisser des messages permettant de signaler les endroits où la créature prétendument perdue aurait été soi-disant aperçue.

Comme le montre l'image-écran de cet exemple, le site web dédié à cette campagne offre à cet effet un formulaire permettant aux internautes d'encoder l'adresse de courrier électronique de leurs relations afin que l'avis de recherche en question soit envoyé à celles-ci.

Aucune mention ou information permettant de constater que l'on se trouve dans le contexte d'une campagne publicitaire n'est fournie. Ce n'est qu'à la fin de la campagne publicitaire (4 à 6 semaines plus tard) que le produit est dévoilé grâce à l'information selon laquelle la créature est réapparue, cette dernière portant le produit d'une marque célèbre en main...

Dans le second exemple visé ci-dessus : vous recevez un courrier électronique (il s'agit ici d'une image écran de votre navigateur, qui est une copie du courrier

électronique reçu) vous indiquant que vous avez commis une infraction de roulage et vous invite à prendre contact par téléphone (en appuyant sur un bouton ad hoc placé dans le courrier électronique) avec un membre de la force publique.

Ce qui est intriguant pour vous et vous donne à penser qu'il ne s'agit ni d'un canular ni d'un message publicitaire d'une campagne de marketing viral, c'est que le message paraît authentique et surtout que les informations indiquées dans le courrier (nom, prénom, marque et couleur de la voiture) sont bien les vôtres !

Vous êtes donc poussé à cliquer sur le bouton d'appel en question. A ce moment, la sonnerie de votre GSM retentit et vous êtes en communication avec le prétendu policier qui a constaté l'infraction. En réalité, il s'agit d'un canular téléphonique. Un message vous prévient que vous avez été piégé par un ami. Pour connaître son identité, il suffit de consulter un site Web déterminé, qui fait la promotion d'un nouveau modèle de véhicule...

Le canular est certes de nature à faire sourire mais il présente un risque de confusion ou de malentendu, sans compter qu'à l'avenir l'internaute pourrait ne pas prendre en compte un message – légitime cette fois – provenant des autorités judiciaires ou administratives, croyant qu'il s'agit à nouveau d'un canular !

Dans les campagnes de marketing viral, le but premier de l'annonceur consiste toujours in fine à promouvoir la vente d'un produit ou d'un service, même si en pratique, le caractère publicitaire du message ou la marque n'apparaît pas toujours dès le début de la campagne.

Les campagnes publicitaires reposant sur la technique du marketing viral sont généralement très efficaces. L'adjectif « viral » est illustratif à cet égard : il décrit le phénomène de propagation qui, notamment sur Internet, se caractérise par un système de diffusion pyramidal et une vitesse de transmission qui rappellent évidemment le mode de transmission d'un virus, d'une épidémie.

Comment réagir ?

Même si elles ne sont pas toujours de bons goûts, les campagnes publicitaires de marketing viral ne présentent certainement pas de dangers comparables à ceux

relatifs aux lettres nigérianes, fausses loteries ou autres arnaques de ce genre. Ces campagnes ne sont d'ailleurs pas interdites en tant que telles par la réglementation.

Néanmoins, la Direction générale de la Régulation et de l'Organisation du marché du SPF Economie, PME, Classes moyennes et Energie a dû rappeler aux annonceurs et agences publicitaires que ce type de campagne doit être mené dans le respect strict des dispositions légales, notamment celles des lois du 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur et du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information.

Vous trouverez la présentation détaillée des principes applicables en la matière dans la note « La légalité du marketing viral », disponible à l'adresse suivante :
http://economie.fgov.be/information_society/spamming/home_fr.htm

Au-delà du rappel des principes légaux applicables, l'objectif de cette note est de conscientiser le consommateur-internaute au jeu dans lequel l'annonceur va tenter de l'impliquer : il ne lui est pas interdit de participer à une campagne publicitaire de marketing viral mais il doit savoir de manière claire qu'il devient ainsi un acteur dans la diffusion d'un message publicitaire pour le compte d'une marque.

C'est la raison pour laquelle le prestataire est tenu, s'il existe un risque de confusion dans le chef du destinataire du message, d'indiquer la mention « Publicité » sur les supports de cette campagne tels que les affiches, les encarts dans la presse écrite, le site web dédié à la campagne ainsi que les éventuels courriers électroniques envoyés dans ce cadre, et ce dès le début de la campagne de marketing viral.

Les informations permettant au consommateur de déterminer qui se cache derrière cette campagne doivent également être fournies (coordonnées de l'annonceur et/ou de l'agence publicitaire).

Il appartient bien entendu au consommateur de prendre ses responsabilités et de décider en connaissance de cause s'il rentre ou non dans le jeu et s'il participe activement à cette campagne.

L'objectif de cette note est aussi d'éveiller le consommateur-internaute aux risques que peuvent présenter la collecte et l'utilisation de ses données per-

sonnelles ainsi que celles de ses relations lorsqu'il participe à une telle campagne.

Pour rappel, le marketing viral fonctionne sur le principe du « bouche à oreille ». L'idée donc est d'inciter l'internaute à exploiter son carnet d'adresses pour colporter le message. **Dans ce cadre, nous vous donnons deux conseils essentiels**.

Le premier conseil est le suivant : pour éviter que les adresses de courrier électronique des relations ne soient visibles par tous les destinataires du courrier électronique transmis et, ainsi, limiter le risque de collecte et d'utilisation à des fins de spamming, **nous conseillons fermement à l'émetteur d'inclure les adresses e-mail dans le champ « ccc » (Copie Conforme Cachée) ou « cci » (Copie Conforme Invisible) ou encore « bcc » (Blind Carbon Copy) de sa messagerie électronique**. De la sorte, chaque destinataire reçoit le message sans que ne soient mentionnées les adresses des autres destinataires.

Le second conseil est le suivant : si un site web vous demande d'introduire dans un formulaire l'adresse de courrier électronique d'une ou plusieurs connaissances en vue de leur communiquer telles actions, informations, promotions, etc, dites-vous bien que non seulement vous le faites à l'insu de votre connaissance mais en plus que vous n'êtes pas certain(e) que l'adresse communiquée ne sera pas utilisée par le responsable du site web à d'autres fins (actions de promotion non visées, vente des adresses à des tiers, etc). **Ce faisant, vous contribuez dans une certaine mesure à augmenter le nombre de spam que risquent de recevoir vos connaissances ! Est-ce bien cela qu'ils attendent de vous ? A vous de prendre vos responsabilités… Si vous voulez informer vos connaissances d'initiatives intéressantes, envoyez leur directement un courrier électronique, plutôt que d'introduire leur adresse dans un formulaire sur un site web dont vous ne connaissez rien. C'est tellement plus simple !**

Le lecteur trouvera une information complète sur cette problématique dans la note précitée du SPF Economie.

Pour en savoir plus

Note du SPF Economie relative à « la légalité du marketing viral » :
www.economie.fgov.be/information_society/spamming/home_fr.htm ;

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

Le site web « hoaxbuster » : www.hoaxbuster.com ;

Le site web « Arnaques » du CRIOC : www.arnaques.be.

Novembre 2006

Direction générale de la Régulation et de l'Organisation du Marché

Cellule économie électronique