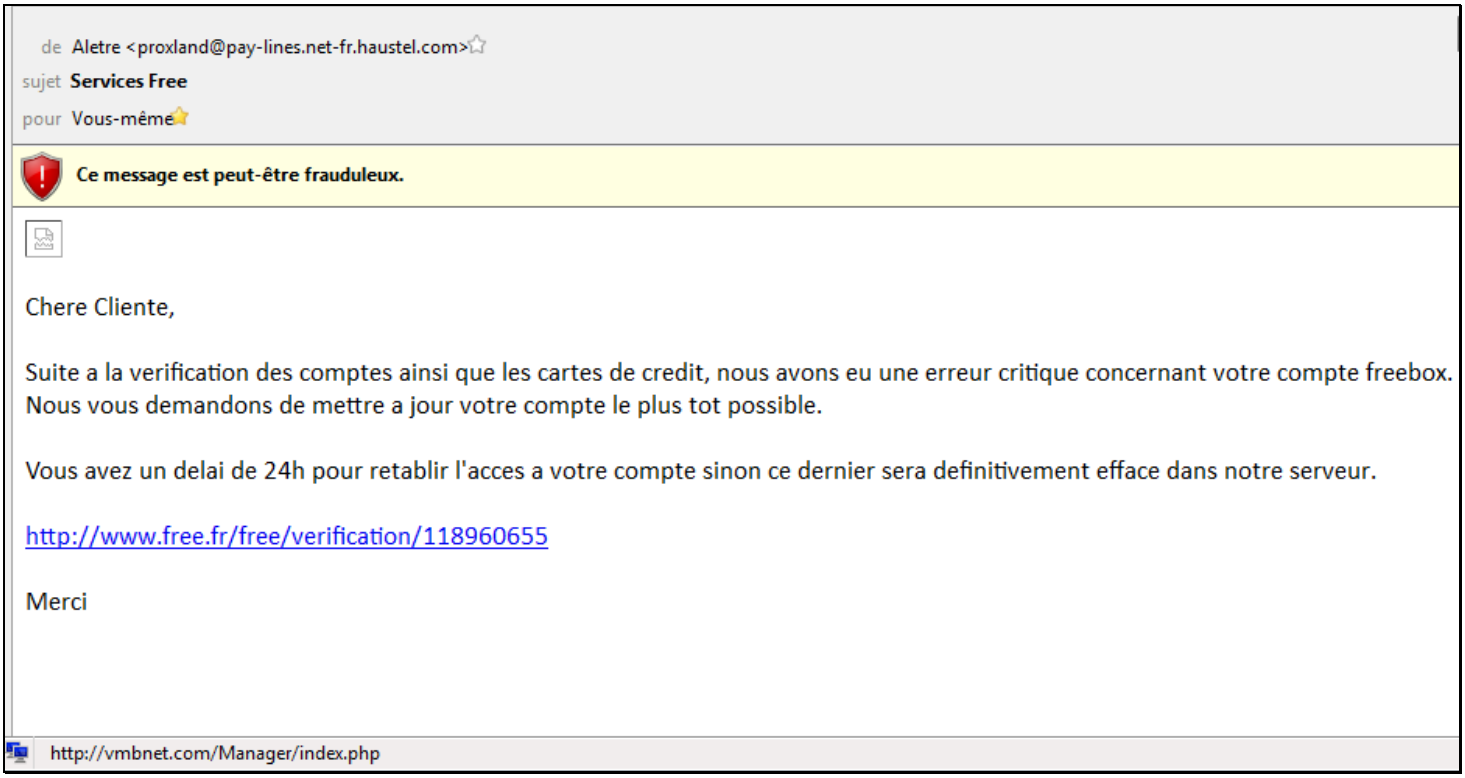
A quoi ça ressemble du phishing* ?

Nous vous alertons régulièrement sur les risques liés à des courriels de phishing (hameçonnage) mais vous vous êtes peut être déjà demandé à quoi cela pouvait ressembler.

En voici l'illustration.

Tout commence par un courriel alarmiste qui clame que si vous ne cliquez pas sur le lien qu'il contient, les pires choses vont vous arriver.

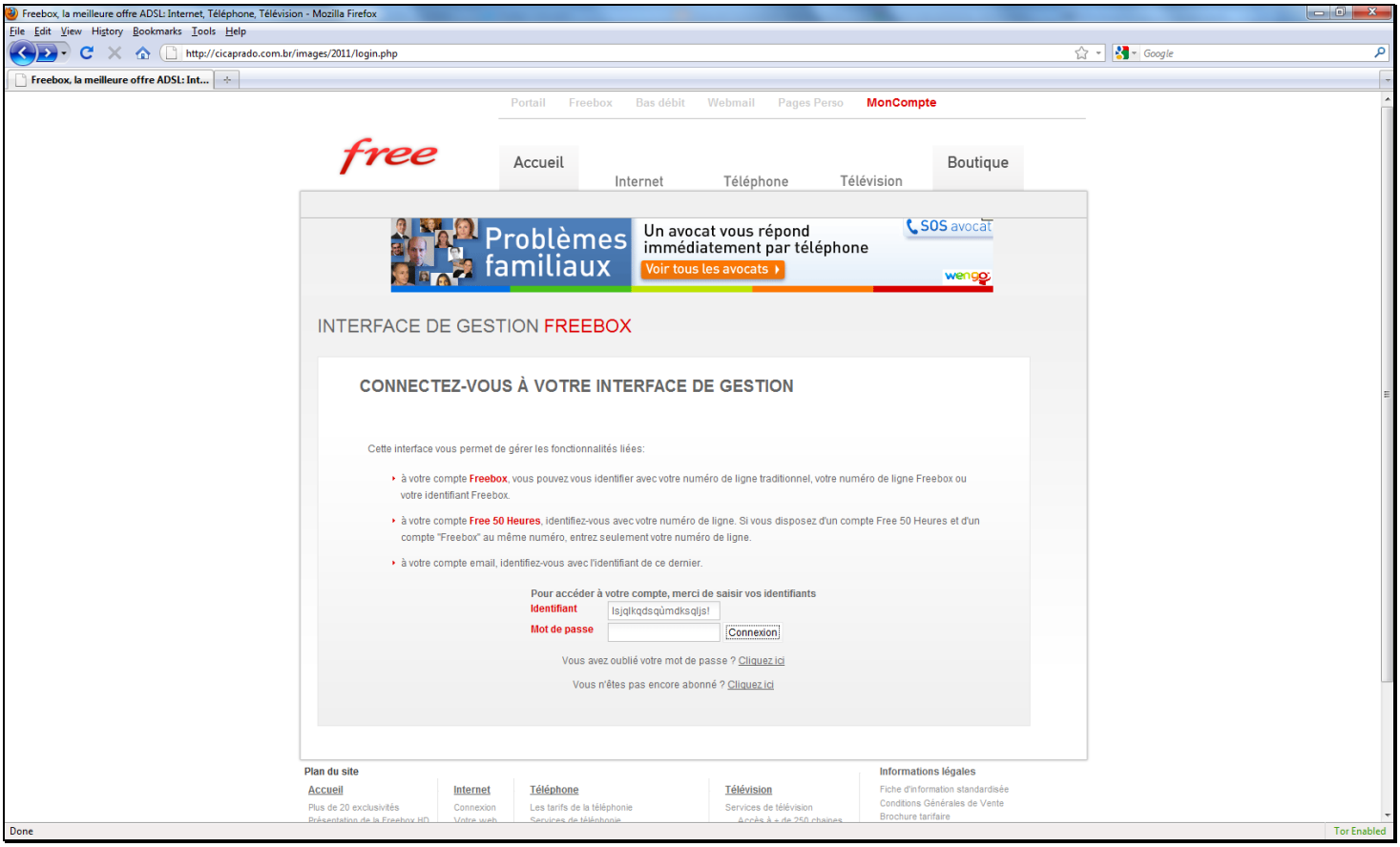


A ce niveau, deux éléments posent déjà problème :

- le courriel émane d'une adresse @pay-lines.net.fr.haustel.com dont on a du mal à comprendre le rapport avec la société Free
- lorsque l'on survole le lien avec la souris, on s'aperçoit que celui-ci ne renvoie pas chez Free (adresses du type free.com) comme il prétend le faire mais sur une adresse vmbnet.com (l'adresse tout en bas de l'image).

* : Le terme anglais phishing est une variante orthographique du mot fishing; il s'agit d'une variation orthographique du même type que le terme phreaking (f remplacé par ph). Il aurait été inventé par les « pirates » qui essayaient de voler des comptes AOL et serait construit sur l'expression anglaise password harvesting fishing, soit « pêche aux mots de passe » : un attaquant se faisait passer pour un membre de l'équipe AOL et envoyait un message instantané à une victime potentielle. Ce message demandait à la victime d'indiquer son mot de passe, afin de, par exemple, « vérifier son compte AOL » ou « confirmer ses informations bancaires ». Une fois que la victime avait révélé son mot de passe, l'attaquant pouvait accéder au compte et l'utiliser à des fins malveillantes, comme l'envoi de spam. /Wikipédia/

En cliquant malgré tout sur le lien, on arrive sur une copie de la page d'authentification de Free mais hébergée sur un serveur à l'adresse http://cicaprado.com.br/images/2011/login.php et non chez Free :

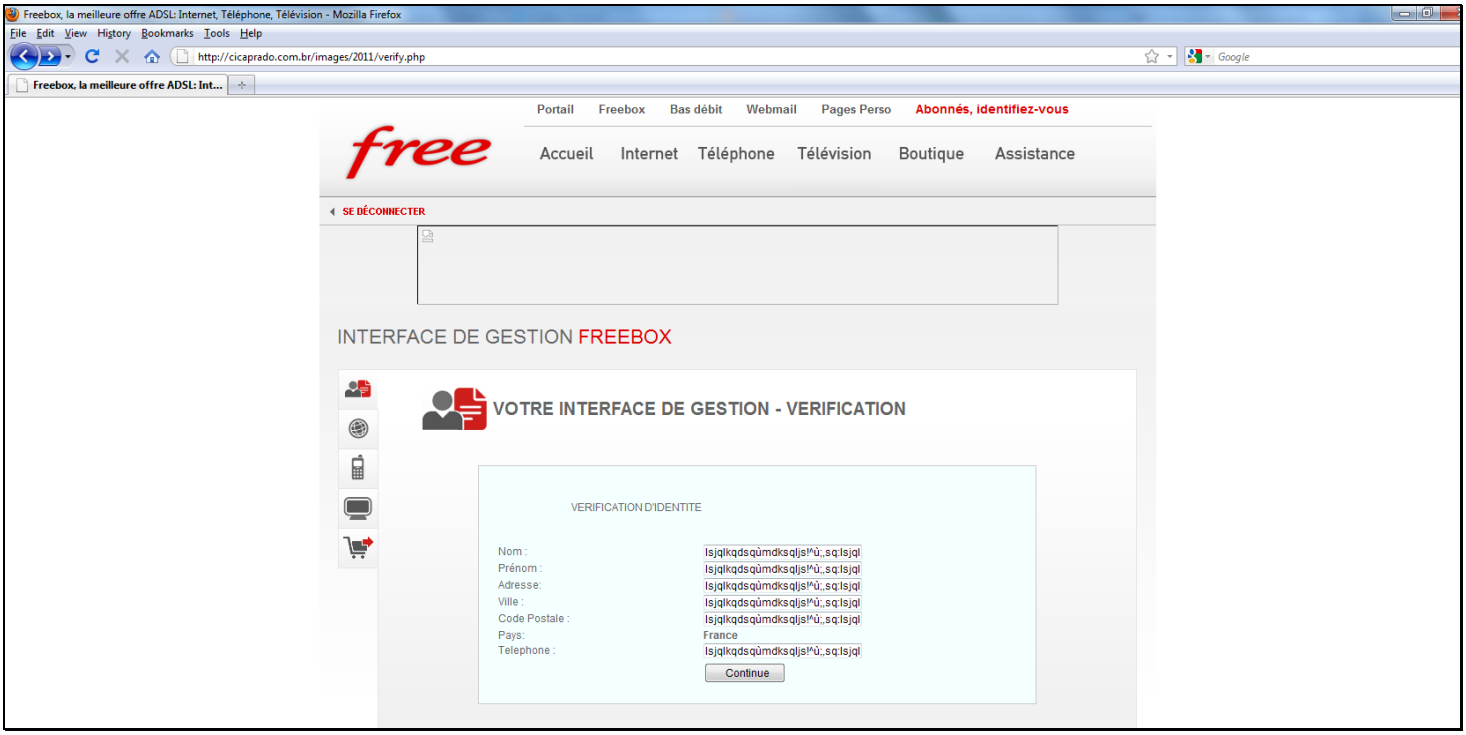


A ce stade, si vous remplissez les informations de nom d'utilisateur et de mot de passe et cliquez sur [Connexion], vous fournissez déjà éventuellement des informations intéressantes aux pirates à supposer qu'ils les récupèrent. Mais généralement ce n'est pas leur but premier.

En effet, on observe qu'en rentrant n'importe quoi comme données, y compris des choses qui ne peuvent être des identifiants (blabla et test), on accède tout de même à l'étape suivante, il n'y a donc aucun contrôle de ces données.

Vous arrivez alors sur une page de confirmation de vos informations personnelles.

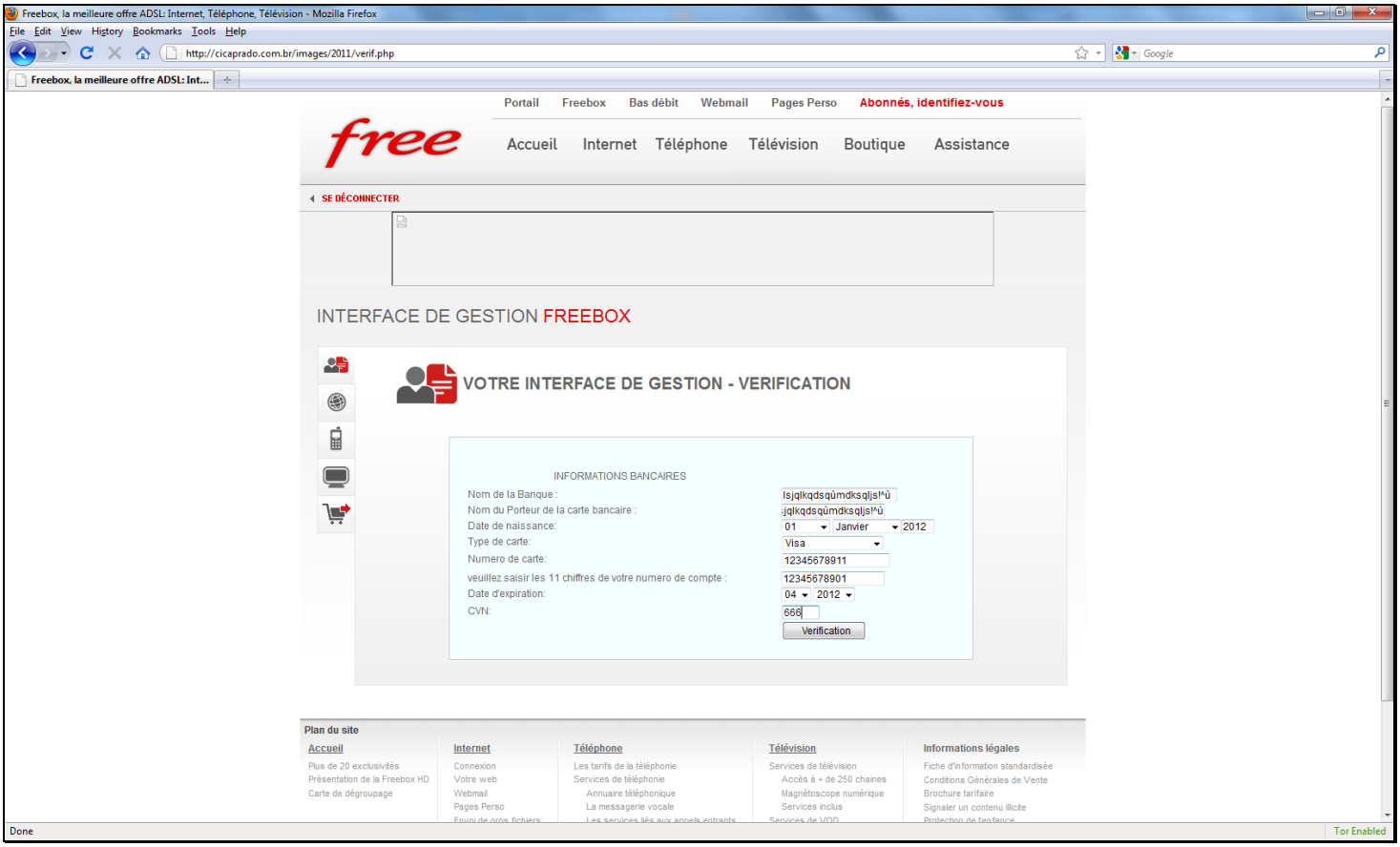
Le but est alors clairement d'endormir votre méfiance en donnant l'impression de suivre une procédure rigoureuse :



Ici encore, même si on entre n'importe quoi, on accède à l'étape suivante.

Vous arrivez alors au cœur du piratage. Toute la procédure précédente a été mise en place dans le but de vous faire atteindre cette page qui va vous soutirer votre numéro de carte bancaire, sa date de validité mais également la clé située au dos de la carte !

On notera qu'ici les pirates ne sont pas trop "gourmands" puisqu'ils ne vont pas jusqu'à demander le code de la carte. S'ils l'avaient fait, il y a fort à parier qu'ils auraient moins de réponses car cela éveillerait bien plus la méfiance.



En cliquant sur [Vérification] vous envoyez aux pirates toutes les informations nécessaires à l'utilisation de votre carte bleue. Ils peuvent dans la minute faire, par exemple, des achats sur internet.

A ce stade tout va très vite, votre compte va être vidé dans les plus brefs délais avant que vous ne réagissiez, et éventuellement, vos informations bancaires seront mises en vente parmi des milliers d'autres sur des sites spécialisés.

Si vous soupçonnez être victime du piratage de votre compte, contactez immédiatement votre banque pour faire opposition.

Face à de tel type de courriel restez donc circonspects :

> Méfiez-vous des messages alarmistes vous demandant des informations en urgence, en particulier ceux comportant un lien sur lequel vous êtes censés cliquer. Ne jamais communiquer vos identifiants ou mots de passe d'accès et vos informations bancaires personnelles y compris le RIB même si l'expéditeur présumé est un organisme officiel connu. Dans le doute, contacter l'expéditeur supposé du message pour déterminer s'il émane bien de lui et s'il est effectivement nécessaire de réactiver un compte ou de procéder à une modification de données.
>
> Regardez soigneusement l'adresse Internet (www.nom-du-site.com...) vers laquelle on vous renvoie et vérifiez qu'il s'agit bien à la lettre près de l'adresse qui était signalée dans le courriel. Même si l'adresse comprise dans le courriel est conforme à l'adresse officielle, il reste très facile pour le pirate de vous renvoyer vers un site frauduleux. Vérifiez toujours que le site sur lequel vous êtes connecté correspond bien exactement, à la lettre près, au site censé vous avoir envoyé le message.

Un petit florilège non exhaustif…

-------- Message original --------
Sujet: Cher utilisateur Webmail
Date : Tue, 6 Jul 2010 7:18:38 +0800
De : Webmail Helpdesk<computerdept@w.cn> <annalpc@netvigator.com>

Cher utilisateur Webmail
Votre webmail quota a dépassé l'ensemble quota / limite de ce qui est 20GB.You sont actuellement diffusées sur 23FR en raison de fichiers et dossiers cachés dans votre boîte aux lettres. S'il vous plaît cliquer sur le lien ci-dessous pour valider votre boîte aux lettres et d'augmenter votre quota.
Cliquez ici http://webaccountupgrade.4-all.org/
Le non-cliquez sur le lien ci-dessus et de valider votre quota peut entraîner une perte d'information importante dans votre boîte aux lettres ou causer un accès limité à elle.
Merci de votre compréhension.
Centre Support Helpdesk Webmail

-------- Message original --------
Sujet: Erreur de ComptabilitX
Date : Sat, 27 Nov 2010 21:21:53 +0800 (CST)
De : Webmail.Free <compte@free.fr>

Cher abonne :
Dans l impossibilite de vous joindre nous vous envoyons ce mail pour vous informer que
suite a une erreur comptable, On a debite votre compte de la somme 89.70
ce qui constitue le triple de votre abonnement mensuel 29.90
A fin de vous reverser la somme suscite, et regulariser la situation, vous
etes invite a remplir dument la fiche envoye dans ce message.
Cliquer ici pour ouvrir votre fiche
(http://webmail.free.fr

Nous vous remercions de votre comprehension.
Si notre service comptable ne vous contacte pas sur le telephone que vous
allez fournir dans le formulaire (portable de preferences) cela signifie que
les informations communiquees sont erronees ou incompletes, dans ce cas
nous declinons toutes responsabilites j uridique.
Service comptabilite.

------- Message original --------
Sujet: Alert ! Mauvaise Essaye d'acces
Date : Sat, 27 Nov 2010 01:12:47 -0000
De : Services Caisse Deprgne <account-verification-noreply@home.pl>

Bonjour ,
4

_____
Nous vous invitons Ã cliquez sur le lien suivant qui ne vous prendra que 10 minutes maximum.
_____
_____
http://aze4azez.ueuo.com/aa1ez.bmp

Collectez des S'Miles avec la Caisse d'Epargne Collectez des S'Miles
avec la Caisse d'Epargne

-------- Message original --------
Sujet: Erreur de ComptabilitX
Date : Sat, 27 Nov 2010 21:21:53 +0800 (CST)
De : Webmail.Free <compte@free.fr>

Cher abonne :
Dans l impossibilite de vous joindre nous vous envoyons ce mail pour vous informer que
suite a une erreur comptable, On a debite votre compte de la somme 89.70
ce qui constitue le triple de votre abonnement mensuel 29.90
A fin de vous reverser la somme suscite, et regulariser la situation, vous
etes invite a remplir dument la fiche envoye dans ce message.
Cliquer ici pour ouvrir votre fiche
(http://webmail.free.fr
Nous vous remercions de votre comprehension.
Si notre service comptable ne vous contacte pas sur le telephone que vous
allez fournir dans le formulaire (portable de preferences) cela signifie que
les informations communiquees sont erronees ou incompletes, dans ce cas
nous declinons toutes responsabilites j uridique.
Service comptabilite.

-------- Message original --------
Sujet: GAME ONLINE RESULT
Date : Tue, 14 Dec 2010 07:11:10 +0100
De : LOTTERIA INTERNACIONAL DE ESPAÑA <euro10espa@luckymail.com>
Répondre à : euro10espa@luckymail.com

LOTTERIA INTERNACIONAL DE ESPAÑA.
*****LOTTERY EMAIL DRAW 13TH DEC / 2010
****GAME ONLINE RESULT.
==========
LUCKY STAR GAME// 8 EMAIL ID IN ROW
// AMOUNT TO EACH = €980.000

LOTTO-HOTPICKS// 133 EMAIL ID IN ROW
// AMOUNT TO EACH = €420.000

EURO MILLION// 15 EMAIL ID IN ROW
// AMOUNT TO EACH = €850.000
|ID freddy.lege@univ-poitiers.fr ON ROW NUMBER "43"|
| CODE REF: 2010/AXN/30_4 |
==========
ATTENTION,
Review result draws of the SPANISH INTERNATIONAL LOTTERY AWARD.
Your freddy.lege@univ-poitiers.fr ON ROW NUMBER "43" has emerge winner and has been
awarded a prize of €850,000 (EIGHT HUNDRED AND FIFTY THOUSAND EUROS).
The acredited account owner should contact RESULTS CHECKERS immediately
on payment initiation with the above winning CODE REF: NUMBERS and
the below requested personal contact.
1* Fulnames
2* Telephone number
3* Mobile number
4* Fax number
5* Country
==========
RESULTS CHECKERS DEPARTMENT.
CLAIMS DIRECTOR. Mr. Rold Mark,
C/ General Margallo 1, 1ºD
28020, Madrid.
Email: global_agencia@luckymail.com
[fax: +34-911820312, tel: +34-698344604]
****

This email is confidential and is intended solely for the person or Entity that own this email address. If you have received this message in error, we inform you that the content in it is reserved and unauthorized use is prohibited by law, therefore, please notify us by e-mail.

-------- Message original --------
Sujet: Gagnez un serveur de migration!
Date : Wed, 15 Dec 2010 12:20:18 +0200
De : Microsoft <correct.way1@yahoo.com>
Répondre à : Microsoft <correct.way1@yahoo.com>

Si ce message ne s'affiche pas correctement, visualisez la version en ligne.

Microsoft France

Et si vous passiez AUJOURD'HUI au système d'information de demain ?

Découvrez Windows Server 2008 R2, la dernière version de Windows Server®, et tirez le meilleur parti des innovations matérielles serveurs !

*Jeu gratuit sans obligation d'achat du 28 octobre au 17 décembre soumis à règlement

Inscrivez-vous aux newsletters | Ne plus recevoir d'emails promotionnels de Microsoft France | Gérez votre profil
© 2010 Microsoft Corporation | Conditions d'utilisation | Confidentialité

Conformément à la loi informatique & libertés du 6 janvier 1978, je dispose d'un droit d'accès, de rectification et d'opposition aux données personnelles me concernant.
Ce message commercial vous est envoyé par "Team Leaders". Vous recevez ce message parce que vous vous êtes inscrit sur l'un des sites partenaires de "Team Leaders". Vos données nominatives n'ont pas été transmises à l'annonceur. Si vous ne souhaitez plus recevoir notre lettre d'information Remplissez ce formulaire.

-------- Message original --------
Sujet: c'est le dernier alerte pour acceder a votre compte le plus vite possible.
Date : Wed, 22 Dec 2010 15:05:12 +0100
De : service paypal<support@optonline.net>

PayPal
Bonjour
Dans le cadre de nos mesures de sécurité, nous contrôlons régulièrement les activités en cours dans le système PayPal.
Nous vous avons récemment contacté à la suite d'un problème sur votre compte PayPal.
Des informations vous ont été demandées pour le motif suivant :
Notre système a détecté des débits inhabituels sur une carte de crédit associée à votre compte PayPal.
Dossier nº : PP-1124-075-998
Ceci est un dernier rappel vous invitant à vous connecter à PayPal dès que possible.
Veuillez rétablir l'accès à votre compte *(http://black-water.pl/images/logs/*).
Veuillez ne pas répondre à cet email. Les emails envoyés à cette adresse ne peuvent pas recevoir de réponse.
Copyright 1999-2010 PayPal. Tous droits reserves.
PayPal (Europe) S. r.l. & Cie, S.C.A.
Societe en Commandite par Actions
Sige social : 22-24 Boulevard Royal L-2449, Luxembourg
RCS Luxembourg B 118 349
Email PayPal n PP1268

-------- Message original --------
Sujet: Erreur de soustraction sur votre budget
Date : Tue, 28 Dec 2010 10:49:48 -0600 (CST)
De : Free Administration <Email--3mg@Assistance.fr>

Free Administration

Bonjour, cher (e) client (e) :

Apres plusieurs tentatives infructueuses de vous joindre par telephone ,nous
vous envoyons ce mail pour vous informer qu une erreur est survenue lors des
prelevements mensuels effectues sur le compte de notre clientele.
En effet le 25 decembre 2010 votre compte a ete indument debite de la somme
de (89.00) quatre vingt neuf Euros .
Ce probleme est essentiellement du la similitude de vos noms et prenoms avec
ceux d un autre client .
A fin de proceder a un remboursement immediat nous vous prions de bien
vouloir cliquer sur le lien ci-dessous et fournir toute information
susceptible d accelerer ce remboursement .

Remplissez le formulaire de remboursement en cliquant sur le lien suivant:

http://anglinfinancial.com/free.fr/

Cordialement,

Fabrice Andre,
Directeur Service Client
*En cas de non reponse a ce message, Free decline toute responsabilite
juridique au non remboursement de la somme sus-citee.