

Un phishing mal fait

Chère Madame, cher Monsieur, :

*Cet email confirme que **Vous** avez bien **créé** un nouveau mot de passe et **sélectionne** des questions **Secrètes** pour votre compte*

*Si vous n'avez pas **effectue** ces Modifications*

*En effet le 25 Mars 2011 nous avons **Prélever** une somme erronée de 137.30 **EURO** Cet confusion est essentiellement **du** la Correspondance de vos noms et prénoms avec ceux d un autre Client.*

A fin de procéder a un remboursement on votre faveur nous Vous prions de bien vouloir cliquer sur le lien ci-dessous et fournir toute Information susceptible d accélérer ce reversement.

*Remplissez le formulaire information de en cliquant sur ce lien **si** Dessous:*

<https://verified.visa.com/aam/data/default/landing.aam?partner=default&resize=yes>

1-Connectez-Vous

2-Confirmer vos informations de compte.

3-Reconnectez vous.

Nous vous remercions de votre grande attention a cette Question. S'il vous plait comprenez que c'est une mesure de sécurité destinée a Vous protéger ainsi que votre compte. Nous nous excusons pour tout inconvénient...

Ce qu'il faut remarquer :

- **Le mail est truffé de fautes d'orthographe et de syntaxe (quelques exemples en rouge)**
- Il n'y a **pas d'accents**. Il s'agit très probablement d'un mail rédigé à l'aide d'un clavier qwerty (sans accents) et retraduit ensuite.
- **Le lien** donné semble valide, mais renvoie sur un site tout à fait différent... (<http://www.adripeeathome.com>)
- Demande de **fourniture des numéros/identifiants**
- **Le contenu abracadabrant** : on nous parle dans un premier temps de notre création de compte et l'on enchaîne sur un prélèvement prétendument abusif... En quoi la création d'un compte sur un site générerait un prélèvement abusif ?
- **Le manque de logique** : si ils ont été capables de prélever de l'argent sur un compte, ils disposent logiquement de toutes les informations nécessaires pour rembourser la somme...

Il s'agit donc d'une escroquerie. Ne répondez pas. Mettez ce mail à la poubelle.

Un phishing bien fait

Sujet: c'est le dernier alerte pour accéder à votre compte le plus vite possible.
De : "service paypal" <supportt@optonline.net>
Date : 26/12/10 13:09
Pour : undisclosed-recipients;

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 n° : 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.](#)

Veillez ne pas répondre à cet email. Les emails envoyés à cette adresse ne peuvent pas recevoir de réponse.

Copyright 1999-2010 PayPal. Tous droits réservés.

PayPal (Europe) S. r.l. & Cie, S.C.A.
Société en Commandite par Actions
Siège social : 22-24 Boulevard Royal L-2449, Luxembourg
RCS Luxembourg B 118 349

Email PayPal n PP1268

Ce qu'il faut remarquer :

- **L'expéditeur** dit se prénommer « service paypal » mais l'adresse email ne correspond pas du tout à Paypal (optonline.net)
- **Les destinataires** ne s'affichent pas. Ce mail est sans doute envoyé à de très nombreuses personnes.
- **Le lien est falsifié.** Il ne renvoie absolument pas vers un site Paypal.
- **La volonté d'être crédible.** Ce mail paraît plutôt très crédible grâce à la présence du logo PayPal, des coordonnées très précises (il s'agit d'ailleurs des vraies coordonnées de Paypal).
- **La demande indirecte.** Ce mail est d'autant plus redoutable qu'il ne vous demande pas d'emblée de fournir des informations confidentielles mais uniquement de vous connecter à une page afin de vérifier votre compte.

Encore une fois, il s'agit d'un phishing, le site a sans doute été falsifié afin de vous amener à vous connecter à Paypal et ainsi récupérer vos coordonnées.