La pêche aux gogos !

Dans le monde de la fraude en ligne, la mode est au *phishing* ou *scam*. *Quezako* ? Une escroquerie qui profite de la crédulité des internautes pour les dépouiller.

Un récent rapport américain d'associations de consommateurs révèle, selon le journal en ligne *The Register*, que le nombre de plaintes concernant des opérations frauduleuses de commerce électronique est en hausse aux États-Unis. Montrés du doigt : les sites de vente pour des produits livrés en retard ou pas du tout, mais aussi les enchères en ligne. Sans oublier les arnaques par mail : ceux promettant aux gens de devenir riches rapidement, et ceux – très fameux – venus d'Afrique (la fraude 419 des Nigérians).

On trouve aussi les offres de crédit particulièrement alléchantes mais frauduleuses, qui passent par la messagerie électronique, les messages à caractère pornographique, ceux qui vous proposent de perdre du poids, etc.

Bref, des messages que l'on reçoit en masse. Aujourd'hui, selon les chiffres de plusieurs fournisseurs d'accès, la moitié des mails seraient des *spams*. Souvent en anglais, et d'un contenu facilement reconnaissable, les *spams* sont plus pénibles que dangereux. Sauf quand ils imitent à s'y méprendre un vrai site dans le but de soutirer mots de passe et numéro de carte bleue. Encore très peu répandue en France, cette pratique appelée *phishing* a récemment touché le secteur bancaire aux États-Unis et en Grande Bretagne. Là encore, un peu de bon sens suffit en général à sauver la mise, même si ce genre de fraude est pour le moins vicieux.

LE PHISHING

Aller à la pêche aux gogos sur le Net est une activité qui peut se révéler lucrative. Les moyens foisonnent et les pirates ne manquent pas d'idées. Le *phishing*, surtout populaire Outre-Manche et Outre-Atlantique, consiste à envoyer un mail portant les couleurs et le logo d'une société, en général une banque (*Paypal* et *Ebay* ont aussi récemment subi ce genre de détournement), afin de soutirer un numéro de carte bleue. Sous le prétexte d'actualiser ses données, ou d'un « contrôle de sécurité de routine », le client doit cliquer sur un lien contenu dans le mail, lien qui le renvoie vers une page où il doit fournir numéro de carte bleue et code secret :

Please verify your information today!

Dear Paypal Member,

Your account has been randomly flagged in our system as a part of our routine security measure. This is a must to ensure that only you have access and use of your paypal account and to ensure a safe paypal experience.

We require all flagged accounts to verify their information on file with us.

To verify your information, click here and enter the details requested.

Thank you for using Paypal!

LES HOAXES

Ces rumeurs circulent elles aussi par mail. La plupart ne réclament pas d'argent, se contentant de véhiculer des informations fausses et de demander aux destinataires de les propager. Mais certains vous promettent de gagner de l'argent rapidement (en général, il faut commencer par avancer...), ou de vous prêter de l'argent à des taux défiant toute concurrence. Les fameuses fraudes 419, en provenance du Nigéria, figurent en bonne place dans la liste. Ces fraudes sont appelées les fraudes 419 par allusion à l'article du code nigérian qui les punit. Ces arnaques représenteraient, selon la Banque de Floride, la cinquième industrie du pays.

Une personne, en général le proche d'un haut dignitaire africain, vous demande par mail de bien vouloir l'aider à sortir de son pays une grosse somme d'argent, moyennant une commission. Si l'on mord, il faut ensuite commencer par verser un acompte...

Le Nigéria s'apprête à ouvrir un bureau spécialisé dans la poursuite de ces fraudeurs. En attendant, continuez de faire comme votre maman vous l'a appris, n'ouvrez la porte à personne et n'acceptez pas de bonbons de gens que vous ne connaissez pas...

5 conseils d'usage

1

Ne donnez jamais votre numéro de carte bleue sur un site qui n'est pas sécurisé.

2

Ne répondez pas à un *spam*, même si c'est pour demander de ne plus le recevoir, cela produirait l'effet inverse en confirmant votre adresse mail.

3

De façon générale, ne prêtez aucune foi à tous les mails, d'où qu'ils viennent, qui vous promettent de gagner beaucoup d'argent rapidement.

4

Accédez toujours au site de votre banque en tapant vous-même son URL.

5

Si vous constatez la moindre irrégularité sur votre compte bancaire, contactez immédiatement votre banque... par téléphone !

Magazine « .Net », Janvier 2004, p. 32-33