INDECOSA la cgt CONSOM' ACTION
www.indecosa.cgt.fr

Internet : comment éviter les fraudes ?

Octobre2013

FICHE PRATIQUE

Face aux multiples arnaques qui guettent les internautes sur la toile, quelques précautions s'imposent et quelques règles de base sont à rappeler.

Achat de médicaments en ligne : prudence obligatoire

Ne jamais acheter de médicaments sur le web en dehors des sites autorisés. L'Ordre des pharmaciens tient à jour la liste de ces sites sur son propre site Internet. Selon l'OMS, un médicament sur deux vendu sur la toile serait contrefait. Au mieux, le médicament est inactif, au pis il est dangereux. Ce marché en France représenterait un milliard d'euros.

Comment repérer les sites illégaux ? Mis en lignes par des fraudeurs souvent installés à l'étranger, il n'est pas rare d'y constater des fautes d'orthographe ou une hotline inaccessible. La vente proposée concerne souvent les stimulants sexuels, les produits pour booster le développement de la masse musculaire, et d'autres pour perdre du poids, parfois interdits en France.

Se méfier des prix excessivement bas.

Comme sur beaucoup d'autres sites marchands frauduleux, les tarifs y sont anormalement bas. Attention en effet aux trop bonnes affaires ! Vous risquer de payer des achats que vous ne recevrez jamais.

Certains sites marchands n'existent que le temps d'empocher votre argent puis, conçus pour être éphémères, disparaissent quelques jours plus tard. Prenez le temps de vérifier les coordonnées du site, le nom de la société, une adresse physique, un numéro de téléphone ainsi que les conditions générales de vente.

S'assurer que le paiement est sécurisé

Avant de régler votre achat, relisez attentivement le récapitulatif de la commande et vérifiez qu'il correspond bien à votre achat.

Au moment de payer, un petit cadenas, symbole de sécurité, doit apparaître sur l'écran et l'adresse URL doit débuter par https, le « s » signifiant « sécurisé ».

Attention au « phishing »

Le « phishing » consiste à vous envoyer des courriers électroniques frauduleux dans le but de récupérer vos données personnelles, principalement vos coordonnées bancaires. Les escrocs utilisent le plus souvent la contrefaçon de sites Internet officiels ou très connus, donc crédibles (une banque, un service public…). Les informations recueillies par les « phishers » sont ensuite utilisées pour effectuer des paiements ou retraits frauduleux à partir de votre compte bancaire.

Face au « phishing » et au « spam », des messages non sollicités (courriers électroniques, SMS ou MMS) envoyés par des expéditeurs inconnus ou difficilement identifiables, ne répondez jamais. Supprimez les messages sans ouvrir les pièces jointes et signalez leur présence sur la plateforme partenaire de la CNIL, www.signal-spam.fr

Pour en savoir plus : http://www.securite-informatique.gouv.fr/gp_rubrique34.html

Dossier préparé par Michèle Berzosa