

## L'hameçonnage ou phishing

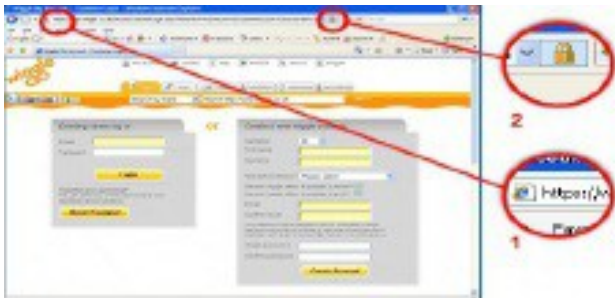
✓ L'hameçonnage ou *phishing* est une attaque ciblée consistant à dérober des informations confidentielles. Vous recevez un e-mail avec un lien ou une pièce jointe. En cliquant sur ce lien ou sur cette pièce jointe, vous êtes dirigé sur un site piégé qui vous invite souvent à ressaisir vos informations confidentielles (ex : numéro de carte bleue) pour confirmation ou vérification.

✓ Ces informations, saisies dans un faux formulaire, sont alors utilisées à mauvais escient par des escrocs.

### Comment éviter le phishing ?

- Je ne réponds pas à un e-mail qui me demande de transmettre mes coordonnées bancaires. Je sais que ma banque ou toute autre institution de confiance **ne me les demandera jamais par e-mail.**

- Quand je dois « rentrer » mes coordonnées bancaires dans un site (ex : site de vente en ligne), la page doit être sécurisée, c'est-à-dire qu'il faut qu'il y ait, dans la barre de navigation, un « s » après http [HTTPS] et qu'un petit cadenas soit visible en haut ou en bas de la page



## L'arnaque à l'annonce...

### Attention aux trop bonnes affaires sur le Net !

**1<sup>er</sup> cas** : Vous souhaitez vendre un bien. Vous déposez une annonce en ligne sur un site de vente entre particuliers. L'acheteur envoie un chèque d'un montant bien supérieur au prix que vous lui avez fixé et vous demandez de lui reverser la différence. En réalité, vous constaterez plus tard que le chèque était volé, faux ou sans provision.

**2<sup>ème</sup> cas** : vous souhaitez acheter un bien sur un faux site de vente en ligne et vous réglez l'achat mais ne recevez pas le bien. Le vendeur prétexte ensuite des frais de transports ou de taxes pour obtenir un peu plus d'argent. En fait, vous ne recevrez jamais l'objet commandé.

**3<sup>ème</sup> cas** : *Les fausses ventes de véhicules.*

Vous pouvez être attiré sur le net par un véhicule en excellent état et à un prix très attractif. Le vendeur précise qu'il est parti à l'étranger et que vu l'urgence, il doit vendre rapidement sa voiture. Il vous invite alors à envoyer votre règlement par virement, par mandat à l'étranger ou à une tierce personne qui réside en France. La voiture ne vous sera jamais livrée !

### Comment éviter l'arnaque à l'annonce ?

- Si je vends ou achète un bien très onéreux, j'organise une rencontre avant la transaction.
- Si je vends un bien, j'attends d'avoir reçu matériellement l'argent **avant** de le livrer.

## Le scam

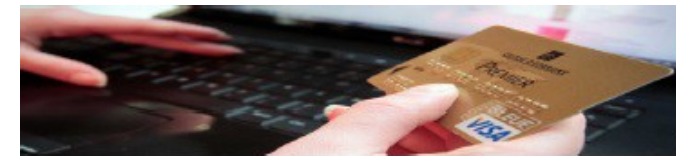
Le *scam* ou "fraude 419" est un e-mail dans lequel une personne affirme posséder une importante somme d'argent (par héritage ou gagnée à la loterie) et fait part de son besoin d'utiliser un compte existant pour transférer rapidement cet argent. Il promet, en échange, un pourcentage sur la somme qui sera transférée.

La victime accepte et avance des sommes pour des frais imaginaires et le transfert n'aura jamais lieu.

### Comment se prémunir d'un "scam" ?

Je classe immédiatement cet expéditeur en "**indésirable**" pour ne plus recevoir ses courriels. Je n'envoie pas d'argent à un inconnu via un service de transfert d'argent ou par virement bancaire.

## Les failles à repérer



**Méfiez vous** d'un interlocuteur qui ne maîtrise pas bien la langue française.

Les textes rédigés par les escrocs comportent souvent de nombreuses fautes et proviennent régulièrement de « copiés/collés ».

Sachez repérer les réponses peu précises par rapport à la question que vous posez.



L'escroquerie est prévue par l'article L. 313-1 du Code Pénal et est punie de cinq ans d'emprisonnement et jusqu'à 375.000 euros d'amende.

#### Sites utiles :

- [www.interieur.gouv.fr](http://www.interieur.gouv.fr) rubrique « escroqueries »
- [www.internet-signalement.gouv.fr](http://www.internet-signalement.gouv.fr)
- [www.securite-informatique.gouv.fr](http://www.securite-informatique.gouv.fr)



Si vous êtes **victime d'une escroquerie**, déposez plainte au commissariat ou à la gendarmerie la plus proche et munissez-vous de tout renseignement pouvant aider à l'identification de l'escroc : copies des e-mails, références du transfert d'argent effectué.

Si vous avez des doutes, appelez le 17 ou rendez-vous à un service de police ou de gendarmerie.

**Direction Départementale de la Sécurité Publique des Hautes-Pyrénées** (28-30 rue Georges Clémenceau, 65000 Tarbes)

**Groupeement de Gendarmerie des Hautes-Pyrénées** (27 rue Massey 65000 Tarbes)

## Comment éviter les pièges...

- ✓ Lors d'un achat par internet, dans la mesure du possible, entrez directement en contact avec le vendeur, par téléphone ou en face-à-face et demandez-lui des renseignements précis sur le produit. Des réponses peu précises peuvent permettre de repérer les escrocs.
- ✓ Dans la mesure du possible, privilégiez le paiement en mains propres afin de voir l'objet et de s'assurer qu'il correspond bien à celui qui vous était proposé.
- ✓ **Ne donnez pas de rendez-vous chez vous** et préférez plutôt une prise de contact dans un lieu public.
- ✓ En cas de paiement en ligne, favorisez le règlement par carte bleue virtuelle proposé par vos établissements financiers.
- ✓ Évitez les achats avec un vendeur situé dans un pays étranger.
- ✓ N'achetez pas des produits exagérément moins chers. Les trop bonnes affaires n'existent pas.
- ✓ Vérifiez sur les forums les avis des internautes sur le site de vente en ligne que vous êtes en train de visiter. Privilégiez les sites connus.
- ✓ En cas de vente de votre véhicule, n'oubliez pas de **masquer l'immatriculation** de votre véhicule avant de "poster" la photo.

Les textes des e-mails ou des sites rédigés par les escrocs comportent souvent de nombreuses fautes d'orthographe ou reflètent une mauvaise maîtrise de la langue française.



## GUIDE ANTI-CYBERCRIMINALITÉ

**Savoir se prémunir**  
**contre les escroqueries**  
**sur internet...**



**« Méfiez-vous des...  
trop bonnes ...affaires ! »**