

## PAS DE MIRACLE SUR INTERNET

### Les sites de rencontres ou de discussion en ligne :



Vous venez de rentrer en contact avec un correspondant. Après plusieurs discussions et un lien d'amitié s'établi, celui-ci vous demande de l'argent. Que faire?

- Dans de nombreux cas, l'unique objectif est de vous appâter (enfant malade, difficulté financière pour payer le billet d'avion,...) afin que vous envoyez de l'argent.

### Loterie / héritage :

Vous consultez votre boîte électronique, et vous apprenez être le grand gagnant d'une loterie ou le légataire d'un héritage. Quelques conseils pour ne pas être piégé :

- Vous ne connaissez pas l'expéditeur = DANGER supprimez le mail sans l'ouvrir
- Pour aucune loterie, le gagnant ne doit verser d'argent, ou faire un achat pour toucher son gain.
- Aucune procédure d'héritage ne peut être réalisé par e-mail, le seul but recherché par l'escroc dans ce cas :
  - Vous demander de l'argent pour régler des frais d'avocat, ou de notaire.
  - Ou recueillir vos coordonnées bancaires.



**Tous ces stratagèmes n'ont qu'un seul objectif obtenir de l'argent ou vos coordonnées bancaires à des fins malveillantes.**

Adresse de la gendarmerie la plus proche de votre domicile

## QUELQUES LIENS UTILES

<http://www.securite-informatique.gouv.fr> : Portail gouvernemental de sécurité en informatique

<http://www.signal-spam.fr> : Pour signaler un courrier électronique indésirable

<http://www.mediateurdunet.fr> : En cas de différent commercial ou privé relatif à internet

<http://www.cnil.fr/vos-libertes/plainte-en-ligne/> : Pour vos problèmes liés à l'internet, attention cette démarche ne se substitue pas à un dépôt de plainte dans une unité de gendarmerie nationale ou de la police nationale



# LUTTONS CONTRE LES ESCROQUERIES ENSEMBLE



**INFO ESCROQUERIES**  
**0811 02 02 17**  
COÛT D'UN APPEL LOCAL

POUR SIGNALER UN COURRIEL  
OU UN SITE INTERNET D'ESCROQUERIES  
[www.internet-signalement.gouv.fr](http://www.internet-signalement.gouv.fr)

## LES BONNES PRATIQUES A L'USAGE D'INTERNET

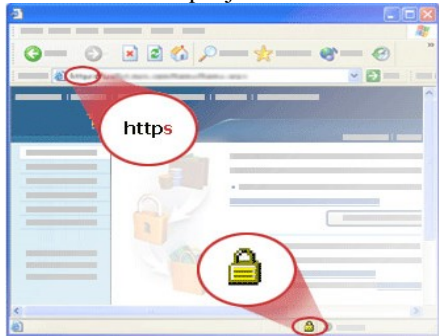
### Vis à vis de l'ordinateur :

- Mise à jour régulière du système d'exploitation (Windows, Linux,...).
- Mise à jour régulière de l'antivirus (de nouveaux virus apparaissent chaque jour).
- Activation du Pare-Feu.
- Changez régulièrement de mot de passe
- Mise à jour régulière du navigateur internet. (Internet Explorer, Mozilla Firefox, Chrome,...)



### Vis à vis de l'utilisateur :

- Je garde toujours un visuel sur ma carte bancaire (ex : ne pas laisser partir le serveur au restaurant avec sa carte bleue)
- Lorsque je fais des achats sur internet :



- je m'assure que le site internet peut-être digne de confiance.
- je suis vigilant aux cases qui sont à cocher ou à décocher et je lis les conditions qui figure sur le site
- lorsque je transmets mes données bancaires je m'assure que l'adresse url commence par https://... et qu'un cadenas est présent.
- La plupart des banques proposent des cartes bleues électroniques à usage unique pour les paiements sur internet, rapprochez-vous de votre conseiller bancaire.

## SITES D'ANNONCES ENTRE PARTICULIERS

### J'achète :



- Je suis plus attentif aux transactions réalisées à l'étranger, point de départ de beaucoup d'arnaques.
- Je suis très vigilant lors d'un paiement par mandat. (ce moyen de paiement doit être limité aux transferts de fond entre particulier qui se connaissent).
- Je privilégie le contact téléphonique ou physique, l'individu malveillant n'aime pas ce contact.
- Soyez vigilant s'il y a un écart trop important entre la

valeur de l'objet et le prix de vente.

- Je n'envoie jamais d'acompte.

### Je vends :

- Pensez à faire des photos neutres, l'acheteur ne doit pas reconnaître le lieu où est en vente l'objet, vous pourrez faciliter le travail de voleurs.
- Je vends mon véhicule, l'immatriculation ne doit pas être visible, aucune adresse, privilégiez les contacts dans des endroits publics.
- Je n'envoie aucun document administratif pour prouver ma bonne foi, l'acheteur intéressé se déplacera.



**NB : Vous remarquez une annonce frauduleuse, prenez le temps de la signaler aux administrateurs du site, cette démarche citoyenne peut éviter qu'un utilisateur distrait soit victime d'une escroquerie.**

## PHISHING / PHARMING

Le **phishing** peut être traduit par "pêche aux victimes". Des escrocs envoient des messages à un maximum d'internautes en se faisant passer pour une banque ou un organisme administratif. Ils invitent les destinataires à mettre à jour leurs coordonnées bancaires via un lien qu'ils vous communiquent. Cette demande n'a qu'un objectif **VIDER VOS COMPTES BANCAIRES**.



La [masqué] vous informe la **suspension temporaire** de votre compte dû à plusieurs tentatives d'accès incorrectes. Nous vous informons que **votre compte ainsi que votre carte bancaire vient d'être suspendu pour vérification**. **Merci de remplir ce formulaire et nous le faire parvenir en répondant à notre mail :**

- Identifiant client:
- Accès par code confidentiel:
- Nom complet:
- Date de naissance:
- Numéro de votre carte bancaire:
- Date d'expiration de la carte bancaire:
- CVV (Cryptogramme visuel) bancaire :

Une fois ces informations reçues et vérifiées, vous recevrez un mail de confirmation vous sera envoyé vous confirmant la **possibilité d'accès de nouveau à votre compte et l'utilisation de votre carte bancaire**.

Nous vous remercions,  
Service Clientèle,  
[masqué]

**Aucun établissement bancaire ou organisme public n'est à l'abri de ces attaques  
SOYEZ VIGILANT**

Le Pharming a pour objectif de copier quasiment à l'identique des sites officiels principalement ceux des banques afin de vous piéger. Soyez vigilant, l'adresse url vous permet de détecter ces faux sites (faute dans le nom, ajout de lettre, terminaison de l'url en .ru, .cx, ...)



### CONSEIL :

Enregistrez les adresses utilisées pour vos consultations de compte et d'organismes dans vos favoris. Utilisez ensuite ce lien ce qui vous évitera toute erreur de saisie.