



GENDARMERIE Internet Sécurité

## QUESTIONS / RÉPONSES

**Je viens de recevoir un e-mail bizarre, d'une personne que je ne connais pas, se disant d'origine étrangère et me demandant de l'aider. Que dois-je faire ?**

*Vous ne devez pas répondre, ni accuser réception. Ce type de message cache une tentative d'escroquerie.*

**J'ai voulu acheter un objet sur un site de vente aux enchères sur Internet. Après quelques échanges par mail avec le vendeur, je lui ai envoyé un virement de la moitié du prix. Je devais recevoir la marchandise dans les huit jours, mais je n'ai jamais rien reçu.**

*Vous avez été victime d'une escroquerie à la « fausse vente ». Vous devez signaler les faits au site marchand, et déposer une plainte au commissariat ou à la gendarmerie le plus proche de votre domicile, même si le vendeur est situé à l'étranger. Cette plainte permettra d'ouvrir une enquête.*

**En cas de plainte, des frais me seront-ils facturés ?**

*Le dépôt de plainte est une formalité totalement gratuite.*

**J'ai été victime d'une utilisation frauduleuse de mon numéro de carte de paiement sur Internet. Est-ce à moi de supporter le montant du préjudice ?**

*Si vous avez signalé le problème à votre banque, elle vous a demandé un récépissé de dépôt de plainte - Si vous avez fourni ce document, votre banque doit recréditer votre compte du montant litigieux dans le délai d'un mois.*

www.gendarmerie.interieur.gouv.fr

Le sentiment de culpabilité est fréquent chez les victimes d'escroquerie sur Internet. Mais les responsables sont les auteurs de ces infractions, déterminés à obtenir par tout moyen ce qu'ils veulent.

Si vous êtes victimes d'une escroquerie sur Internet :

- ➔ Appelez en priorité votre banque pour le signaler.
- ➔ Déposez une plainte à votre brigade de gendarmerie (si vous ne pouvez pas vous déplacer, les gendarmes peuvent prendre votre plainte à votre domicile).

## CONTACTS

Pour aller plus loin ou obtenir de l'information :

[www.gendarmerie.interieur.gouv.fr](http://www.gendarmerie.interieur.gouv.fr)



**EN CAS D'URGENCE,  
COMPOSEZ LE 17**

Votre point de contact local ?

Selon la gravité de votre incident, ce point de contact local sera en mesure de faire intervenir des enquêteurs spécialisés en cybercriminalité.

COORDONNÉES DE VOTRE CONTACT LOCAL

Pour signaler :

- des contenus illégaux sur Internet : <https://www.internet-signalement.gouv.fr>
- des courriels ou sites d'escroqueries : <https://www.internet-signalement.gouv.fr> ou 0811 02 02 17
- des spams : <https://www.signal-spam.fr/>
- des sites de phishing : <http://www.phishing-initiative.com/>

# INTERNET EN TOUTE SÉCURITÉ

# LES PRINCIPAUX DANGERS D'INTERNET

## L'HAMEÇONNAGE :

Vous pensez recevoir un courriel d'une société ou d'une administration notoirement connue (banque, opérateur téléphonique, impôt, caisse d'allocations familiales...) qui vous invite à fournir des informations confidentielles (code d'accès, n° de carte bancaire...). Les pirates récupèrent alors ces données et les utilisent à leur profit.

## LES LOGICIELS MALVEILLANTS

Lorsque vous ouvrez un mail ou que vous accédez à un site web, votre ordinateur peut être infecté par un virus. Ce dernier permet alors d'intercepter vos données confidentielles (identifiants, codes secrets, n° de carte bancaire, cryptogramme visuel...).

## LES ESCROQUERIES

- ➔ Un courriel vous informe que vous avez gagné un cadeau mais on vous demande de payer des frais de livraison et de communiquer vos codes bancaires. Vous ne verrez jamais les cadeaux.
- ➔ Un courriel vous informe que vous avez gagné une somme importante à la loterie mais que vous devez envoyer de l'argent par mandat international pour les frais de transfert (Western Union par exemple). Vous ne verrez jamais la somme promise.
- ➔ Un courriel vous informe qu'une personne a besoin de votre aide (maladie, handicap, problèmes financiers), elle vous demande de lui envoyer de l'argent à l'étranger par mandat international.



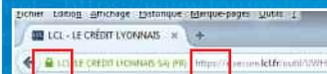
# POUR VOTRE SÉCURITÉ



- ➔ Installez un logiciel anti-virus, un logiciel anti-espion et un pare-feu régulièrement mis à jour.

PROTÉGER  
VOTRE  
ORDINATEUR

- ➔ Réalisez vos achats uniquement sur les sites de confiance dont l'adresse, au moment de la transaction, commence par «https».



- ➔ L'apparition d'icônes en bas du navigateur (cadenas et clés) est un gage de sécurité.

SÉCURISER  
VOS ACHATS  
EN LIGNE

- ➔ Méfiez-vous des gains trop faciles, des cadeaux, des bonnes affaires et des demandes d'argent faisant appel à votre compassion.

- ➔ Méfiez-vous des demandes urgentes d'informations personnelles, surtout lorsqu'elles contiennent des fautes d'orthographe.

- ➔ N'ouvrez pas les courriels si vous avez des doutes sur leur provenance.

- ➔ Ne cliquez pas sur les liens reçus par courriel surtout si on vous demande vos coordonnées bancaires.