Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PRÉFET DU CHER

escroquerie
SCAM
nigériane
pishing
web
vishing
SPAM
internet
arnaques
anti-virus
https://
préjudices
pare-feu

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

DES CONSEILS POUR SE PROTEGER

PROTECTION DE SON ORDINATEUR

- Utiliser un anti-virus régulièrement mis à jour
- Activer le pare-feu de window (ou autre)

ACHAT EN LIGNE

- Se méfier des offres trop alléchantes
- Ne conclure aucun achat important sans rencontrer le vendeur, ni avoir vu ou essayé le bien dans le cas d'une voiture par exemple
- Privilégier des sites connus (solutions de paiement en ligne) avant d'effectuer un transfert de fonds ou un virement bancaire à l'étranger
- Vérifier la présence du «s» dans l'adresse https:// et la présence d'un cadenas en bas ou en haut de la page sécurisée
- Vérifier son «panier» et le prix du produit avant de confimer ses achats

ESCROQUERIE DITE « NIGÉRIANE » OU SCAM

Vous recevez un mail d'un richissime étranger. Il dit avoir besoin de votre aide pour récupérer sa fortune bloquée à l'étranger.
Objectif ? Vous amener à verser de l'argent (parfois des centaines de milliers d'euros) pour payer des frais de dossiers imaginaires en vous faisant miroiter une partie du pactole.

Comment faire ?

Ne répondez en aucun cas à ces messages et détruire directement ce mail.

Comment s'en prémunir ?

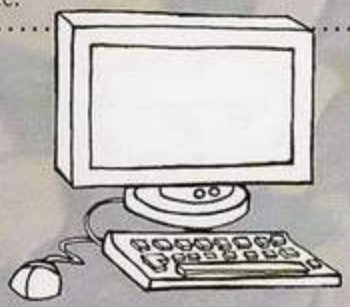
Ne vous fiez jamais aux propositions mirobolantes d'une personne inconnue, classez l'expéditeur en indésirable pour ne plus recevoir ses mails.

LE VISHING

« L' hammeçonnage vocal » est l'utilisation de la technologie via un message pré-enregistré dans le but de duper quelqu'un en lui faisant divulguer de l'information personnelle ou ses identifiants bancaires.

Comment s'en prémunir ?

Si un message vous demande de rappeler tel numéro, ne le composez pas. Aucune banque ne demande de renseignements par courriers électroniques ou téléphone. Dans le doute, contactez votre banque.



ESCROQUERIE PAR CARTE BANCAIRE

A savoir

Depuis la loi « sécurité quotidienne » du 15 novembre 2001, la responsabilité du titulaire d'une carte de crédit n'est pas engagée si la carte a été contrefaite ou si le paiement contesté a été effectué frauduleusement, à distance, sans utilisation physique de la carte.

Comment faire ?

Avertissez votre banque et signifiez lui que vous vous opposez formellement au paiement de l'opération en question.

Comment s'en prémunir ?

- Ne pas laisser traîner votre carte bancaire à la vue d'autres personnes, ni la laisser dans votre voiture ou tout autre lieu sans protection
- Après chaque achat, penser à reprendre votre carte bancaire
- Ne jeter pas vos tickets de caisse sans les détruire totalement, votre numéro de carte bancaire y figure
- Ne jamais communiquer votre numéro de carte bancaire à une tierce personne
- Ne pas laisser le numéro de code secret avec votre carte bancaire
- Votre carte bancaire doit porter votre signature au dos

LE PISHING

Le pishing est une technique frauduleuse utilisée par les pirates informatiques pour récupérer des informations (généralement bancaires) auprès d'internautes via un site web factice copie conforme du site original.

Comment s'en prémunir ?

- Ne cliquez pas directement sur le lien contenu dans le mail, mais saisissez vous-même l'adresse URL d'accès au service
- Assurez-vous que le navigateur est en mode sécurisé, c'est-à-dire que l'adresse dans la barre du navigateur commence par **https** et qu'un petit cadenas est affiché dans la barre d'état au bas de votre navigateur.

LE SPAM

Envoi massif de « Courriers électroniques indésirables » Ces courriers sont pour la plupart des messages de type publicitaire.

Comment s'en prémunir ?

- Il ne faut jamais répondre à ce type de message car cela indique à l'expéditeur que l'adresse électronique est valide
- Il est conseillé d'utiliser des logiciels permettant de supprimer automatiquement des messages.

De plus amples informations sont disponibles sur le site **www.signal-spam.fr**

SI VOUS ÊTES VICTIME, PORTEZ PLAINTE

Si vous êtes victime d'une escroquerie sur Internet, déposez plainte au commissariat ou à la gendarmerie la plus proche

Munissez-vous de tous les renseignements permettant d'identifier l'escroc :

- Références du transfert d'argent effectué
- Références de la ou les personnes contactées (adresse de messagerie, pseudo, copie des courriels...)

Gendarmerie nationale

POLICE NATIONALE

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