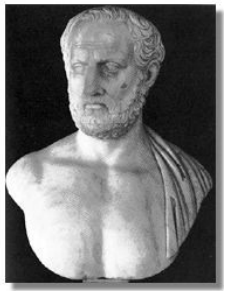
Adopter les principes simples proposés dans cette brochure réduira sensiblement les risques de captation de vos données confidentielles de carte bancaire

Soyez conscient que les dispositifs de

sécurité les plus exigeants ne remplaceront jamais votre volonté de vous prémunir des risques



Thucydide, l'auteur de la Guerre du Péloponnèse (Vème siècle av JC)

"L'épaisseur d'un rempart compte moins que la volonté de le défendre."

Cachet du service chargé de la diffusion

internet-signalement.gouv.fr

Portail officiel de signalement des contenus illicites de l'Internet

Numéros et adresses utiles :

Carte bancaire perdue ou volée - utilisation frauduleuse de données bancaires

Le plus simple et le plus rapide est d'appeler le numéro spécial du serveur interbancaire ☏ 0 892 705 705
Vous trouverez aussi le numéro de téléphone à appeler à côté des distributeurs de billets, et il est en général également indiqué au dos des tickets de retrait.
A l'étranger vous pouvez faire opposition en appelant le numéro figurant sur les distributeurs des réseaux Visa et Eurocard Mastercard

Les informations à fournir :

Lorsque vous contacterez le service concerné, il vous sera demandé le numéro à 16 chiffres de votre carte et sa date d'expiration, car cela facilitera la recherche et permettra d'accélérer l'opposition. Par prudence, vous avez donc intérêt à noter ces informations sur un document conservé en sécurité, évidemment pas au même endroit que la carte, et facilement accessible en cas de perte ou vol de votre carte. Le centre de mise en opposition vous communiquera en principe un numéro d'enregistrement à conserver. (Source : Fédération bancaire française)

Signaler un site illicite : **Signaler >>**

vous pouvez transmettre des signalements de contenus ou de comportements illicites auxquels vous vous seriez retrouvés confrontés au cours de votre utilisation d'Internet

https://www.internet-signalement.gouv.fr/PortailWeb
http://www.interieur.gouv.fr/
http://www.clusif.asso.fr/
http://www.cartes-bancaires.com/
http://www.phishing.fr/
http://www.secuser.com/phishing/index.htm

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

FICHES PRATIQUES

Préfecture de l' EURE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTERE DE L'INTERIEUR, DE L'OUTRE-MER ET DES COLLECTIVITES TERRITORIALES

FRAUDES A LA CARTE BANCAIRE

Gendarmerie nationale

MINISTÈRE DU BUDGET DES COMPTES PUBLICS ET DE LA RÉFORME DE L'ÉTAT

POLICE NATIONALE

Escroqueries

La forte hausse des escroqueries via Internet, qui représentent aujourd'hui une escroquerie sur deux, nécessite une particulière vigilance de votre part. Le développement accéléré du commerce en ligne pose la question de la parade à adopter face aux escrocs. Les pièges peuvent être évités à condition d'avoir à l'esprit quelques mesures de précaution élémentaires.

Zoom sur quelques escroqueries

<u>à son domicile</u> :

- Monsieur X reçoit un mail à l'en-tête très officiel de la direction des impôts l'informant d'un trop perçu de l'administration qui lui propose un remboursement.

- Il est dirigé sur un site où il communique ses références bancaires ou le n° de sa carte de crédit.
- Malheureusement il s'agissait d'un site pirate.

- Le numéro de sa carte bancaire est revendu sur les réseaux illicites et Monsieur X se voit débiter des sommes importantes sur son compte bancaire.

<u>Exemple :</u>

- Madame *X* reçoit sur sa boîte E-mail, le message d'un ami indiquant qu'il se trouve dans un pays étranger, qu'il a été victime du vol de ses documents et de son argent et demande qu'on lui transmette par mandat cash du numéraire.
- Madame *X* contacte par téléphone son ami qui, en réalité, ne se trouve pas à l'étranger et qui n'est pas à l'origine de l'E-mail.

- Madame *X* est victime d'une tentative d'escroquerie, son ami s'est en fait fait pirater sa boîte E-mail.

* * *

- Monsieur *X*, désirant acquérir un véhicule, se rend sur un site de vente de voitures d'occasion. Il trouve une offre intéressante et contacte le vendeur par E-mail.

- Le vendeur lui demande un acompte via mandat cash pour assurer la réservation du véhicule.

- Monsieur X envoie le mandat mais n'est jamais livré.

- Monsieur X est victime d'une escroquerie, l'annonce étant totalement fausse.

***<u>au distributeur automatique de billets</u>* :**

le collet marseillais

-Madame X insère sa carte bancaire dans le D.A.B pour effectuer un retrait d'argent.

- Elle aperçoit une affichette indiquant que l'appareil est momentanément hors service et qu'elle doit composer son code secret pour récupérer sa carte.

-Un individu arrive derrière Madame X et lui confirme l'opération à effectuer.

-Madame X s'exécute et compose le code mais elle ne parvient pas à récupérer sa carte. L'agence bancaire étant fermée, elle quitte les lieux.

- Après le départ de Madame X, l'individu récupère la carte à l'aide d'une fine pince.

- Le lendemain, Madame X constate que des retraits ont été effectués la veille avec sa carte bancaire.

<u>Concernant sa carte bancaire</u> :

- Ne jamais confier sa carte bancaire.
- Ne jamais laisser son code confidentiel et sa carte ensemble.
- Ne pas quitter sa carte bancaire des yeux.
- Bien faire attention aux regards indiscrets qui essayent de voir le code secret de la carte (*a fortiori* si la carte est restée bloquée dans le D.A.B)..
- Ne jamais laisser traîner sa carte bancaire à la vue de tous (meuble d'entrée, buffet de salle ...).
- S'assurer que le lecteur de carte (distributeur de billets ...) n'est pas modifié.
- Ne pas se laisser distraire lors d'un retrait au distributeur.

Il est rappelé que les administrations ne demandent jamais le numéro de la carte bancaire. Restez vigilants.

<u>Concernant l'utilisation de sa carte bancaire sur internet</u> :

- Effectuer des commandes de préférence sur des sites dont l'enseigne est connue.
- Vérifier que vous disposez bien de l'adresse postale complète du commerçant.
- Eviter de payer directement par virement ou mandat (notamment sur les sites d'enchères).
- Conserver toujours une copie de votre commande et des principaux points de contrat.
- Ne jamais suivre le lien d'un site dans un E-mail, faire la recherche soit même.
- Sur les sites de paiement, s'assurer qu'il s'agit bien d'un site sécurisé.

1. Connectez vous en tapant l'adresse de votre organisme bancaire ou financier dans votre navigateur (www.nom-de-votre-banque.com) et enregistrer le lien dans vos favoris.

2. Ne passez jamais par un moteur de recherche comme Google pour localiser votre banque car les hackers peuvent parfois faire apparaitre leur faux site dans les résultats de Google.

3. Dans le doute, contacter l'expéditeur officiel du message en passant par le site officiel sur lequel vous avez l'habitude de vous connecter, pour déterminer s'il est bien l'expéditeur du message et s'il est effectivement nécessaire de réactiver un compte ou de procéder à une modification de données. Consulter la liste des principaux sites de phishing à l'adresse suivante : http://www.secuser.com/phishing/index.htm