

À savoir

Pour la sécurité de vos transactions, gardez secret le cryptogramme visuel (CVV) de votre carte bancaire. Cet identifiant est nécessaire pour réaliser des achats sur internet. Il ne vous sera jamais demandé par les forces de l'ordre ni par les établissements bancaires.



Recommandations

- ◆ Ne répondez jamais à un courriel vous demandant des informations personnelles ou vos numéros de carte bancaire, même s'il semble émis par un de vos fournisseurs (banque, téléphone, internet).
- ◆ Effectuez régulièrement des analyses antivirus et antispyware de vos ordinateurs personnels.
- ◆ Mettez régulièrement à jour vos antivirus, antispyware, navigateurs internet, systèmes d'exploitation en particulier et vos logiciels en général.
- ◆ Sauf si vous en avez absolument besoin, n'utilisez jamais d'ordinateur public pour faire un achat sur internet.
- ◆ Ne mentionnez jamais vos données personnelles ou vos numéros de carte bancaire dans un courriel, même envoyé à un proche.

Repérer les fraudes

- ◆ Regardez régulièrement vos relevés de compte pour vérifier les paiements qui y sont passés.
- ◆ Consultez très fréquemment la situation de votre compte sur l'espace personnel de votre site bancaire, qui permet une meilleure réactivité.



PERCEV@L

FRAUDE À LA CARTE BANCAIRE SUR INTERNET

Simplifier les démarches des victimes

Mieux prévenir les atteintes et identifier les auteurs

Signaler votre situation aux forces de l'ordre
directement sur service-public.fr
« fraude carte bancaire »



Quel type de fraude peut être signalé sur PERCEV@L ?

→ toutes transactions par carte bancaire sur internet dont **vous n'êtes pas à l'origine** alors que **vous êtes toujours en possession** de la carte ;

→ identifiables sur votre relevé d'opérations bancaires par la mention :

- soit du nom d'un e-commerçant ;
- soit du nom d'un prestataire de paiement en ligne par carte bancaire (en cas de doute, vérifier sur internet l'activité de la société mentionnée).

Que pouvez-vous faire ?

- prévenez votre banque pour provoquer l'opposition sur la carte (n°interbancaire d'opposition : **0 892 705 705** ouvert 7/7 et 24h/24 - numéro violet ou majoré; coût d'appel vers un numéro fixe + service payant, depuis un téléphone fixe ou mobile) ;
- **effectuez un signalement sur Internet grâce à la plateforme PERCEV@L**. Vous gardez le droit de déposer plainte ultérieurement ;
- demandez le remboursement de l'opération auprès de votre banque.

À quoi sert PERCEV@L ?

En utilisant le téléservice PERCEV@L, après avoir fait opposition, vous êtes guidé au travers d'une **démarche simple** de signalement aux forces de l'ordre sur internet, sans avoir à vous déplacer.

Votre signalement est **exploité exclusivement par les forces de l'ordre** en vue d'identifier les auteurs d'appropriations frauduleuses/recels de numéros de cartes bancaires.

Accéder à la plateforme :

Rendez-vous sur « service public » :
<https://www.service-public.fr> et saisissez « fraude carte bancaire » ou « Percev@l »

Pour réaliser votre démarche en ligne, munissez-vous :

- de votre carte bancaire (son numéro vous sera demandé) ;
- des relevés d'opérations bancaires sur lesquels figurent les achats frauduleux (les libellés et montants de ces achats vous seront demandés).

Et après ?

- pour faciliter la démarche de remboursement, vous pouvez présenter à votre banque le récépissé de signalement sur PERCEV@L ;
- vous pouvez obtenir le remboursement de l'opération frauduleuse indépendamment du signalement sur PERCEV@L (articles L133-18 et suivants du Code monétaire et financier) ;
- le traitement des signalements est opéré de manière confidentielle et sous la responsabilité de la Gendarmerie nationale ;
- les informations fournies sont rassemblées et analysées par des officiers de police judiciaire ;
- vous êtes susceptible d'être contacté par la Police ou la Gendarmerie nationale si les faits entrent dans le cadre d'une enquête.