



LA FRAUDE À LA CARTE BANCAIRE



EN BREF

QU'EST-CE QUE C'EST ?

La fraude à la carte bancaire correspond à l'utilisation frauduleuse des coordonnées d'une carte bancaire sans que son titulaire ne l'ait perdue ou se soit fait voler physiquement la carte. L'origine de la fraude peut être difficile à déterminer, car les fraudeurs disposent de nombreux moyens pour obtenir ces informations : hameçonnage (phishing) incitant la victime à fournir ses coordonnées, piratage d'un compte en ligne où elles sont enregistrées, compromission d'un appareil informatique (ordinateur, téléphone...), exploitation d'une fuite de données d'un site Internet, piégeage de distributeur de billets, ou encore recueil des informations lors d'un paiement chez un commerçant malhonnête. Ces données volées permettent ensuite de réaliser des achats ou opérations frauduleuses, souvent en ligne, à l'insu du titulaire.

BUT RECHERCHÉ : Dérober les coordonnées bancaires de la victime pour en faire un usage frauduleux (achats en ligne, etc.).



Voici 6 bonnes pratiques à adopter si vous êtes victime

- 1 FAITES IMMÉDIATEMENT OPPOSITION À VOTRE CARTE BANCAIRE**
- 2 ALERTEZ VOTRE BANQUE AU PLUS VITE POUR EN DEMANDER LE REMBOURSEMENT**
- 3 DÉPOSEZ PLAINTÉ**
- 4 METTEZ À JOUR VOS ÉQUIPEMENTS**
- 5 RÉALISEZ UNE ANALYSE ANTIVIRALE COMPLÈTE (SCAN)**
- 6 ASSUREZ-VOUS QU'AUCUN DE VOS COMPTES EN LIGNE NE SOIT PIRATÉ**

► Voir détail page "6 BONNES PRATIQUES À ADOPTER"

Page 1/3





LA FRAUDE À LA CARTE BANCAIRE



6 BONNES PRATIQUES À ADOPTER

1. FAITES IMMÉDIATEMENT OPPOSITION À VOTRE CARTE BANCAIRE

Pour faire opposition à votre carte bancaire, vous pouvez : contacter immédiatement le numéro d'opposition de votre banque (disponible sur votre relevé ou sur son site Internet).

2. ALERTEZ VOTRE BANQUE AU PLUS VITE POUR EN DEMANDER LE REMBOURSEMENT

Dès l'identification d'un débit frauduleux sur votre compte bancaire, alertez votre banque au plus vite pour en demander le remboursement.

3. DÉPOSEZ PLAINTE

Déposez plainte au commissariat de police ou à la gendarmerie dont vous dépendez ou en écrivant au procureur de la République du tribunal judiciaire en fournissant toutes les preuves en votre possession.

4. METTEZ À JOUR VOS ÉQUIPEMENTS

Mettez à jour vos équipements pour corriger les failles de sécurité qu'aurait pu utiliser le fraudeur pour en prendre le contrôle.

5. RÉALISEZ UNE ANALYSE ANTIVIRALE COMPLÈTE (SCAN)

Réalisez une analyse antivirus complète (scan) de vos appareils pour supprimer les virus qui auraient pu être à l'origine de la fraude à la carte bancaire.

6. ASSUREZ-VOUS QU'AUCUN DE VOS COMPTES EN LIGNE NE SOIT PIRATÉ

Assurez-vous qu'aucun de vos comptes en ligne ne soit piraté. Au moindre doute, changez les mots de passe et activez la double authentification si disponible. Choisissez des mots de passe différents et complexes pour chacun de vos comptes.

EN FONCTION DU CAS D'ESPÈCE, LES INFRACTIONS SUIVANTES PEUVENT ÊTRE RETENUES :

1

- En cas d'utilisation frauduleuse de coordonnées de carte bancaire : l'escroquerie. L'article 313-1 du code pénal dispose que : « l'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge ». Ce délit est passible d'une peine d'emprisonnement de cinq ans et de 375 000 euros d'amende.



LA FRAUDE À LA CARTE BANCAIRE



COMMENT S'EN PROTÉGER ?

Ne communiquez jamais vos coordonnées bancaires :

par messagerie, par téléphone ou sur Internet.

Conservez précieusement votre carte bancaire et son code confidentiel :

ne le notez jamais sur un support accessible.

Vérifiez régulièrement votre compte bancaire :

pour identifier tout débit suspect.

N'enregistrez pas vos coordonnées bancaires pour des achats ponctuels :

et supprimez-les si vous ne les utilisez plus. Vérifiez la notoriété du site avant tout achat.

Privilégiez les moyens de paiement sécurisés :

comme l'e-Carte Bleue, Paylib, etc., et renseignez-vous auprès de votre banque sur les solutions disponibles.

Soyez vigilant aux demandes de validation inhabituelles :

elles peuvent viser à vous faire approuver des transactions frauduleuses.

N'ouvrez pas les messages suspects et ne cliquez pas sur les liens :

provenant d'expéditeurs inconnus ou dont le contenu est inhabituel.

Utilisez des mots de passe complexes et changez-les au moindre doute :

activez la double authentification lorsque c'est possible (voir fiche "Les mots de passe").

Mettez régulièrement à jour vos équipements et logiciels :

pour corriger d'éventuelles failles de sécurité.

Effectuez régulièrement une analyse antivirus complète :

après avoir vérifié que votre antivirus est à jour.

Évitez d'utiliser un ordinateur ou un réseau Wi-Fi publics :

car ils peuvent être contrôlés par un pirate.



EN FONCTION DU CAS D'ESPÈCE, LES INFRACTIONS SUIVANTES PEUVENT ÊTRE RETENUES :

2

- En cas de piratage d'un système informatique (ordinateur, téléphone mobile, tablette...) : l'infraction d'atteinte à un système de traitement automatisé de données (STAD) peut être retenue. Les articles 323-1 à 323-7 du code pénal disposent notamment que : « le fait d'accéder ou de se maintenir frauduleusement » dans un STAD, « la suppression ou la modification de données contenues dans le système », « le fait [...] d'extraire, de détenir, de reproduire, de transmettre [...] les données qu'il contient » ou l'« altération du fonctionnement de ce système » sont passibles de trois à cinq ans d'emprisonnement et de 100 000 à 150 000 euros d'amende.
- Dans le cas de la fabrication d'une carte bancaire contrefaite : l'infraction de faux et usage d'une contrefaçon d'un moyen de paiement peut être retenue. L'article 163-3 du Code monétaire et financier dispose que : « Est puni d'un emprisonnement de cinq ans et d'une amende de 375 000 euros le fait pour toute personne : 1. De contrefaire ou de falsifier un chèque ou un autre instrument mentionné à l'article L. 133-4 ; 2. De faire ou de tenter de faire usage, en connaissance de cause, d'un chèque ou un autre instrument mentionné à l'article L. 133-4 contrefaisant ou falsifié ; 3. D'accepter, en connaissance de cause, de recevoir un paiement au moyen d'un chèque ou d'un autre instrument mentionné à l'article L. 133-4 contrefaisant ou falsifié. »