DIRECTION DU RENSEIGNEMENT ET DE LA SÉCURITÉ DE LA DÉFENSE

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

FLASH INFO*

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

cybermalveillance.gouv.fr

n° 3, la fraude à la carte bancaire

Vous constatez un débit de carte bancaire sur vos comptes que vous êtes certain de ne pas avoir réalisé ! Comme au moins 1,4 millions de personnes chaque année, vous êtes peut-être victime d'une fraude à la carte bancaire. De quoi s'agit-il et comment s'en prémunir ?

Qu'est-ce que la fraude à la carte bancaire ?

La fraude à la carte bancaire désigne l'**utilisation frauduleuse des coordonnées de la carte bancaire d'une personne** pour réaliser des transactions financières à son insu.

Trouver **l'origine précise d'une telle fraude** est souvent difficile. En effet, pour obtenir les coordonnées de la carte bancaire de la victime, le fraudeur peut utiliser de nombreuses méthodes classées ci-dessous par fréquence d'occurrence :

- l'**hameçonnage** (*phishing* en anglais) à travers un message frauduleux (courriel ou SMS) incitant la victime à fournir ses coordonnées de carte ;
- le **piratage d'un compte** en ligne de la victime sur lequel les coordonnées de la carte seraient inscrites (commerce en ligne, réseaux sociaux…) ;
- le **piratage d'un équipement** informatique de la victime (ordinateur, téléphone, tablette…) ;
- l'utilisation d'une **fuite de données** d'un site en ligne sur lequel la victime aurait laissé les coordonnées de sa carte ;
- le **piégeage d'un distributeur** de billets visant à copier les cartes ;
- lors d'un **paiement chez un commerçant malhonnête** qui aurait pu photographier votre carte.

Dans la très grande majorité des cas, **c'est en examinant leurs relevés de compte que les victimes découvrent des transactions frauduleuses** sur leur carte bancaire, qu'elles sont certaines de ne pas avoir réalisées.

Aujourd'hui **les cybercriminels fonctionnent en réseau et se revendent les numéros de cartes bancaires dérobées** pour pouvoir les utiliser au détriment de leur détenteur légitime tant qu'elles n'ont pas été mises en opposition.

DIRECTION DU RENSEIGNEMENT ET DE LA SÉCURITÉ DE LA DÉFENSE

Selon l'observatoire de la sécurité des moyens de paiement de la Banque de France, **le montant déclaré des fraudes à la carte bancaire s'élève à 473 millions d'euros et touche 1,4 millions de personnes par an pour un préjudice moyen de 63€.**

Ce montant relativement faible de préjudice est un moyen pour les cybercriminels de rendre difficilement détectables leurs transactions frauduleuses par les banques ou par les victimes qui n'examinent pas régulièrement et avec attention leurs relevés d'opérations bancaires.

Il n'est ainsi pas rare de voir des personnes se rendre compte a posteriori qu'elles ont été victimes de prélèvements de carte bancaire frauduleux durant plusieurs mois avant qu'elles ne s'en aperçoivent.

Comment se protéger d'une fraude à la carte bancaire ?

Conservez le contrôle de votre carte bancaire : ne la perdez jamais des yeux quand vous faites un paiement.

N'enregistrez pas vos coordonnées de carte bancaires sur les sites Internet pour des achats ponctuels et supprimez-les si vous n'utilisez plus ces sites.

Vérifiez la notoriété des sites Internet avant de réaliser un achat (recherche sur Internet ou prise en compte d'avis par exemple) et au moindre doute ne donnez pas vos coordonnées de carte bancaire.

Privilégiez les moyens de paiement sécurisés ou à usage unique (e-Carte Bleue, Paylib, etc.). Contactez votre banque pour connaître les solutions qu'elle propose.

Soyez vigilant en cas de demande de code de validation d'achat que vous n'auriez pas réalisé. Celles-ci prennent souvent la forme de numéro à communiquer et qui pourraient vous amener à valider des transactions dont vous n'êtes pas à l'origine.

N'ouvrez pas les messages suspects et/ou leurs pièces jointes et ne cliquez par sur les liens provenant de chaînes de messages, d'expéditeurs inconnus ou d'un expéditeur connu mais dont le contenu du message est inhabituel ou vide.

Utilisez des mots de passe différents et complexes pour chaque compte ou service utilisé et changez-les au moindre doute. Activez la double authentification si

Qu'est-ce que la double authentification ?

Appelée également authentification multifacteurs, à deux facteurs ou encore 2FA… Il s'agit d'un procédé qui, en plus de votre nom de compte et de votre mot de passe, vous demande une confirmation pour autoriser la connexion. Cette confirmation peut prendre la forme d'un code temporaire reçu par SMS ou courriel, ou généré via une application ou une clé spécifique ou encore par reconnaissance biométrique. Cette option permet de confirmer que vous autorisez bien la connexion aux comptes protégés. Bien que non activée par défaut, la majorité des services de messagerie et de réseaux sociaux propose cette option, ainsi que de plus en plus de services de commerce en ligne.

disponible. Celle-ci permet de vous envoyer une demande de confirmation en cas de détection d'une connexion inconnue.

Mettez régulièrement à jour vos appareils ainsi que les logiciels et applications qui y sont installés afin de corriger leurs failles de sécurité.

Faites régulièrement une analyse antivirale complète (scan) de vos appareils après avoir vérifié que leur antivirus fonctionne et est à jour.

Évitez de vous connecter à vos comptes depuis un ordinateur en libre-service ou à un réseau Wi-Fi public. Ces équipement et services non maîtrisés peuvent être contrôlés par des cybercriminels qui pourraient intercepter vos mots de passe et/ou coordonnées de carte bancaire.

Vérifiez régulièrement votre compte bancaire pour identifier tout débit suspect. Effacer le trigramme se trouvant au dos de la carte bleue est également une solution simple et pragmatique qui ne remet toutefois pas en cause les recommandations évoquées supra.

Comment réagir face à une fraude à la carte bancaire ?

Faites immédiatement opposition à votre carte bancaire en cas de fraude en contactant le numéro fourni par votre banque ou via le service interbancaire d'opposition à carte bancaire 0 892 705 705 (ouvert 7 jours/7 et 24h/24), numéro surtaxé 0,34 € TTC/min.

Alertez votre banque et demandez le remboursement des sommes prélevées : si vous n'avez pas donné votre code et que vous n'avez commis aucune négligence, vous êtes en droit de contester tout paiement par carte bancaire et votre banque est tenue de vous rembourser.

Signalez la fraude bancaire sur la plateforme Perceval du ministère de l'intérieur et ce, même si votre banque vous rembourse afin de faire connaître les faits aux autorités. À noter que certaines banques demandent un récépissé Perceval ou un dépôt de plainte pour enclencher l'étude du remboursement.

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

Informez votre officier de sécurité pour tout usage frauduleux qui pourrait être en lien avec un déplacement professionnel.

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.

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

DIRECTION DU RENSEIGNEMENT ET DE LA SÉCURITÉ DE LA DÉFENSE

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

Pour plus de conseils dans vos démarches, contactez la plateforme Info Escroqueries du ministère de l'Intérieur au 0 805 805 817 (appel et service gratuits de 9h à 18h30 du lundi au vendredi).

Pour en savoir plus

Fiche réflexe sur la fraude à la carte bancaire de Cybermalveillance.gouv.fr : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/fraude-carte-bancaire

Signaler une fraude à la carte bancaire sur le service Perceval du ministère de l'intérieur : https://www.service-public.fr/particuliers/vosdroits/R46526

Rapport annuel de l'Observatoire de la sécurité des moyens de paiement 2020 : https://www.banque-france.fr/rapport-annuel-de-lobservatoire-de-la-securite-des-moyens-de-paiement-2020

Que faire en cas de perte ou de vol de sa carte bancaire avec Service-public.fr : https://www.service-public.fr/particuliers/vosdroits/F31241

A propos de Cybermalveillance.gouv.fr

Cybermalveillance.gouv.fr est la plateforme du dispositif national de prévention et d'assistance aux victimes de cybermalveillance au profit des particuliers, des entreprises, des associations et des collectivités. Elle propose gratuitement de nombreuses ressources de sensibilisation et des services d'assistance en ligne.

Le ministère des Armées est membre depuis 2020 du GIP ACYMA, qui opère la plateforme Cybermalveillance.gouv.fr, et lui apporte son soutien dans sa mission d'intérêt public.