RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

COMPRENDRE LES RISQUES

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 à son insu alors que celle-ci est pourtant toujours en possession de sa carte. 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 comme l'hameçonnage (***phishing*** en anglais) à travers un message incitant la victime à fournir ses coordonnées, 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…), 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 ou même lors d'un paiement chez un commerçant malhonnête qui aurait pu photographier la carte.

BUT RECHERCHÉ

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

SI VOUS ÊTES VICTIME

FAITES IMMÉDIATEMENT OPPOSITION À VOTRE CARTE BANCAIRE en cas de fraude.

Dès l'identification d'un débit frauduleux sur votre compte bancaire, **ALERTEZ VOTRE BANQUE AU PLUS VITE POUR EN DEMANDER LE REMBOURSEMENT.**

SIGNALEZ LA FRAUDE BANCAIRE AUPRÈS DE LA PLATEFORME PERCEVAL du ministère de l'Intérieur.

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.

METTEZ À JOUR VOS ÉQUIPEMENTS pour corriger les failles de sécurité qu'aurait pu utiliser le fraudeur pour en prendre le contrôle.

RÉALISEZ UNE ANALYSE ANTIVIRALE COMPLÈTE (SCAN) de vos appareils pour supprimer les virus qui auraient pu être à l'origine de la fraude à la carte bancaire.

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.

MESURES PRÉVENTIVES

Ne communiquez jamais vos coordonnées bancaires par messagerie, par téléphone ou sur Internet.

Conservez précieusement votre carte bancaire et son code confidentiel.

Vérifiez régulièrement votre compte bancaire pour identifier tout débit suspect.

Pour des achats ponctuels sur un site Internet, **n'enregistrez pas vos coordonnées bancaires** et supprimez-les si vous ne l'utilisez plus. Vérifiez également la notoriété du site Internet avant de réaliser un achat (recherche sur Internet ou d'avis par exemple).

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

Si vous n'avez pas réalisé d'achat, **soyez vigilant aux demandes de validation** qui prennent souvent la forme de numéro à communiquer et qui pourraient vous amener à valider des transactions dont vous n'êtes pas l'auteur.

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

Utilisez des mots de passe suffisamment complexes et changez-les au moindre doute (tous nos conseils pour gérer vos mots de passe). **Activez la double authentification** si disponible.

Mettez régulièrement à jour votre appareil, votre système d'exploitation ainsi que les logiciels et applications installés.

Après avoir vérifié que votre antivirus est en état de fonctionnement et à jour, **faites régulièrement une analyse antivirale complète (scan)** de votre appareil et supprimez les virus.

Évitez de vous connecter à un ordinateur ou à un réseau Wi-Fi publics. Non maîtrisés, ils peuvent être contrôlés par un pirate

EN PARTENARIAT AVEC:
MINISTÈRE DE L'INTÉRIEUR
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

LES **INFRACTIONS**

En fonction du cas d'espèce, les infractions suivantes peuvent être retenues :

- 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.

- 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.* »

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

V230417