Vol de coordonnées bancaires : des manoeuvres simples et quasi-invisibles

«En consultant mon relevé de compte, j'ai découvert que des opérations avaient été réalisées à mon insu avec les références de ma carte bancaire».

Protection des coordonnées bancaires : les règles de vigilance

❶ Sur Internet

- Je réalise mes achats uniquement sur les sites de confiance, signalés par le logo et dont l'adresse commence, au moment de la transaction, par «https»
- J'évite le piratage de ma carte bancaire en protégeant mon ordinateur avec un anti-virus, un pare-feu et un logiciel anti-espion à jour

❷ Les automates (distributeurs de billets)

- Je compose discrètement mon code et masque le clavier avec ma main
- Je ne me laisse pas distraire par des inconnus qui proposent leur «aide» ; il s'agit souvent d'escrocs qui cherchent à subtiliser ma carte et récupérer mon code secret.

❸ En magasins

- Numéro de carte bancaire + date d'expiration + cryptogramme = danger !
  Dans le cadre d'une transaction en magasin, il est très facile pour l'escroc d'identifier ces numéros et de les noter. Ces références sont suffisantes pour effectuer des achats en ligne.
- Je ne quitte jamais des yeux ma carte bancaire, je ne la confie à personne
- Je ne conserve pas mon code secret au même endroit que la carte

❹ De manière générale, je suis les conseils de mon banquier

L'ESCROQUERIE : CE QUE DIT LA LOI

Extraits

Article L313-1 du Code Pénal

«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. L'escroquerie est punie de cinq ans d'emprisonnement et de 375 000 euros d'amende».

Si vous êtes victime, portez plainte

Si vous êtes victime d'une escroquerie, déposez plainte au commissariat ou à la gendarmerie la plus proche.

Munissez-vous de tous les renseignements en votre possession :

- **références du ou des transferts d'argent effectués,**
- **références de la ou des personnes contactées : adresse de messagerie ou postale, pseudos utilisés, numéros de téléphone, fax, copie des courriels/ courriers échangés...,**
- **tout autre renseignement pouvant aider à l'identification de l'escroc.**

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

POUR TOUT RENSEIGNEMENT
0811 02 02 17
COÛT D'UN APPEL LOCAL

POUR SIGNALER UN COURRIEL OU UN SITE INTERNET D'ESCROQUERIES
www.internet-signalement.gouv.fr

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

ESCROQUERIES
N'EN PAYEZ PAS LE PRIX

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

POUR SIGNALER UN COURRIEL OU UN SITE INTERNET D'ESCROQUERIES
www.internet-signalement.gouv.fr

ESCROQUERIES
N'EN PAYEZ PAS
LE PRIX

ZOOM SUR QUELQUES ESCROQUERIES

«Faites un virement pour acheter ce produit sur internet, c'est plus simple»

Escroqueries sur Internet : Transactions virtuelles, pertes bien réelles

«J'ai déniché une annonce proposant une voiture à un prix très attractif. Après plusieurs échanges avec le vendeur, j'ai reçu un courriel au nom du site définissant les modalités de paiement. Je ne me suis pas méfié et j'ai réglé le bien en passant par un service de transfert d'argent. En fait, c'est le vendeur escroc qui avait envoyé ce courriel ! L'argent a été retiré le jour même. Je n'ai jamais reçu le bien que j'avais payé».

- **Si je vends ou achète un bien très onéreux, j'organise une rencontre avant la transaction**
- **Si je vends un bien, j'attends d'avoir reçu matériellement l'argent avant de le livrer**

« Je suis policier, gendarme, pompier : aidez nous financièrement »

Fausse qualité : l'escroc était bien caché

«Je suis commerçant et j'ai reçu un appel d'un homme se disant commissaire de Police de ma ville. Il m'a invité à financer le petit journal du commissariat en y achetant un encart publicitaire pour la promotion de mon commerce. J'ai accepté. J'ai ensuite reçu par fax le bon de commande indiquant la somme à payer. Rassuré par la présence du logo de la Police, j'ai envoyé un chèque. Sans nouvelles quelques semaines plus tard j'ai contacté mon commissariat : j'ai appris qu'il n'existait aucun journal ! Résultat : pensant aider le commissariat j'ai enrichi un escroc et j'ai perdu beaucoup d'argent».

- **Avant de payer quoi que ce soit, je contacte le service concerné pour me renseigner**
- **Je vérifie toujours la qualité déclarée de mon interlocuteur**

«Une valise d'argent pour si peu : la belle affaire ! »

L'escroquerie aux billets noircis

«Dans un bar, une personne m'a accosté pour me proposer une affaire très intéressante. Elle disposait d'une mallette pleine de billets tachés d'encre noire. Elle m'a montré, avec un peu de produit, comment les traiter et de vrais billets sont apparus, dont elle m'a fait cadeau. Elle m'a proposé la moitié des billets de la mallette à condition d'avancer l'argent pour acheter le produit, trop cher pour elle seule. Convaincu, j'ai accepté. J'ai donc versé une première somme d'argent pour acheter à l'étranger ce produit nettoyant, puis une seconde pour débloquer le produit à la douane. Quatre versements plus tard, je me suis rendu compte de l'escroquerie dont j'avais été victime».

- **Billets tachés, maculés → je dois me méfier**
- **L'appât du gain ne doit pas me détourner du bon sens**

«Je suis votre banque et j'ai besoin de votre mot de passe de connexion»

«Phishing» : un mail ça peut faire très mal

«J'ai reçu un courriel de ma banque me demandant mon identifiant de connexion et le mot de passe de consultation de mon compte en ligne. Ils m'avaient alors expliqué qu'ils avaient besoin de mettre à jour mes données de connexion. Le problème c'est que ce n'était pas ma banque. Mon compte a été vidé».

- **Je ne réponds jamais à un courriel qui me demande de transmettre mes coordonnées bancaires ; je sais que ma banque ou toute autre institution de confiance ne me les demandera jamais par courriel**
- **En cas de doute, j'appelle directement ma banque**

« Un placement à taux rémunérateur record !»

Une fausse épargne qui vous ruine

«J'ai reçu les confidences d'une connaissance qui m'a dit avoir trouvé la solution pour arrondir facilement ses fins de mois : une de ses collègues de travail lui a proposé un placement très rémunérateur : 10 % par mois. Elle m'a dit qu'il faudrait placer 5000 euros. Après avoir un peu hésité, j'ai décidé d'investir 1000 euros, et elle m'a effectivement remis, après 30 jours, la somme de 1100 euros. Confiante, j'ai décidé de lui confier toutes mes économies, que je n'ai jamais revues».

- **Je sais que les trop bonnes affaires n'existent pas**
- **Je ne confie pas d'argent à un inconnu**

«Bravo, vous avez gagné le gros lot !»

L'escroquerie à la fausse loterie

«J'ai été avisé par courrier que j'avais gagné une grosse somme d'argent à un jeu. Mais avant, j'ai dû verser une somme afin de récupérer le gain. J'ai versé l'argent mais je n'ai jamais rien reçu !»

- **Je ne réponds jamais à ce type de proposition**
- **Si je n'ai pas joué, j'ai peu de chance d'avoir gagné**

«Aidez-moi à toucher mon héritage, vous ne le regretterez pas»

L'escroquerie à l'héritage

«J'ai reçu un courriel d'un inconnu qui m'a proposé de servir d'intermédiaire financier. Il se disait bénéficiaire d'un héritage conséquent qu'il ne pouvait toucher, faute de moyens suffisants pour avancer les frais de succession. Il m'a demandé de lui avancer la somme et proposé de toucher en retour 20% de l'héritage. Je lui ai envoyé l'avance par virement bancaire. Une fois les versements effectués, le contact a été rompu. Je n'ai jamais reçu la commission promise».

- **Je n'envoie pas d'argent à un inconnu via un service de transfert d'argent ou par virements bancaires**
- **Je ne réponds jamais à ce type de proposition**