JANVIER 2021

HORS-SÉRIE

LES
MINI-GUIDES
BANCAIRES

Fraudes aux opérations bancaires

Comment réagir ? Dans quels cas puis-je être remboursé ?

www.lesclesdelabanque.com

Le site pédagogique sur la banque et l'argent

FÉDÉRATION
BANCAIRE
FRANÇAISE

les clés de la banque

CE GUIDE VOUS EST OFFERT PAR

Pour toute information complémentaire, nous contacter : info@lesclesdelabanque.com

Éditeur : FBF - 18 rue La Fayette 75009 Paris - Association Loi 1901
Directeur de publication : Maya Atig
Imprimeur : Concept graphique,
ZI Delaunay Belleville - 9 rue de la Poterie - 93207 Saint-Denis
Dépôt légal : Janvier 2021

SOMMAIRE

Introduction **2**

Informations et recommandations générales **3**
Comment se prémunir contre les fraudes ? 3
Comment réagir aux fraudes et tentatives ? 4
Comment être remboursé en cas de fraude ? 5

Panorama par moyen de paiement / opération **6**
La carte 6
Le chèque 11
Le virement 14
Le prélèvement 16
L'accès à sa banque et les opérations à distance 17

Annexe 1 – **Tableau récapitulatif** **20**

Annexe 2 - **Quelques pièges types à (re)connaître** **24**
1. La fraude aux coordonnées bancaires 25
2. Le chantage à la webcam 26
3. Le ransomware 27
4. Le faux prêt 28
5. La fraude aux faux tests techniques 29
6. La fraude aux sentiments 30
7. Les arnaques sur les réseaux sociaux 31
8. La fraude aux offres d'emploi 33
9. La fraude à la loterie 34
10. Etre payé par un autre moyen de paiement que celui prévu 35
11. L'acquéreur trop généreux 36
12. Etre recruté comme mule 37

INTRODUCTION

Les opérations bancaires nécessitent un degré élevé de sécurité, qu'elles soient initiées en agence, par téléphone ou Internet. Les banques ont mis en place des systèmes de protection qu'elles renforcent sans cesse pour faire face aux nouvelles tentatives de fraudes.

Ainsi, pour toutes les opérations à distance, se met progressivement en place ce qu'on appelle « l'authentification forte du client » ou « double authentification ». Celle-ci vise notamment à renforcer leur niveau de sécurité et mieux protéger les utilisateurs de services de paiement (consommateurs, entreprises, professionnels) lorsqu'ils accèdent à leur espace de banque à distance et initient des opérations de paiement électronique.

Après quelques informations générales, ce guide propose un panorama des principaux types de fraudes, les réflexes à adopter lorsque vous pensez en être victime et les modalités de remboursement s'il y a lieu.

INFORMATIONS ET RECOMMANDATIONS GÉNÉRALES

Vous êtes responsable de l'utilisation que vous faites des services bancaires et de paiement mis à votre disposition. La prévention et la réaction sont déterminantes pour lutter efficacement contre les fraudes et tentatives.

Comment se prémunir contre les fraudes ?

En tant que client de la banque, votre rôle est essentiel dans l'utilisation sécurisée de vos moyens de paiement et des services de la banque à distance. Comme avec vos papiers d'identité ou vos clés, vous devez **faire attention à vos données bancaires personnelles**. En les protégeant, vous vous protégez.

Consultez régulièrement **la rubrique sécurité du site Internet de votre banque**. Elle est souvent mise à jour pour tenir compte des fraudes les plus récentes et les plus courantes.

Pour tous les réflexes de prévention, consultez notre ***collection de guides Sécurité*****.**

Comment réagir aux fraudes et tentatives ?

Vous devez **réagir rapidement** en cas de tentatives ou de fraudes. En cas de doute ou si vous n'êtes pas à l'origine d'une opération, prévenez immédiatement votre banque. Selon la nature de l'opération relevée, la banque pourra faire des recherches. Toutes les banques respectent des règles communes sur le traitement de la fraude. Les processus internes, mis en place pour respecter ces règles et assurer le meilleur service possible aux clients, sont propres à chaque banque.

Seule **une consultation régulière de votre compte** peut vous permettre de **détecter un incident ou une anomalie**. Connectez-vous au moins une fois par semaine à votre espace de banque à distance via le site ou l'application mobile de votre banque et vérifiez les opérations inscrites à votre compte ou vérifiez ces opérations dans votre relevé de compte dès sa réception, notamment avec les talons des chèques émis, les tickets de paiement carte et les courriels de confirmation de paiement (fournis la plupart du temps pour les achats sur Internet).

Assurez-vous que votre banque ait toujours **vos coordonnées à jour** (téléphone, adresse de courrier électronique…). En cas d'opération douteuse, elle peut avoir besoin de vous joindre rapidement.

Comment être remboursé en cas de fraude ?

Concernant les règles de remboursement, **tout dépend du moyen de paiement concerné**. Il est, dans tous les cas, recommandé de vous rapprocher de votre conseiller bancaire, qui sera le plus à même d'expliquer les démarches à suivre dans votre situation.

Chaque banque s'organise pour apprécier la situation au cas par cas, selon les circonstances et le type de fraude, et en assurer le traitement.

Ci-après, nous vous proposons un panorama des principaux types de fraudes, les réflexes à adopter lorsque vous pensez en être victime et les modalités de remboursement s'il y a lieu.

En cas de difficultés, contactez votre conseiller qui est votre interlocuteur de référence.

Pour plus d'informations sur la marche à suivre en cas de litige, consultez le mini-guide ***« Comment régler un litige avec ma banque »***.

PANORAMA PAR MOYEN DE PAIEMENT / OPÉRATION

La carte

La carte contient certaines informations, une piste magnétique et une puce électronique qui vous permettent de payer en magasin ou à distance, de retirer des espèces à un distributeur de billets (DAB), de faire des achats sur Internet. **Pour protéger ces informations et éviter les utilisations frauduleuses, il convient de conserver précieusement votre carte et veiller à taper votre code à l'abri des regards indiscrets**. Pour rappel : ne confiez ni votre carte ni votre code à des tiers, même à vos proches.

Votre carte est toujours en votre possession mais vous craignez que votre code confidentiel ait été intercepté ? Sachez qu'avec seulement le code confidentiel, personne ne peut effectuer de paiement sans la carte. Par précaution, vous pouvez demander à votre banque une nouvelle carte et un nouveau code confidentiel. Vous avez simplement oublié votre code ? Contactez votre banque.

LA PERTE OU LE VOL DE VOTRE CARTE OU DE SES DONNÉES

Comment réagir ?

- **Faites** sans tarder **opposition dès que vous constatez la perte, le vol, ou toute utilisation non autorisée de votre carte** ou de ses données en appelant le numéro fourni par votre banque, à défaut le 0 892 705 705 Service 0,34 € / min + prix appel accessible depuis la France métropolitaine (aussi accessible depuis l'étranger) pour que la carte ne puisse plus être utilisée.
  A l'étranger, appelez le numéro communiqué au préalable **par votre banque** ou celui figurant sur les distributeurs de billets.

La procédure d'opposition est définitive : vous ne pouvez pas demander la remise en service de votre carte après opposition même si vous la retrouvez par la suite. Pour avoir une nouvelle carte, faites-en la demande à votre banque. La carte aura un nouveau numéro et le cas échéant, un nouveau code confidentiel.

ATTENTION

Une opposition tardive vous priverait de la prise en charge par la banque des opérations contestées.

- Il est recommandé de **porter plainte auprès de la police** ou de la gendarmerie en cas de vol de votre carte. Il est important de faire cette démarche pour contribuer à la lutte contre la fraude même si ce n'est pas une condition préalable pour que la banque vous rembourse.

Quel remboursement ?

Si des opérations non autorisées ont été réalisées **avant l'opposition**, vous supportez **une franchise de 50 euros si le code confidentiel ou vos autres données de sécurité personnalisées ont été utilisés**. Cette franchise peut éventuellement être prise en charge si vous avez souscrit une assurance sur vos moyens de paiement.

Si vos données de sécurité personnalisées n'ont pas été utilisées ou que votre code confidentiel n'a pas été utilisé (paiement sans contact), vous êtes remboursé intégralement.

En cas d'opération postérieure à la mise en opposition de la carte, votre responsabilité ne sera pas engagée.

à savoir

VOTRE RESPONSABILITÉ RESTERA ENGAGÉE ET LES OPÉRATIONS NON AUTORISÉES RESTERONT À VOTRE CHARGE SI VOUS AVEZ FAIT PREUVE DE NÉGLIGENCE INTENTIONNELLE OU GRAVE NOTAMMENT DANS LA CONSERVATION DE VOTRE CARTE, DE VOTRE CODE CONFIDENTIEL OU DE VOS AUTRES DONNÉES DE SÉCURITÉ PERSONNALISÉES, EN CAS D'OPPOSITION TARDIVE, OU ENCORE SI VOUS AVEZ AGI FRAUDULEUSEMENT.

UN DÉBIT CARTE NON AUTORISÉ OU ERRONÉ

Vous venez de vérifier votre relevé de compte et un montant ne correspond pas à un de vos achats ou retraits ? La vérification de votre relevé de compte avec vos tickets de paiement carte permet de s'assurer que les opérations par carte débitées de votre compte sont bien celles que vous avez effectuées et que le montant est le bon.

Comment réagir ?

- Si vous ne retrouvez pas le ticket de paiement carte, peut-être l'avez-vous reçu par mail ou SMS. Vous avez peut-être aussi effectué un paiement à distance (par téléphone ou par Internet) ou accepté des paiements récurrents par carte (ex : abonnement) ou échelonnés (facilité de paiement).
- En cas de fraude, **faites opposition** en appelant le numéro fourni par votre banque, à défaut au **0 892 705 705** Service 0,34 € / min + prix appel en France métropolitaine (accessible aussi depuis l'étranger) pour que la carte ne puisse plus être utilisée. Une opposition tardive vous priverait de la prise en charge par la banque des opérations contestées. Demandez à votre banque une nouvelle carte et un nouveau code confidentiel.

En cas d'erreur de montant ou de tout autre litige avec le commerçant, vous ne devez pas faire opposition car il ne s'agit pas d'un cas d'utilisation frauduleuse de la carte ou de ses données. C'est avec le commerçant que vous devrez dialoguer.

- En cas d'**opération non autorisée** ou mal exécutée, **signalez-la rapidement à votre banque** et au plus tard dans les :
  - 13 mois suivant la date du débit de votre compte pour un paiement dans l'Espace Economique Européen – EEE (ce délai peut être plus court pour les clients professionnels),
  - 70 jours suivant la date du débit de votre compte, pour un paiement hors de l'EEE (le contrat carte peut prévoir un délai plus long ne pouvant excéder 120 jours).
- Il est recommandé de **porter plainte auprès de la police ou de la gendarmerie. Une pré-plainte en ligne est possible sur le site service-public.fr**. Il est important de faire cette démarche pour contribuer à la lutte contre la fraude même si ce n'est pas une condition préalable pour que la banque vous rembourse. Enfin, vous pouvez aussi signaler la fraude à la carte bancaire sur la **plateforme Perceval** depuis le site service-public.fr grâce au système d'identification France Connect.

Quel remboursement ?

Votre responsabilité ne sera pas engagée :

- en cas d'opération postérieure à la mise en opposition de la carte,
- si votre carte est toujours en votre possession en cas d'opérations effectuées par détournement de la carte ou de ses données ou en cas de contrefaçon de la carte et que votre code confidentiel ou vos autres données de sécurité personnalisées n'ont pas été utilisées.

En cas de paiement non autorisé, et sauf fraude ou négligence grave de votre part, le remboursement des opérations non autorisées et débitées à tort s'effectue, au plus tard, à la fin du premier jour ouvrable suivant. La banque rétablira votre compte dans l'état où il serait si l'opération n'avait pas eu lieu.

à savoir

VOTRE CARTE SANS CONTACT RÉPOND AUX MÊMES EXIGENCES ET VOUS FAIT BÉNÉFICIER DES MÊMES GARANTIES QUE LES AUTRES CARTES BANCAIRES EN CAS D'OPÉRATION NON AUTORISÉE OU MAL EXÉCUTÉE.

Le chèque

Que vous disposiez d'un chéquier ou que vous receviez un chèque en paiement, vous devez être particulièrement vigilant pour éviter les tentatives de fraude.

LA PERTE OU LE VOL D'UN CHÉQUIER / CHÈQUE VIERGE : LE FAUX CHÈQUE

Comment réagir ?

En cas de perte ou vol d'un chéquier ou de formule(s) de chèque vierge, vous devez **faire opposition au plus tôt** afin que votre banque puisse refuser le paiement d'un chèque qui se présenterait.

Le risque est aggravé par le fait que le chéquier comprend des chèques vierges pour lesquels ni la date ni le montant ne sont connus.

Tant que les chèques n'ont pas été encaissés, faites opposition via les moyens de communication mis à disposition par votre banque en indiquant le numéro du ou des chèques concernés.

Quel remboursement ?

En principe, la banque devra rembourser le paiement d'un chèque que vous n'avez pas fait ni signé. Toutefois, si vous avez commis une faute ou si vous avez permis la réalisation de la fraude (ex : faute dans la conservation du chéquier, opposition tardive, vérification tardive de vos relevés de compte…), vous pourrez également voir votre responsabilité engagée.

LA PERTE OU LE VOL D'UN CHÈQUE SIGNÉ : LA FALSIFICATION

Le bénéficiaire d'un de vos chèques ne l'a jamais reçu ?

Comment réagir ?

- Si le chèque n'a pas été encaissé :
  - **faites immédiatement opposition** via les moyens de communication mis à disposition par votre banque en indiquant le numéro du chèque concerné,
  - procédez à un nouveau paiement pour régler votre dette et demandez au bénéficiaire de vous donner une lettre de désistement (renonçant ainsi à présenter le chèque s'il était retrouvé).

Après avoir émis un chèque, il est illégal de faire opposition pour un motif autre que la perte, le vol, l'utilisation frauduleuse du chèque, une procédure de sauvegarde, de redressement judiciaire ou de liquidation judiciaire du bénéficiaire.

- Si le chèque a été encaissé, la banque :
  - peut vous confirmer l'opération,
  - **ne peut pas vous indiquer les coordonnées de la personne qui l'a encaissé** (cette indication est couverte par le secret bancaire). Seule la police, sur réquisition judiciaire, pourra l'obtenir.

Quel remboursement ?

En cas de falsification grossière et apparente (altération ou surcharge) d'un chèque valablement émis, la banque vous remboursera le montant du chèque falsifié.

à savoir

LA FALSIFICATION PEUT AUSSI CONCERNER LES CHÈQUES DE BANQUE.

LE FAUX CHÈQUE DE BANQUE

Le chèque de banque est utilisé parfois pour les paiements entre particuliers de montant important (ex : vente de voiture). Si vous devez être payé par chèque de banque, vérifiez qu'il comporte bien le **filigrane de sécurité**. Tous les chèques de banque, peu importe la banque émettrice, comportent un filigrane de haute qualité comparable à celui figurant sur les billets de banque et sur les pièces d'identité. Le motif (mention chèque de banque) est intégré au papier et non pas imprimé sur celui-ci, afin d'éviter les contrefaçons.

Il est recommandé de faire la transaction un jour d'ouverture des banques (évitez les week-ends et jours fériés). Appelez directement la banque émettrice au numéro que vous trouverez vous-même, en cherchant dans l'annuaire. Indiquez-lui le numéro du chèque de banque, son montant et le bénéficiaire. Elle vous confirmera qu'elle est bien à l'origine de l'émission de ce chèque.

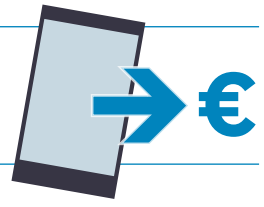
Comment réagir ?

Ces recommandations sont importantes car si le chèque est contrefait, créé de toute pièce par le fraudeur et payable par exemple sur une banque imaginaire ou même existante, il ne sera finalement pas payé et vous en supporterez le préjudice. Ni votre banque, ni celle faussement prétendue émettrice du chèque de banque ne sont concernées. **Vous devrez porter plainte à la police ou à la gendarmerie.**

Quel remboursement ?

Il y a peu de chance de récupérer l'argent qu'on vous devait une fois que le bien a été remis à l'escroc.

Le virement



Vous avez réalisé un virement ou vous constatez un virement débité que vous n'avez pas initié vous-même. A noter : le virement n'est réalisé qu'à partir de l'IBAN (International Bank Account Number).

L'UTILISATION D'UN IBAN FRAUDULEUX

Vous avez utilisé l'IBAN qu'on vous a fourni, spécialement, pour effectuer un virement. Mais c'est une personne mal intentionnée qui vous l'a fourni en se faisant passer pour quelqu'un que vous connaissiez. Dans ce cas, **il s'agit d'une usurpation d'identité**, fraude en forte recrudescence.

Comment réagir ?

Dans cette situation, il ne s'agit pas d'une « opération non autorisée » car la transaction a bien été réalisée sur la base de vos instructions. Cependant, vous avez été abusé par cette usurpation d'identité.

Signalez la fraude à la personne dont l'identité a été usurpée. Celle-ci pourra utilement porter plainte pour usurpation d'identité auprès de la police ou de la gendarmerie et se prémunir ainsi contre des incidents de son propre côté.

Quel remboursement ?

Une demande de rappel de fonds pourra être faite par votre banque à la banque du bénéficiaire, sans obligation de remboursement par le bénéficiaire ou la banque du bénéficiaire. En cas d'échec, vous pourrez demander à votre banque d'obtenir de la banque du bénéficiaire du virement, les informations qui vous permettront l'exercice de vos recours, y compris en justice, pour récupérer les fonds directement auprès du bénéficiaire.

LA FOURNITURE ERRONÉE D'UN IBAN OU LA SAISIE D'UN MAUVAIS NUMÉRO DE COMPTE BANCAIRE

Les informations nécessaires et suffisantes pour un virement sont :

- le numéro du compte à débiter,
- le montant, éventuellement la date d'exécution souhaitée,
- les coordonnées bancaires du compte à créditer (IBAN - International Bank Account Number).

C'est uniquement sur la base de ces informations (prévues par la réglementation) que les banques exécutent les virements. Notamment l'IBAN suffit à identifier sans équivoque le compte du bénéficiaire.
Il est donc primordial de le renseigner avec attention.

En effet, en cas d'erreur, si vous vous êtes trompé par exemple d'un chiffre, le virement sera tout de même exécuté par votre banque sur la base de cet IBAN erroné. Comme dans la situation précédente, vous pourrez **demander à votre banque de récupérer les fonds, sans garantie de remboursement** par le bénéficiaire, la banque du bénéficiaire ou votre banque, puisqu'il s'agit d'une opération que vous avez valablement effectuée.

Le prélèvement

Le prélèvement permet de payer de manière récurrente et régulière, pour des montants variables. **Il s'agit le plus souvent de régler un prestataire de services, d'énergie, etc**.

Des escrocs peuvent se faire passer pour un de ces prestataires, souvent les plus connus, pour récupérer votre IBAN et ainsi mettre en place des prélèvements sur votre compte. Voir la fraude aux coordonnées bancaires en annexe 2, n°1.

LE DÉTOURNEMENT D'IBAN

Comment réagir ?

Si en vérifiant vos comptes, vous constatez un prélèvement douteux, contactez rapidement votre banque pour lui signaler.

Vous devez **contester le prélèvement non autorisé rapidement** à votre banque et au plus tard dans les 13 mois suivant la date du débit de son compte pour un paiement dans l'Espace Economique Européen – EEE (ce délai peut être plus court pour les clients professionnels).

Votre banque vous remboursera alors l'opération en question.

Quel remboursement ?

En cas de paiement non autorisé, et sauf fraude ou négligence grave de votre part, le remboursement des opérations non autorisées et débitées à tort s'effectue, au plus tard, à la fin du premier jour ouvrable suivant. La banque rétablira votre compte dans l'état où il serait si l'opération n'avait pas eu lieu.

L'accès à sa banque et les opérations à distance

Pour lutter contre les fraudes, **une authentification forte vient compléter vos codes d'accès classiques en cas de connexion à la banque à distance, en cas d'opérations de paiement et/ou d'opérations sensibles**.

Ainsi, en plus de vos identifiant et mot de passe, un autre élément peut être exigé : un élément que vous connaissez, une caractéristique personnelle qui vous est intimement liée comme un élément biométrique (voix, visage, empreinte digitale…) ou encore l'utilisation d'un appareil qui vous appartient : téléphone portable, montre connectée, appareil dédié fourni par votre banque…

Plus d'infos sur l'authentification forte sur www.lesclesdelabanque.com.

LE FAUX SITE INTERNET D'UNE BANQUE, D'UN COMMERÇANT OU AUTRE…

Vous avez reçu un email d'un escroc se présentant comme votre banque ou comme un commerçant (enseigne connue en général) qui vous donne un lien pour vous connecter au site Internet de votre banque ou du commerçant. L'objectif de cet email est de vous soutirer des informations personnelles pour **usurper votre identité**, c'est ce qu'on appelle du **phishing** ou hameçonnage en français.

Si vous cliquez sur le lien, vous arriverez par exemple sur un faux site Internet de banque, que vous penserez à tort être votre espace personnel de banque à distance. Le but de l'escroc est d'y récupérer vos identifiant et mot de passe lors de votre connexion sur ce faux site de banque.

Contre le hameçonnage (ou phishing) la prévention est essentielle afin de ne jamais communiquer vos données de paiement ou vos codes d'accès à la banque en ligne : il ne faut jamais cliquer sur un lien envoyé par email pour se connecter à votre banque, il faut saisir vous-même l'adresse habituelle du site de votre banque en ligne.

Comment réagir ?

Contactez votre banque si vous avez un doute sur le site Internet bancaire sur lequel vous vous trouvez (exemple : tentative de phishing).

Sans attendre les instructions de la banque, **utilisez un autre terminal informatique pour changer vos codes d'accès**, puis vérifiez les dernières opérations effectuées.

Ayant accès à vos comptes à distance, les pirates pourraient procéder à des virements ou, en récupérant vos codes BIC et IBAN, mettre en place des prélèvements SEPA.

Si vous avez fourni vos codes d'accès à votre espace de banque à distance à un tiers via un site Internet, communiqué des éléments sur vos moyens de paiement ou si vous avez constaté des débits frauduleux sur votre compte, **contactez immédiatement votre banque**, aux coordonnées habituelles (n'utilisez pas celles du message email que vous venez de recevoir) afin de contester les opérations frauduleuses. **Le cas échéant, déposez plainte au commissariat de police ou à la gendarmerie la plus proche.**

Quel remboursement ?

Si vos codes d'accès ou données de paiement ont été utilisés et si un paiement a pu être réalisé, **la banque appréciera au cas par cas** s'il y a eu négligence grave de votre part ayant facilité la fraude, **avant tout remboursement**.

LA PERTE OU LE VOL DE VOS CODES D'ACCÈS À LA BANQUE À DISTANCE OU DES AUTRES DONNÉES DE SÉCURITÉ PERSONNALISÉES

En cas de perte ou vol de vos codes d'accès à votre espace de banque à distance ou de vos autres données de sécurité personnalisées, vous risquez qu'une autre personne les utilise à votre insu pour réaliser un paiement au débit de votre compte bancaire.

Comment réagir ?

- Alertez immédiatement votre banque, sans lui indiquer vos identifiants : elle n'a pas à les connaître.
- N'effectuez aucune opération de banque à distance.
- Connectez-vous, à partir d'un autre terminal, autre ordinateur ou smartphone le cas échant, au site de la banque en entrant manuellement son adresse.
- Changez vos codes d'accès de banque en ligne.
- Vérifiez que les dernières opérations enregistrées sont correctes, ainsi que les opérations en attente et les bénéficiaires de virement qui sont enregistrés.

Quel remboursement ?

Si vos codes d'accès et/ou vos données de sécurité personnalisées ont été utilisés et si un paiement a pu être réalisé, la banque appréciera au cas par cas **s'il y a eu négligence grave ou agissement intentionnel ou frauduleux de votre part** dans cette situation. Dans ces hypothèses, **la banque pourra refuser le remboursement**.

Annexe 1

TABLEAU RÉCAPITULATIF

MOYEN	FRAUDE / INCIDENT	RÉACTION	REMBOURSEMENT	RÉSERVE ÉVENTUELLE
CARTE	Perte / vol de la carte	• Opposition rapide au numéro fourni par sa banque • Vérifier les opérations passées et les contester s'il y a lieu le plus rapidement possible • Plainte à la police / gendarmerie recommandée	• Si débit, sans utilisation du code, remboursement intégral • Si débit avec utilisation du code ou données de sécurité personnalisées avant opposition, franchise de 50 euros et remboursement au-delà	Sauf si opposition tardive, si négligence grave ou intentionnelle, ou fraude du client
CARTE	Détournement des données	• Opposition rapide au numéro fourni par sa banque • Vérifier les opérations passées et les contester s'il y a lieu le plus rapidement possible • Plainte à la police / gendarmerie recommandée	Analyse au cas par cas, par la banque, des circonstances de la fraude. En l'absence de négligence grave du client, celui-ci est remboursé par la banque	Sauf si opposition tardive, si contestation tardive, si négligence grave ou intentionnelle, ou fraude du client
CHÈQUE	Perte / vol chèque vierge	• Opposition rapide via les moyens de communication mis à disposition par sa banque • Plainte à la police / gendarmerie recommandée	Remboursement du chèque faux, dont le client n'est pas l'auteur	Si opposition tardive ou vérification tardive des relevés de compte
CHÈQUE	Perte / vol chèque signé et falsifié	• Opposition rapide via les moyens de communication mis à disposition par sa banque • Plainte à la police / gendarmerie recommandée	• Responsabilité de la banque en cas de faute dans le traitement du chèque (altération, surcharge apparente…) • Responsabilité partagée si client négligent	Si opposition tardive

MOYEN	FRAUDE / INCIDENT	RÉACTION	REMBOURSEMENT	RÉSERVE ÉVENTUELLE
VIREMENT	Erreur involontaire d'IBAN	• Alerter rapidement sa banque qui pourra adresser une demande de rappel de fonds à l'autre banque • À défaut de remboursement, récupération des informations afin que l'émetteur du virement exerce ses recours contre le bénéficiaire	Rappel de fonds par la banque ou action en justice par l'émetteur du virement	
VIREMENT	Fraude à l'IBAN	• Alerter rapidement sa banque qui pourra adresser une demande de rappel de fonds à l'autre banque • À défaut de remboursement, récupération des informations afin que l'émetteur du virement exerce ses recours contre le bénéficiaire	Rappel de fonds par la banque ou action en justice par l'émetteur du virement	
PRÉLÈVEMENT	Fraude à l'IBAN	Alerter rapidement sa banque et maximum dans les 13 mois du prélèvement non autorisé	Le remboursement s'effectue, au plus tard, à la fin du premier jour ouvrable suivant la demande. Le compte est rétabli dans l'état où il serait si l'opération n'avait pas eu lieu	Sauf fraude ou négligence grave du client
ACCÈS BANQUE À DISTANCE	Si codes d'accès ou autres données de sécurité personnalisées fournis ou détournés / ou si débit constaté (ex : cas de phishing)	• Signaler rapidement l'incident à sa banque • Changer les codes et le cas échéant les autres données de sécurité personnalisées • Plainte à la police / gendarmerie recommandée • Signaler l'incident sur internet-signalement.gouv.fr	Analyse au cas par cas, par la banque, des circonstances de la fraude. En l'absence de négligence grave du client, celui-ci est remboursé par la banque	Sauf si négligence grave ou intentionnelle, ou fraude du client
ACCÈS BANQUE À DISTANCE	Perte / vol des codes d'accès / autres données de sécurité personnalisées	• Changer les codes d'accès sur un autre terminal de préférence • Signaler rapidement l'incident à sa banque	Remboursement	Sauf si négligence grave ou intentionnelle, ou fraude du client

Annexe 2

QUELQUES PIÈGES TYPES À (RE)CONNAÎTRE

Nous présentons ci-après un panel de fraudes types, des plus récentes aux plus anciennes. De plus en plus organisées et abouties, elles utilisent souvent les sites et les réseaux sociaux. La grande majorité des fraudes joue sur la palette émotionnelle que peut ressentir toute cible de ces tentatives. Ainsi, les "offres" mettront en avant ou utiliseront :

- la peur… de perdre de l'argent, de perdre un droit, de manquer une occasion…,
- l'envie… de gagner de l'argent, de faire mieux que les autres…,
- la solidarité… le besoin d'être utile, de participer à l'effort collectif…

C'est pourquoi, tout message, appel téléphonique ou bannière publicitaire doit vous alerter s'il (elle) présente un caractère urgent, un gain rapide, un rendement certain, une absence de risque, une facilité de mise en place, une gratuité, etc. Rappelons-le : il n'y a pas de forte rentabilité sans risque.

De plus, pour rendre ces offres crédibles, les escrocs utilisent des adresses de messagerie ou des sites aux noms rassurants, le nom d'entreprises réelles ou au nom très proche de celles-ci. Ils utilisent des noms bien connus de grandes entreprises ou d'administrations publiques pour inspirer votre confiance en usurpant l'identité par exemple de la CAF, des impôts, de banques, fournisseurs d'énergie ou d'Internet, etc…

1. La fraude aux coordonnées bancaires

Les circonstances

Vous recevez un courrier d'un de vos organismes créanciers vous informant de faire désormais vos virements vers de nouvelles coordonnées bancaires jointes (nouveau RIB : IBAN BIC) ou vous réclame votre IBAN.

Où est le piège ?

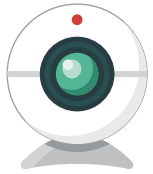
Un escroc fait croire à un changement de domiciliation bancaire de votre bailleur, d'un fournisseur ou de tout autre créancier légitime pour les prochains règlements de loyers ou de factures. Il envoie les nouvelles coordonnées bancaires par courrier, électronique le plus souvent, avec des caractéristiques de messagerie très proches de celles de votre interlocuteur habituel.

Comment l'éviter ?

Ce type de fraude, qui concernait au départ surtout les entreprises, touche désormais de plus en plus les particuliers. Un ordre de virement ne peut pas être annulé, la somme ne peut donc pas être restituée par un transfert en sens inverse.

Vous devez être particulièrement vigilant quand vous remettez vos coordonnées bancaires. Vous devez vous assurer qu'il s'agit de personnes ou prestataires de confiance. Que ce soit par virement ou prélèvement, si un de vos correspondants habituels vous informe d'un changement de coordonnées bancaires ou vous réclame votre IBAN, assurez-vous de la véracité de cette information en contactant la personne (ou organisme) au numéro de téléphone (ou adresse) que vous utilisez habituellement ou en trouvant vous-même les cordonnées.

2. Le chantage à la webcam



Les circonstances

Une personne malveillante vous fait croire qu'elle détient des photos ou des vidéos compromettantes de vous pour vous faire du chantage. Elle va notamment vous menacer de diffuser ces éléments (sur Internet ou de les envoyer à vos familles, amis, proches…) si vous refusez de payer une rançon.

Où est le piège ?

Cette arnaque s'opère particulièrement sur les sites de rencontre et sur les réseaux sociaux : les pirates vont tenter de gagner votre confiance grâce à un faux profil attractif. La plupart du temps, les escrocs n'ont tout simplement rien récupéré vous concernant. Ils envoient massivement un message ; ils ont ainsi une probabilité de récupérer un minimum de paiements en comptant sur la panique des personnes ciblées.

Comment l'éviter ?

Ne vous laissez pas impressionner par les messages alarmants, même si vous utilisez quelquefois votre webcam. Utilisez un antivirus régulièrement mis à jour et ne cliquez jamais sur une pièce jointe ou un lien de provenance inconnue ou douteuse.

3. Le ransomware

Les circonstances

Tranquillement en train de surfer sur Internet ou d'utiliser un logiciel de votre ordinateur, l'écran se bloque sur un message alarmant. Il vous indique que votre ordinateur est bloqué et vos données inaccessibles. Vous ne pourrez les récupérer qu'en payant une rançon. Le message est insistant : il faut payer vite sans quoi, vous perdrez tout.

Où est le piège ?

Un ransomware est un programme malveillant utilisé par des pirates informatiques pour piéger votre matériel (ordinateur, smartphone, tablette…), bloquer vos fichiers ou vos accès et vous extorquer de l'argent. On peut distinguer le ransomware :

- crypto, où vos fichiers, documents, images, vidéos… sont chiffrés et en quelque sorte pris en otage,
- locker, où l'accès à votre ordinateur (ou à certaines fonctionnalités de celui-ci) vous est refusé.

Comment l'éviter ?

Souvent le ransomware infecte votre matériel en s'infiltrant à travers un fichier téléchargé sur Internet ou reçu par email. Ces emails peuvent aussi inclure des pièces jointes piégées ou des liens vers des sites malveillants.

Il est primordial de ne pas cliquer sur une pièce jointe ou un lien de provenance inconnue ou douteuse. Ayez toujours un antivirus à jour sur votre matériel.

Vous ne devez jamais payer la rançon demandée. Vous n'avez aucune garantie que les escrocs vous fourniront la clé qui permettra de déchiffrer vos fichiers ou débloquer votre ordinateur.

Avertissez votre banque et faites opposition si nécessaire.

Signalez la tentative d'escroquerie sur www.internet-signalement.gouv.fr. En cas de difficultés, vous pouvez trouver de l'assistance auprès de www.cybermalveillance.gouv.fr.

Variante : *Vous êtes sur Internet et une page s'affiche faisant croire qu'un virus bloque votre ordinateur ou smartphone. Le message demande d'appeler un numéro de téléphone afin de télécharger un logiciel pour débloquer l'appareil. N'appelez jamais ce numéro, il suffit de redémarrer le poste pour que celui-ci fonctionne à nouveau.*

4. Le faux prêt

Les circonstances

Dans ce type de fraude, vous recevez un message vous proposant le rachat de vos crédits à un taux imbattable. Les escrocs se font passer pour une banque ou une société financière.

Où est le piège ?

L'idée pour les fraudeurs est de récupérer toutes vos données pour usurper votre identité afin de se faire octroyer un crédit en ligne à votre place. Pour ce faire, les escrocs prétextent les démarches pour constituer votre dossier de rachat de crédit. La somme empruntée est bien versée sur votre compte mais vous êtes recontacté ensuite pour transférer le montant vers un compte externe, pour finaliser ainsi l'opération de rachat de crédit.

Comment l'éviter ?

Avant toute démarche, contactez directement votre conseiller bancaire et/ou l'établissement de crédit concerné en trouvant vous-même les coordonnées, pour vérifier la démarche.

Méfiez-vous d'un taux qui ne rentrerait pas dans la fourchette des taux actuellement pratiqués.

5. La fraude aux faux tests techniques

Les circonstances

Vous recevez un appel ou un email des services techniques de la banque ou encore son service fraude ou sécurité. Il vous est demandé d'effectuer des tests, afin de renforcer le niveau de sécurité, ou l'on vous offre des mises à jour de votre espace abonné. Vous vous rendez sur l'environnement de test et/ou vous suivez les instructions données.

Où est le piège ?

Il ne s'agit pas en réalité des techniciens de la banque mais de fraudeurs. Ils peuvent même vous proposer de prendre la main sur votre ordinateur ou encore vous inciter à réaliser un virement pour tester des mises à jour. En leur « obéissant », vous venez de donner un accès aux informations et à votre espace de banque en ligne.

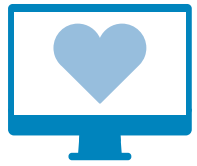
Comment l'éviter ?

Votre banque ne vous contactera jamais pour faire un test technique. Devant un tel appel ou message, différez l'intervention et rapprochez-vous de votre banque aux coordonnés habituelles pour lui signaler.

Si des tests devaient être réalisés, ce serait à votre initiative devant une difficulté que vous rencontreriez. Les banques ne font jamais de test de virement.

Soyez particulièrement suspicieux si la demande est urgente, insistante, le montant élevé et le virement demandé vers un pays inhabituel.

6. La fraude aux sentiments



Les circonstances

Vous êtes inscrit sur un site de rencontre.

Où est le piège ?

Les fraudeurs prennent leur temps pour instaurer la confiance, la relation se noue, vous échangez des messages, et peu à peu votre vigilance s'estompe. Ils ont utilisé de fausses identités et de fausses photos particulièrement sur les sites de rencontre. Ensuite, l'idée est de vous manipuler pour vous soutirer de l'argent, en inventant des histoires de proches, en détresse médicale ou financière par exemple. Une fois l'argent envoyé, ils disparaissent du réseau.

Comment l'éviter ?

Evitez de donner trop de renseignements personnels sur les réseaux sociaux, et notamment sur les sites de rencontre. Ne donnez jamais aucune indication sur vos données bancaires.

Restez vigilant et méfiez-vous des rencontres idylliques en ligne.

N'envoyez jamais d'argent et n'acceptez jamais non plus d'en recevoir par exemple en encaissant un chèque en échange d'un transfert d'argent ou de cartes prépayées. Il s'agira sûrement d'un chèque sans provision ou d'un chèque volé.

7. Les arnaques sur les réseaux sociaux

Les circonstances

Vous êtes inscrit sur un ou plusieurs réseaux sociaux. Une multitude de sollicitations apparaît chaque jour. Parfois, il s'agit de promesse d'argent facile, travail sur-rémunéré, demande de service contre commission... Les fraudeurs sont nombreux et utilisent de faux comptes et de faux profils.

Où est le piège ?

La fraude la plus fréquente est celle du virement « rémunéré » ou « commissionné ». En échange d'une commission intéressante, on vous demande de réceptionner des fonds puis d'effectuer un virement généralement vers une banque étrangère ou une banque en ligne.

Une variante consiste à ce qu'on vous demande votre carte de paiement et votre code confidentiel pour pouvoir effectuer des retraits au Distributeur Automatique de Billets/Guichet Automatique Bancaire (DAB/GAB).

Cette fraude joue sur l'appât du gain : être payé pour juste réaliser un virement, c'est de l'argent facile et c'est donc très tentant. Il suffit de donner son IBAN pour recevoir la « commission ». Seulement si votre compte se retrouve bien crédité de ladite commission, c'est via l'encaissement d'un chèque que vous aurez accepté de déposer sur votre compte ; vous effectuez le virement tel que demandé. Le chèque se révèlera par la suite être un faux chèque ou un chèque sans provision. Et votre compte sera débité du montant du chèque. La personne n'est alors plus joignable et tous ses profils sur les réseaux sociaux sont fermés.

Ce type de fraude sur les réseaux sociaux est la transposition modernisée de la fraude qui consiste à recruter une mule par email (cf. page 37). Le comportement de mule est un délit : vous risquez d'être reconnu complice d'une fraude passible de poursuites judiciaires

Comment l’éviter ?

Sur les réseaux sociaux, n'acceptez comme relation que les personnes que vous connaissez vraiment dans votre réseau personnel et professionnel.

Méfiez-vous des promesses d'argent facile car cela n’existe pas dans la vraie vie.

Ne communiquez jamais vos coordonnées bancaires sur les réseaux sociaux. Ne partagez que des données que vous considérez comme publiques ; toutes les données, que vous publiez vous-même, pourraient être vues et récupérées par des personnes malveillantes même si vous pensez les réserver à votre cercle d’amis. Les termes de confidentialité peuvent ne pas être bien paramétrés sur votre compte.

8. La fraude aux offres d’emploi

Les circonstances

Vous êtes en recherche d’emploi et consultez de nombreux sites en ligne. Les sites d'offres d'emploi cachent parfois des arnaqueurs qui cherchent à profiter de la situation et notamment de la détresse de certains demandeurs d’emploi.

Où est le piège ?

Vous tombez sur des offres d’emploi alléchantes ou très engageantes. L'unique objectif de ces fausses offres est d'obtenir des informations personnelles ou de vous escroquer de l'argent.

Comment l’éviter ?

Soyez vigilant si l’offre comporte un salaire anormalement élevé, des horaires très allégés ou un travail peu laborieux, si elle est envoyée à des heures très inhabituelles, si l’expéditeur est d'un autre pays ou continent, ou encore si vous devez envoyer de l'argent pour obtenir un entretien ou un dossier de candidature ou au contraire, si l’entreprise veut vous verser de l’argent avant la signature du contrat.

Vérifiez la présence de l'entreprise sur le web et sa réputation. Si vous ne trouvez aucune information sur cette société ou si le site vous parait étrange, ne donnez pas suite.

Les vraies annonces sont rédigées par des professionnels des ressources humaines, sans faute d’orthographe ni phrases originales.

9. La fraude à la loterie

Les circonstances

Vous recevez un courrier électronique sur votre ordinateur ou un SMS sur votre téléphone portable. Il prétend que vous avez gagné un prix et vous invite à répondre en joignant vos coordonnées bancaires afin que le prix puisse être viré sur votre compte.

Où est le piège ?

Vous communiquez vos coordonnées bancaires à des escrocs qui sont susceptibles de les utiliser ou de les transférer. Si vous appelez au numéro indiqué, l'appel est surfacturé et n'aboutit à rien.

Comment l'éviter ?

Une offre trop alléchante est sans doute une arnaque. Elle peut provenir d'un faux commerçant et/ou vous rendre complice d'une fraude.

10. Etre payé par un autre moyen de paiement que celui prévu

Les circonstances

Vous vendez un bien. L'acquéreur vous demande vos coordonnées bancaires pour vous faire un virement. Il vous adresse finalement un chèque que vous déposez sur votre compte. Le montant prévu arrive sur votre compte et vous livrez la marchandise (un véhicule par exemple). Le montant a été ainsi crédité via l'encaissement du chèque et non via virement comme prévu initialement. Quelques jours plus tard, le chèque encaissé est rejeté et votre compte est débité du montant du chèque.

Où est le piège ?

Le chèque déposé était un faux chèque, il a donc été rejeté. Votre compte est débité.

Comment l'éviter ?

Assurez-vous que le paiement est réalisé selon les modalités convenues avec l'acheteur. N'encaissez pas un chèque si vous deviez recevoir un virement. Dans le cas cité, avant de livrer le bien, vérifiez que votre compte est bien crédité par un virement.

11. L'acquéreur trop généreux

Les circonstances

Vous vendez un bien. L'acquéreur vous propose un prix supérieur en prétextant qu'il vous procure un service complémentaire (des frais de transport par exemple). Vous recevez un chèque du montant global (prix + service) que vous encaissez. L'acquéreur annule le service supplémentaire (transport par exemple) et vous demande de lui rembourser la différence entre le prix d'origine du bien et le montant total qu'il vous a déjà payé, soit par virement sur un compte de tiers, soit par transfert d'espèces à un tiers.

Où est le piège ?

Le chèque étant un faux, il reviendra impayé. Au mieux, vous gardez votre bien mais vous perdez le montant soi-disant « remboursé ».

Comment l'éviter ?

Méfiez-vous d'une offre de prix supérieure au montant demandé, n'acceptez que des montants correspondant au montant de la transaction. Dans le cas cité, refusez, n'encaissez pas le chèque et ne livrez pas le bien.

12. Etre recruté comme mule

Les circonstances

Vous recevez un courrier électronique vous proposant de collaborer à une soi-disant société financière (parfois un contrat de travail est joint à l'offre pour la rendre plus crédible). On vous offre une rémunération si vous rendez le service suivant : recevoir sur votre compte une somme d'argent d'un certain montant puis la transférer ensuite sur un autre compte qu'on vous indiquera. Il s'agit de promesse d'argent facile.

Où est le piège ?

Par ce transit d'argent, l'escroc « blanchit » de l'argent provenant probablement d'un trafic.

La fraude est difficile à détecter et la récupération des fonds compliquée. En tant que « mule », vous risquez d'être reconnu complice d'une fraude passible de poursuites judiciaires.

Comment l'éviter ?

Ne vous laissez pas tenter par l'appât du gain. N'acceptez pas d'encaisser un chèque sur votre compte pour le compte d'un tiers, et refusez d'effectuer tout virement. Refusez l'opération. Détruisez ce type de message dès réception.