Fraudes aux opérations bancaires

COMMENT RÉAGIR ?
DANS QUELS CAS PUIS-JE ÊTRE REMBOURSÉ ?

les clés de la banque

LES GUIDES BANCAIRES
Hors-Série

CE GUIDE VOUS EST OFFERT PAR :

les clés de la banque

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 : septembre 2024

SOMMAIRE

Introduction

La sécurité des opérations bancaires est essentielle, que ce soit en agence, par téléphone ou en ligne. Les banques renforcent constamment leurs systèmes de protection contre les fraudes. En 2021, « l'authentification forte » a été introduite pour une meilleure sécurité lors des opérations à distance telles que la connexion en ligne, les paiements et les opérations sensibles.
Pour déjouer ces nouvelles mesures sécuritaires, les escrocs utilisent des techniques de manipulation.

Ce guide fournit des informations générales, des recommandations spécifiques par moyen de paiement et identifie les fraudes courantes à (re)connaître, tout en indiquant les conditions de remboursement éventuel.

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 rapidité de réaction sont cruciales pour lutter efficacement contre les fraudes et tentatives.

1. Se prémunir contre les fraudes

Protégez vos données

En tant que client de la banque, vous devez faire attention à vos données personnelles et bancaires comme vous le faites avec vos papiers d'identité ou vos clés. En les protégeant, vous vous protégez.

Limitez la mise en ligne d'informations pour réduire le risque d'escroquerie. Vos données personnelles, même non confidentielles, peuvent en effet être mal sécurisées, et donc volées et utilisées à votre insu notamment pour récupérer ensuite vos données bancaires.

Gardez vos codes strictement confidentiels, qu'il s'agisse de vos moyens de paiement ou de la connexion à vos comptes à distance. Ne les partagez avec personne, pas même avec votre conseiller bancaire. **Codes, mots de passe et identifiants bancaires : ne donnez jamais ces données !**

Ne conservez pas vos données sur des supports non sécurisés, qu'ils soient physiques (carnet, post-it…) ou informatiques (messagerie électronique, disque dur, téléphone portable…). Si nécessaire, utilisez un gestionnaire de mot de passe sécurisé.

Lisez bien toutes les informations données lors du parcours d'autorisation d'une opération

Lors de la validation d'une opération, **prenez le temps de vérifier tous les détails pour assurer sa sécurité.**

Le processus de validation fournit des informations claires sur l'opération en cours, telles que le montant, le bénéficiaire, l'horodatage, le caractère unique ou récurrent, et la périodicité le cas échéant, le caractère irrévocable de la validation de l'ordre de paiement.

Soyez attentif à la concordance entre l'identité du bénéficiaire et l'IBAN lors du 1er virement vers un compte. Le parcours d'autorisation rappelle explicitement que la concordance n'aura pas fait l'objet d'un contrôle par la banque.

Par ailleurs, le parcours d'autorisation propose clairement la possibilité de refuser l'opération.

ATTENTION L'authentification forte ne permet jamais d'annuler une opération de paiement, mais bien de valider l'autorisation d'exécution d'un paiement, d'un ajout de bénéficiaire, d'une augmentation de plafond, etc. N'autorisez jamais une opération dont vous n'êtes pas à l'origine.

Gardez le lien avec votre banque

Utilisez toujours un canal sécurisé et connu pour établir un contact. **Ne cliquez jamais sur un lien reçu par e-mail ou SMS.**

Informez votre banque de tout changement de coordonnées (téléphone, adresse de courrier électronique…) via le canal habituel préconisé par votre banque. En cas d'opération douteuse, elle pourra ainsi vous joindre rapidement.

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

Pour plus de réflexes de prévention, consultez notre collection de guides Sécurité.

2. Réagir aux tentatives de fraude

Adoptez ces **réflexes simples** pour vous protéger :

- Restez calme et faites preuve de bon sens.
- Prenez le temps d'analyser la demande qui vous est faite.
- Consultez des personnes de confiance pour obtenir un avis extérieur.
- Recherchez des informations supplémentaires pour confirmer la légitimité de la demande.
- Effectuez une recherche sur Internet avec les mots clés + « arnaque ».
- Évitez de divulguer des informations sur les réseaux sociaux ou les sites Internet en cas de doute.
- Ne fournissez aucune information par téléphone si vous n'avez pas initié le contact.
- Abstenez-vous d'agir ou de répondre en cas de doute.
- Ne partagez jamais vos codes d'accès bancaires, les données de votre carte ou vos mots de passe.

Vous avez un doute ou vous n'avez pas initié l'opération ? Prévenez immédiatement votre banque. **Consultez régulièrement votre compte pour détecter tout incident ou anomalie**. Connectez-vous au moins 1 fois par semaine à votre espace bancaire en ligne via le site ou l'application mobile. Vérifiez les opérations inscrites à votre compte notamment avec les tickets de paiement carte (papier ou numérique), les talons des chèques émis.

Cybermalveillance.gouv.fr, propose des modules d'e-sensibilisation (« SensCyber »), accessibles à tous, pour comprendre, agir, partager les bonnes pratiques et tester vos connaissances en matière de cybersécurité.

3. Faire une contestation pour obtenir un éventuel remboursement en cas de fraude

Votre démarche auprès de la banque

Contactez votre conseiller bancaire, il vous expliquera comment procéder selon le moyen de paiement concerné. Le caractère « **non autorisé** » de la transaction peut être essentiel pour obtenir un remboursement par la banque.

Fournissez à la banque **tous les éléments concernant la fraude** dont vous êtes victime : nature et circonstances de l'opération (informations sur l'escroc, procédés techniques ou manipulations supposés, appareils utilisés, messages ou appels reçus, actions réalisées sous la manipulation du fraudeur, etc.).

Indiquez également **les actions entreprises** : blocage du moyen de paiement, blocage de votre espace bancaire en ligne, signalement via les plateformes Perceval ou Thésée, dépôt de plainte auprès des forces de l'ordre, etc.

Le traitement par la banque

Chaque banque analyse la situation au cas par cas pour décider du remboursement éventuel, généralement dans un délai d'1 jour ouvré. Elle effectue une 1ère analyse de l'opération pour déterminer si celle-ci doit faire l'objet d'un remboursement (ou pas).

La banque peut être amenée à approfondir ses recherches pour valider sa décision. Elle pourra donc finalement récupérer les fonds qu'elle vous avait remboursés à J+1.

Elle examine différents éléments comme les paramètres techniques (l'origine de la transaction, l'appareil utilisé, la localisation géographique, l'authentification forte, le contexte) pour déterminer si vous avez autorisé ou non l'opération. **En cas de doute sur votre consentement, elle procède au remboursement immédiat de la transaction sauf démonstration d'une négligence grave de votre part.**

- **En cas de remboursement** : une reprise des fonds, remboursés à J+1 par la banque, est possible dans les 30 jours suivant (sauf situation exceptionnelle), en fonction du résultat de ses recherches.
- **En cas de refus de remboursement** : la banque vous indiquera les motifs et vous donnera s'il y a lieu des éléments le justifiant (par ex : mandat de prélèvement, éléments transmis par le commerçant, preuve de négligence grave…). Dans ce cas, elle vous guidera pour toute réclamation éventuelle.

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

Pour plus d'informations en cas de litige, consultez le guide « Comment régler un litige avec ma banque ? ».

Recommandations par moyen de paiement/ opération

Soyez vigilant pour préserver la sécurité de vos moyens de paiement et leurs données (mot de passe, code confidentiel, cryptogramme...).

1. La carte

Protégez votre carte pour éviter les utilisations frauduleuses. Conservez-la précieusement et tapez votre code à l'abri des regards indiscrets. Ne confiez jamais votre carte ou votre code à un tiers, même pas à un proche.

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

La perte ou le vol, de votre carte ou de ses données

Comment réagir ?

Dès que vous constatez la perte, le vol, ou toute utilisation non autorisée de votre carte ou de ses données, selon la situation **vous pouvez bloquer temporairement la carte ou sinon faites opposition** :

- depuis votre application bancaire ;
- en vous connectant à votre espace bancaire en ligne ;
- en appelant votre banque.

A défaut, contactez le 0.892.705.705 (service 0,35€/min + prix appel), depuis la France métropolitaine ou l'étranger, pour bloquer la carte.

Depuis l'étranger, c'est pareil via l'application et le site. En revanche, la banque a pu mettre en place un numéro de téléphone spécial. À défaut, appelez le numéro figurant sur les distributeurs de billets.

La procédure d'opposition est définitive : vous ne pourrez pas demander la remise en service de votre carte, même si vous la retrouvez. Adressez-vous à votre banque pour obtenir une nouvelle carte. Celle-ci aura un nouveau numéro et éventuellement, un nouveau code confidentiel.

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

En cas de vol, portez plainte (pré-plainte possible sur le site service-public.fr) et signalez la fraude sur Perceval. Ces démarches contribuent à la lutte contre la fraude même si elles ne sont pas obligatoires pour que la banque vous rembourse.

Quel remboursement ?

Vous êtes **remboursé intégralement si les données de votre carte** et le code confidentiel **n'ont pas été utilisés** (ex : paiement sans contact).

En revanche, s'ils ont été utilisés, vous supportez une **franchise de 50 € pour les opérations non autorisées**, réalisées **avant l'opposition**. Cette franchise peut être prise en charge si vous avez souscrit une assurance sur vos moyens de paiement.

En cas d'opérations de paiement après l'opposition de la carte, votre responsabilité n'est, bien sûr, pas engagée.

Les opérations non autorisées resteront à votre charge si vous avez fait preuve de négligence intentionnelle ou grave dans la conservation de votre carte, de votre code confidentiel ou de vos données personnelles de sécurité. De même, en cas d'opposition tardive, ou encore si vous avez agi frauduleusement.

Un paiement carte non autorisé ou erroné

Pour réagir rapidement, **consultez régulièrement votre compte** via vos relevés, le site web ou l'application de votre banque. Vérifiez vos tickets de paiement carte (papier ou numérique, reçu par mail ou SMS selon les cas). N'oubliez pas les paiements à distance (téléphone ou Internet) que vous avez pu réaliser ou les paiements échelonnés (facilité de paiement) et les paiements récurrents par carte que vous avez acceptés (ex : abonnement).

Comment réagir ?

- En cas de fraude, **faites opposition pour bloquer la carte** en appelant le numéro fourni par votre banque. A défaut, appelez au 0.892.705.705 (service 0,34€/min + prix appel) en France métropolitaine (accessible aussi depuis l'étranger). 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.

L'opposition est interdite en cas d'erreur de montant ou de tout autre litige avec le commerçant car il ne s'agit pas d'une utilisation frauduleuse de la carte ou de ses données. Dans ce cas, vous devez prendre contact avec le commerçant pour résoudre le problème avec lui.

- **Signalez rapidement à votre banque toute opération non autorisée** ou mal exécutée. Selon la date du débit en compte, vous disposez d'un délai maximum de :

  - 13 mois pour un paiement effectué dans l'Espace Economique Européen (EEE) ;

  - 70 jours pour un paiement effectué hors de l'EEE (le contrat de la carte peut prévoir un délai plus long mais jamais plus de 120 jours).

- **Portez plainte** (pré-plainte possible sur le site service-public.fr) et signalez la fraude sur Perceval. Ces démarches contribuent à la lutte contre la fraude même si elles ne sont pas obligatoires pour que la banque vous rembourse.

Quel remboursement ?

Votre responsabilité ne sera pas engagée pour un paiement non autorisé :

- après la mise en opposition de la carte ;
- suite à un détournement de la carte ou de ses données, et si votre carte est toujours en votre possession ;
- en cas de contrefaçon de la carte et si ses données et le code confidentiel n'ont pas été utilisés (ex : paiement sans contact).

Sauf fraude ou négligence grave de votre part, le remboursement s'effectue, au plus tard, à la fin du 1er jour ouvrable suivant.
La banque rétablira votre compte dans l'état où il serait si l'opération n'avait pas eu lieu.

2. Le chèque

Avec votre chéquier comme avec les chèques que vous recevez 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 ?

Le risque est aggravé en cas de formules de chèque vierge car ni la date ni le montant ne sont remplis. C'est pourquoi, en cas de perte ou vol, vous devez **faire opposition au plus tôt et avant tout encaissement** via les moyens de communication mis à disposition par votre banque. Indiquez le numéro du ou des chèques concernés. Votre banque pourra ainsi refuser leur paiement s'ils se présentaient.

Quel remboursement ?

Si le chèque est déjà passé à l'encaissement, en principe, **la banque devra le rembourser si vous n'êtes pas à l'origine de ce paiement par chèque. 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 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 ;
- 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).

ATTENTION Il est illégal de faire opposition à un chèque 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 pourra** vous **confirmer l'opération, sans** pouvoir **vous indiquer les coordonnées de la personne qui l'a encaissé** (information 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.

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).

Vous acceptez d'être payé par chèque de banque ? Vérifiez qu'il comporte bien le **filigrane de sécurité** (mention « chèque de banque »), intégré au papier et non imprimé. Obligatoire sur tous les chèques de banque, peu importe la banque émettrice, il vise à éviter les contrefaçons. De haute qualité, il est comparable à celui figurant sur les billets de banque et les pièces d'identité.

N'opérez la transaction qu'un jour où la banque est ouverte (pas 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 ?

En cas de chèque contrefait, vous devrez **porter plainte** à la police ou à la gendarmerie pour le préjudice subi car le chèque ne sera finalement pas payé, puisque créé de toute pièce par le fraudeur. Ni votre banque, ni celle faussement prétendue émettrice du chèque de banque ne sont concernées.

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.

3. Le virement

Le virement n'est réalisé qu'à partir de l'IBAN (International Bank Account Number). Vous devez donc être particulièrement vigilant lors de l'ajout d'un bénéficiaire de virement.

ATTENTION Le champ « Nom du bénéficiaire » ne vous assure pas de la concordance entre l'identité du bénéficiaire et l'IBAN fourni. Il ne sert qu'à vous faciliter le suivi des opérations. Aucun contrôle n'est en effet effectué par la banque ou l'établissement de paiement.
À compter d'octobre 2025, un contrôle de concordance entre le nom du bénéficiaire et l'IBAN sera effectué (règlement européen du 13 mars 2024).

L'utilisation d'un IBAN frauduleux

Vous avez utilisé un IBAN pour effectuer un virement mais il venait d'une personne mal intentionnée qui s'est fait passer pour une de vos connaissances ? **L'usurpation d'identité** est 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.

- **Informez rapidement votre banque pour envisager un rappel de fonds.**
- **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 ?

Votre banque pourra procéder à une demande de rappel de fonds auprès de la banque du bénéficiaire, sans obligation de remboursement, ni par le bénéficiaire ni par sa banque. En cas d'échec, demandez à votre banque d'obtenir les informations nécessaires auprès de la banque du bénéficiaire du virement. Ces informations vous

permettront d'exercer vos recours, y compris en justice, pour récupérer les fonds directement auprès du bénéficiaire.

La fourniture erronée d'un IBAN : saisie d'un mauvais numéro de compte bancaire

Voici les informations nécessaires et suffisantes (prévues par la réglementation) pour que les banques exécutent un virement :

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

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. Vous pourrez **demander à votre banque de récupérer les fonds, sans garantie de remboursement** ni par le bénéficiaire ni par la banque du bénéficiaire ni par votre banque, puisqu'il s'agit d'une opération que vous avez valablement effectuée.

4. Le prélèvement

Le prélèvement permet de payer, de manière récurrente et régulière, 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 ou fraude au RIB page 26.*

Le détournement d'IBAN

Comment réagir ?

Vous constatez un prélèvement douteux à la consultation de votre compte ? **Contactez rapidement votre banque** pour lui signaler, voire contester le prélèvement.

Vous avez un délai maximum de 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).

Quel remboursement ?

En cas de paiement non autorisé, et sauf fraude ou négligence grave de votre part, **votre banque vous remboursera le prélèvement débité à tort**, au plus tard, à la fin du 1er jour ouvrable suivant. La banque rétablira votre compte dans l'état où il serait si l'opération n'avait pas eu lieu.

5. L'accès à sa banque et opérations à distance

Pour plus de sécurité contre les fraudes, une **authentification forte** s'ajoute à vos codes d'accès habituels lors de la connexion à la banque à distance, des paiements et des opérations sensibles.

En plus de votre identifiant et mot de passe, un élément sera exigé : une information que vous connaissez ou une caractéristique biométrique (voix, visage, empreinte digitale) ou encore l'usage d'un appareil que vous possédez (téléphone portable, montre connectée ou fourni par votre banque).

Consultez notre vidéo dédiée pour en savoir plus sur l'authentification forte.

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). Il comporte un lien vers son site Internet. L'objectif est d'y récupérer des informations personnelles **pour usurper** ensuite **votre identité**. C'est ce qu'on appelle du « **phishing** » ou « hameçonnage ».

Sur un faux site de banque, l'escroc tentera de récupérer vos données d'accès : identifiant et mot de passe. Sur un faux site commerçant, il visera à récupérer vos données de paiement.

Contre le phishing, 2 réflexes sont essentiels :

- **Ne jamais cliquer sur un lien envoyé par email ou SMS (y compris QR code) pour se connecter à sa banque.** Saisissez vous-même l'adresse du site de votre banque dans la barre d'url.

- **Ne jamais communiquer vos données de paiement ou vos codes d'accès à votre banque en ligne** à qui que ce soit. Même votre banque n'a pas à les connaître.

Comment réagir ?

- Au moindre doute sur un site, contactez votre banque. Sans attendre ses instructions, **utilisez un autre terminal informatique pour changer vos codes d'accès** de banque à distance, puis vérifiez les dernières opérations effectuées.
  En effet, s'ils ont accès à vos comptes à distance, les pirates peuvent procéder à des virements ou, en récupérant vos codes BIC et IBAN, mettre en place des prélèvements SEPA.
- Vous avez fourni à un tiers vos codes d'accès à votre espace de banque à distance ou des éléments sur vos moyens de paiement ? Vous constatez des débits frauduleux sur votre compte ? **Contactez immédiatement votre banque** aux coordonnées habituelles (n'utilisez pas celles du message que vous venez de recevoir) afin de signaler les opérations frauduleuses. Le cas échéant, **déposez plainte** au commissariat de police ou à la gendarmerie la plus proche, ainsi que sur la plateforme Thésée (service-public.fr).

Quel remboursement ?

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

La perte ou le vol de vos codes d'accès à la banque à distance ou des autres données personnelles de sécurité

Vous risquez qu'une autre personne les utilise à votre insu pour réaliser un paiement depuis 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 tapant son adresse sans faute.
- 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 personnelles de sécurité ont été utilisés, avant tout remboursement 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.**

Les fraudes courantes à (re)connaître

De plus en plus organisées et abouties, les fraudes prospèrent notamment via Internet et les réseaux sociaux. Les escrocs cherchent à vous **manipuler**, en jouant sur vos émotions, pour vous faire réaliser des paiements à leur profit.

Ils utilisent par exemple :

- 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… ;
- l'**empathie** : le besoin d'être solidaire, utile, de participer à l'effort collectif…

Tout message, appel téléphonique ou bannière publicitaire doit donc vous alerter s'il 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.**

Pour gagner votre **confiance** et être **crédibles**, les escrocs surfent le plus souvent sur l'**actualité**, par exemple les différentes aides que l'État a pu mettre en place. **Ils se font passer pour des grandes entreprises, des organismes ou administrations publics** connus et utilisent des adresses de messagerie ou des sites à leurs noms : **Caf, impôts, banques, fournisseurs d'énergie ou d'Internet, entreprises de livraison de colis, etc.**

La fraude au conseiller bancaire

Les circonstances

Vous recevez **un appel de votre banque**, parfois même avec le numéro de votre banquier affiché. La personne vous donne de nombreuses informations sur votre compte et vos habitudes. Elle **vous informe que des paiements suspects viennent d'être effectués sur votre compte…**

Elle vous rassure en vous indiquant que vous allez pouvoir rapidement régulariser cela ensemble. Elle **vous demande** alors **d'agir directement sur votre téléphone** ou de donner certaines informations : identifiant de connexion bancaire, code ou mot de passe d'activation, ou encore code de sécurité pour valider des opérations en ligne.

Où est le piège ?

L'escroc peut obtenir votre adresse, celle de votre agence, votre numéro de compte ou de carte, etc. via les réseaux sociaux ou un email de phishing. Avec ces informations, il est alors crédible lorsqu'il se fait passer pour votre banque, au téléphone.

ATTENTION **Avec l'essor de l'intelligence artificielle, les escrocs peuvent générer la voix, voire l'apparence de votre conseiller bancaire, pour vous contacter par téléphone ou en visio. C'est ce qu'on appelle un deepfake.**

En réalité, **au lieu d'annuler les opérations suspectes, vous en effectuez des nouvelles, à son profit.** Autrement dit, il vous fait procéder à l'authentification forte et vous autorisez ainsi les opérations. Et si vous lui donnez des informations personnelles (cryptogramme, codes d'accès de banque à distance, ou code SMS de validation…) il va pouvoir les réaliser lui-même.

Comment l'éviter ?

- **Raccrochez !** Si vous avez le réflexe, enregistrez l'appel pour le fournir ensuite aux autorités. Ne donnez jamais suite à une telle demande.

- **Contactez votre banque** aux coordonnées habituelles pour lui signaler cet appel suspect et vérifier ensemble l'état de votre compte.
- **Vérifiez les activités récentes** sur vos comptes en ligne et **les dernières opérations** passées.

ATTENTION L'authentification forte ne permet jamais d'annuler des paiements. Elle permet d'autoriser leur exécution ou l'ajout d'un bénéficiaire, l'augmentation de plafond… Votre banque ne vous demandera jamais ni vos codes d'accès, ni vos codes de validation.

La fraude au coursier

C'est une variante de la fraude au conseiller bancaire. En général, un phishing préalable permet à l'escroc de récupérer des informations sur vous, votre compte… en se faisant passer par exemple pour la sécurité sociale, Colissimo, etc.

Les circonstances

En apparence, **votre conseiller vous appelle ou vous envoie un SMS**. Le numéro semble bien être le sien. Il vous alerte sur le fait que **votre carte bancaire paraît compromise par une fraude**. Il vous informe qu'un coursier viendra la récupérer à votre domicile (souvent en soirée). Pour gagner votre confiance, il vous communique un code que le coursier devra vous donner et vous assure qu'une nouvelle carte vous sera envoyée sous peu.

Où est le piège ?

L'appel ou le SMS usurpe l'identité de votre banque. En réalité, un faux coursier viendra à votre domicile récupérer la carte bancaire soi-disant compromise. L'escroc tentera de récupérer votre code confidentiel, voire les codes de sécurité ou de validation des opérations à distance. Ce coursier vous fera croire qu'il détruit la carte devant vous.

Comment l'éviter ?

Ne confiez jamais ni votre carte ni votre code confidentiel à quiconque et ne divulguez pas les codes d'activation ou de sécurité que vous recevez. **Votre banque ne vous demandera jamais ces informations.**

La fraude aux coordonnées bancaires ou fraude au RIB

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**) 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 un nouveau RIB par courrier électronique le plus souvent, depuis une adresse de messagerie quasi identique à celle de votre interlocuteur habituel.

Comment l'éviter ?

Ce type de fraude cible tant les entreprises que les particuliers. Comme **un ordre de virement ne peut pas être annulé**, la somme ne peut pas être restituée par un transfert en sens inverse. Vous devez donc être particulièrement vigilant dès qu'il s'agit de RIB.

Assurez-vous de la véracité de la démarche en contactant la personne (ou organisme) au numéro de téléphone (ou adresse) que vous utilisez habituellement ou en trouvant vous-même les cordonnées.

Le chantage à la webcam

Les circonstances

Une personne malveillante vous fait croire qu'elle détient des photos ou des vidéos compromettantes de vous et vous fait du **chantage**. Elle vous menace notamment 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 et ont ainsi une certaine probabilité de récupérer des paiements, en comptant sur la panique des personnes ciblées. Payer ne vous protègerait de rien.

Comment l'éviter ?

Ne vous laissez pas impressionner par les messages alarmants, même si vous utilisez parfois 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.**

Le ransomware

Les circonstances

Pendant que vous utilisez votre ordinateur ou téléphone, l'écran se bloque d'un coup sur un message alarmant et insistant. Il vous indique qu'il « est bloqué et vos données inaccessibles. Vous ne pourrez les récupérer qu'en payant une **rançon**. 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** : vos fichiers, documents, images, vidéos… sont chiffrés et en quelque sorte pris en otage ;
- **locker** : l'accès à votre ordinateur (ou à certaines fonctionnalités de celui-ci) vous est refusé.

Souvent le ransomware infecte votre matériel via un fichier téléchargé sur Internet ou reçu par email. Le courriel peut aussi inclure une pièce jointe piégée, un lien ou un QR code vers un site malveillant.

Comment l'éviter ?

- **Ne cliquez jamais sur une pièce jointe ou un lien de provenance inconnue ou douteuse.**
- Ayez toujours un **antivirus à jour**, y compris sur votre smartphone et tablette.
- **Ne payez jamais** 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 : Votre ordinateur ou smartphone est bloqué. Un message demande d'appeler un numéro de téléphone afin de télécharger un logiciel pour débloquer l'appareil. N'appelez jamais ce numéro et ne téléchargez rien. Il suffit souvent de redémarrer le poste pour que celui-ci fonctionne à nouveau.

Le faux prêt

Les circonstances

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 ?

En récupérant tous les éléments de votre demande de rachat de crédit, les escrocs vont pouvoir **usurper votre identité et se faire octroyer un crédit en ligne à votre place**. La somme est bien versée sur votre compte mais vous êtes recontacté ensuite pour la transférer vers un compte externe, soi-disant pour finaliser l'opération de rachat de crédit.

Comment l'éviter ?

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 serait pas cohérent avec les taux actuellement pratiqués.

La fraude au faux placement

Les circonstances

Vous pouvez être contacté par **mail** ou **téléphone**, voir une **publicité** en ligne ou sur les réseaux sociaux, via le compte d'influenceurs. **Le placement est proposé avec une très forte rentabilité, un taux d'intérêt très élevé et des revenus garantis.** Si vous donnez suite, vous recevez des documents et/ou vous êtes redirigé vers un site Internet pour renseigner vos informations personnelles et bancaires.

Où est le piège ?

L'escroc se fait passer pour un établissement de crédit, une banque ou encore un courtier. La fraude repose (encore une fois) sur l'usurpation d'identité. Le site vers lequel on est renvoyé inspire confiance en utilisant des mentions légales, le nom et le logo d'une banque ou d'un établissement financier connu, etc.

Variante : Pour un faux livret, il suffit de verser les 1ers dépôts pour percevoir au plus vite les intérêts promis. La fraude fonctionne de la même façon pour les placements financiers : diamants, champagne, vin, cryptoactifs, etc.

Comment l'éviter ?

Au moindre doute, utilisez l'**application AMF protect épargne** et consultez **les listes blanches et noires de l'AMF**.

La fraude au faux test technique

Les circonstances

Les services techniques de la banque, son service fraude ou sécurité, vous contactent et **demandent d'effectuer des tests ou** encore **vous offrent 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 d'escrocs qui 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. Suivre leurs instructions, c'est leur donner accès aux informations et à votre espace de banque en ligne.

Comment l'éviter ?

Différez l'intervention, mettez fin aux échanges 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.

Votre banque ne vous contactera jamais pour faire un test technique ou de virement. **Soyez particulièrement suspicieux si la demande est urgente, insistante, voire menaçante, le montant élevé et le virement demandé à destination de l'étranger.**

La fraude aux sentiments

Les circonstances

Vous êtes inscrit sur un site de rencontre ou via les réseaux sociaux.

Où est le piège ?

Les fraudeurs prennent leur temps pour instaurer la confiance et nouer une relation. À mesure des échanges, parfois sur plusieurs mois, votre vigilance s'estompe. Utilisant de fausses identités et photos, ils inventent des **histoires de proches en détresse** médicale ou financière par exemple, pour vous manipuler et tenter de vous soutirer de l'argent. **Une fois l'argent envoyé, ils disparaissent du réseau ou site de rencontre.**

Comment l'éviter ?

- Restez vigilant et méfiez-vous des rencontres idylliques en ligne.
- Ne donnez pas trop de renseignements personnels sur les réseaux sociaux et les sites de rencontre.
- **Ne donnez jamais aucune indication sur vos données bancaires.**
- **N'envoyez jamais d'argent. N'acceptez pas non plus d'en recevoir** par exemple en encaissant un chèque en échange d'un transfert d'argent ou de cartes prépayées. Il s'agirait sûrement d'un chèque sans provision ou d'un chèque volé.

Les arnaques sur les réseaux sociaux

Les circonstances

Vous êtes inscrit sur des réseaux sociaux. Une multitude de sollicitations apparaît chaque jour. Parfois, il s'agit de **promesse d'argent facile**, travail surrémunéré, 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 en ligne.

Variante : 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).

En soi, c'est simple et tentant : il suffit de donner son IBAN pour récupérer l'argent, augmenté de votre commission, puis de reverser le montant comme demandé. En réalité, si votre compte est bien crédité, c'est par un chèque qui se révèlera être un **faux ou un chèque sans provision. Votre compte sera donc finalement débité du montant, tandis que votre virement sera lui bien réalisé** et donc déduit de votre compte. Vous ne pourrez pas l'annuler. L'escroc disparaît bien sûr et son faux profil sur les réseaux sociaux est fermé.

Cette fraude est une version modernisée de la « fraude à la mule » (cf. page 39), c'est-à-dire réaliser un paiement à autrui pour le compte de quelqu'un d'autre à des fins de **blanchiment d'argent**. C'est être passible de poursuites judiciaires pour complicité.

Comment l'éviter ?

- Sur Internet et 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 publiées sont accessibles. Elles pourraient donc être récupérées par des personnes malveillantes même si vous pensez les réserver à votre cercle d'amis. Ajustez régulièrement les paramètres de confidentialité sur votre profil.

La fraude à l'offre d'emploi

Les circonstances

En recherche d'emploi, vous consultez de nombreux sites et réseaux en ligne. Les escrocs cherchent à **profiter de la situation et notamment de la détresse de certains demandeurs d'emploi.**

Où est le piège ?

Les fausses offres d'emploi, alléchantes ou très engageantes, se sont multipliées. Elles visent à **obtenir vos informations personnelles et à vous escroquer de l'argent.**

Comment l'éviter ?

De nombreux indices peuvent vous interpeller : salaire anormalement élevé, horaires très allégés ou travail peu laborieux, offre envoyée à des heures inhabituelles, expéditeur d'un autre pays ou continent, un envoi d'argent vous est demandé pour obtenir un entretien, un dossier de candidature ou au contraire, 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.

La fraude à la loterie

Les circonstances

Un mail, un SMS ou un appel vous informe que **vous avez gagné un prix. Il 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 vraisemblablement une arnaque.
Elle peut provenir d'un faux commerçant et/ou vous rendre complice d'une fraude.

Être finalement payé par chèque, voire plus que prévu

Les circonstances

Vous vendez un bien. L'acquéreur vous demande votre RIB 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.**

Variante : vous avez convenu de recevoir un chèque et l'acquéreur vous propose un prix supérieur en prétextant un service complémentaire (des frais de transport par exemple). Vous recevez un chèque pour l'ensemble, que vous encaissez. Annulant finalement le service supplémentaire, l'acquéreur vous demande son remboursement, par virement sur un compte de tiers ou transfert d'espèces à un tiers.

Où est le piège ?

Le chèque déposé était un **faux chèque**, il a donc été rejeté. Votre compte est débité. Au mieux, vous gardez votre bien mais vous perdez le montant soi-disant « remboursé ».

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. Avant de livrer le bien, vérifiez que votre compte est bien crédité par virement. **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.

Être 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** puis la transférer ensuite sur un autre compte qu'on vous indiquera.

Où est le piège ?

Il s'agit de promesse d'argent facile. Par ce transit d'argent, apparemment simple et sans risque, **l'escroc « blanchit » de l'argent** provenant probablement d'un trafic.

La fraude est difficile à détecter et la récupération des fonds quasi-impossible. 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.

Annexe – Tableau récapitulatif

MOYEN	FRAUDE/INCIDENT	RÉACTION
CARTE	Perte/vol de la carte	• Opposition rapide au numéro fourni par votre banque • Vérifier les opérations passées et les contester s'il y a lieu le plus rapidement possible • Plainte à la police/gendarmerie recommandée
CARTE	Détournement des données	• Opposition rapide au numéro fourni par votre banque • Vérifier les opérations passées et les contester s'il y a lieu le plus rapidement possible • Plainte à la police/gendarmerie recommandée
CHÈQUE	Perte/vol chèque vierge	• Opposition rapide via les moyens de communication mis à disposition par votre banque • Plainte à la police/gendarmerie recommandée
CHÈQUE	Perte/vol chèque signé et falsifié	• Opposition rapide via les moyens de communication mis à disposition par votre banque • Plainte à la police/gendarmerie recommandée
VIREMENT	Erreur involontaire d'IBAN	• Alerter rapidement votre banque qui pourra adresser une demande de rappel de fonds à l'autre banque • À défaut de remboursement, récupération des informations pour que vous puissiez exercer un recours contre le bénéficiaire du virement

REMBOURSEMENT	RÉSERVE ÉVENTUELLE
• Si débit, sans utilisation du code, remboursement intégral • Si débit avec utilisation de votre code ou données personnelles de sécurité avant opposition, franchise de 50 € et remboursement au-delà	Si de votre part, opposition tardive, négligence grave ou intentionnelle, ou fraude
Analyse au cas par cas par la banque des circonstances de la fraude, avec remboursement le cas échéant.	Si de votre part, opposition tardive, contestation tardive, négligence grave ou intentionnelle, ou fraude
Remboursement du faux chèque, dont vous n'êtes pas l'auteur	Si de votre part, opposition tardive ou vérification tardive des relevés de compte
• Responsabilité de la banque en cas de faute dans le traitement du chèque (altération, surcharge apparente…) • Responsabilité partagée si négligence de votre part	Si opposition tardive
Rappel de fonds par votre banque ou action en justice à mener contre le bénéficiaire du virement	

MOYEN	FRAUDE/INCIDENT	RÉACTION
VIREMENT	Fraude à l'IBAN	• Alerter rapidement votre banque qui pourra adresser une demande de rappel de fonds à l'autre banque • À défaut de remboursement, récupération des informations afin que vous puissiez exercer un recours contre le bénéficiaire du virement
PRÉLÈVEMENT	Fraude à l'IBAN	Alerter rapidement votre banque et au maximum dans les 13 mois du prélèvement non autorisé
ACCÈS BANQUE À DISTANCE	Si codes d'accès ou autres données personnelles de sécurité fournis ou détournés/ ou si débit constaté (ex : cas de phishing)	• Signaler rapidement l'incident à votre banque • Changer les codes et le cas échéant les autres données personnelles de sécurité • Plainte à la police/ gendarmerie recommandée • Signaler l'incident sur internet-signalement.gouv.fr
ACCÈS BANQUE À DISTANCE	Perte/vol des codes d'accès/autres données personnelles de sécurité	• Changer vos codes d'accès, depuis un autre terminal sécurisé • Signaler rapidement l'incident à votre banque

REMBOURSEMENT	RÉSERVE ÉVENTUELLE
Rappel de fonds par votre banque ou action en justice à mener conte le bénéficiaire du virement	
Le remboursement s'effectue, au plus tard, à la fin du 1er jour ouvrable suivant votre demande. Votre compte est rétabli dans l'état où il serait si l'opération n'avait pas eu lieu	Si de votre part, fraude ou négligence grave
Analyse au cas par cas, par votre banque, des circonstances de la fraude. Remboursé par la banque en l'absence de négligence grave de votre part	Si de votre part, négligence grave ou intentionnelle, ou fraude
Remboursement	Si négligence grave ou intentionnelle, ou fraude du client

lesclesdelabanque.com

FÉDÉRATION
BANCAIRE
FRANÇAISE