Fraudes aux opérations bancaires :

COMPRENDRE, ÉVITER, RÉAGIR

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

Le présent guide est exclusivement diffusé à des fins d'information du public. Il ne saurait en aucun cas constituer une quelconque interprétation de nature juridique de la part des auteurs et/ou de l'éditeur. Tous droits réservés. La reproduction totale ou partielle des textes de ce guide est soumise à l'autorisation préalable de la Fédération Bancaire Française.

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 : octobre 2026

SOMMAIRE

Introduction 2

Comprendre les fraudes bancaires et les reconnaître 3

Pourquoi les fraudes bancaires sont-elles de plus en plus convaincantes ? 4

Comment reconnaître une tentative de fraude ? 8

Quelles sont les principales fraudes visant les comptes et les paiements ? 11

Réagir en cas de doute ou de fraude 21

Je vérifie avant d'agir 22

J'ai reçu une demande suspecte (appel, message, etc.) 24

J'ai déjà cliqué ou communiqué une information ou validé une opération 26

Je constate une opération suspecte sur mon compte 29

Mémos pratiques 31

Tableau des situations fréquentes 32

Connaître ses droits et les démarches 34

Puis-je être remboursé en cas de fraude ? 35

Faut-il déposer plainte ? 38

Pourquoi utiliser les plateformes de signalement ? 39

Conclusion 40

Annexe – Tableau récapitulatif 41

Introduction

Les services bancaires à distance et les moyens de paiement numériques font partie du quotidien. Consulter ses comptes, effectuer un virement ou régler un achat en ligne se fait souvent depuis un ordinateur ou un téléphone mobile.

Si de nombreux dispositifs de sécurité existent, leur efficacité repose aussi sur la vigilance de chacun. Les fraudeurs utilisent aujourd'hui des techniques toujours plus élaborées pour convaincre leurs victimes d'agir.

Ce guide pratique vous aide à mieux comprendre les méthodes utilisées par les escrocs, à repérer les situations qui doivent alerter et à adopter les bons réflexes selon le contexte : avant d'agir, en cas de doute, après une opération suspecte ou lorsqu'une démarche de contestation doit être engagée.

Comprendre les fraudes bancaires et les reconnaître

Comprendre les mécanismes les plus courants, repérer les signaux d'alerte et connaître les principales techniques utilisées aujourd'hui permet d'adopter les bons réflexes et de réduire les risques.

Pourquoi les fraudes bancaires sont-elles de plus en plus convaincantes ?

Des données et informations personnelles déjà connues des fraudeurs

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. **Codes, mots de passe et identifiants bancaires : ne donnez jamais ces données !**

Mais aujourd'hui, cela ne suffit plus : des fuites de données ont déjà touché des organismes de tous secteurs. Des informations telles que votre nom, votre numéro de téléphone, votre adresse électronique ou certaines données vous concernant peuvent alors être récupérées et utilisées par des fraudeurs. Ces informations leur permettent de personnaliser leurs messages ou leurs appels et de rendre leurs sollicitations plus convaincantes.

Le fait qu'une personne dispose d'informations exactes vous concernant ne prouve ni son identité ni la légitimité de sa démarche.

Des techniques de manipulation psychologique sophistiquées

Les fraudeurs ne cherchent pas toujours à contourner techniquement les systèmes de sécurité. Ils cherchent souvent à vous convaincre d'agir vous-même : communiquer une information, cliquer sur un lien, effectuer un paiement ou valider une demande d'authentification.

Pour y parvenir, les fraudeurs exploitent des mécanismes psychologiques en s'appuyant sur des émotions et des comportements humains :

- **la peur** : en évoquant la perte d'argent, la suppression d'un droit ou le risque de de manquer une occasion ;
- **l'appât du gain ou l'envie** : en promettant un avantage, un remboursement, une opportunité exclusive ;
- **la crainte ou le respect de l'autorité** : en se présentant comme un conseiller, une administration, un service de sécurité ou toute autre personne en position d'autorité ;
- **l'empathie** : en suscitant la compassion, la solidarité, l'envie d'aider une personne en difficulté ;
- **la proximité** : en se faisant passer pour un proche, un collègue, un ami ou une personne de confiance ;
- **la flatterie et l'orgueil** : en valorisant la vigilance, l'intelligence ou l'esprit critique de la victime afin de gagner sa confiance et l'amener à baisser sa garde.

Ne réalisez que les opérations que vous avez vous-même décidées et dont vous comprenez parfaitement l'objet. Une demande d'authentification sert toujours à autoriser une opération, jamais à l'annuler, la bloquer ou à sécuriser un compte.

La fraude par manipulation atteint ainsi 516 millions d'euros en 2025, soit un peu plus de 40 % du montant annuel total de fraude aux moyens de paiement – une proportion qui a doublé en quatre ans.
(Observatoire sur la Sécurité des Moyens de Paiement)

L'usurpation d'identité facilitée par l'IA (deepfakes vocaux et vidéos)

L'intelligence artificielle permet aujourd'hui de générer rapidement des messages, des documents, des images, et même des messages vocaux et des vidéos réalistes à partir d'extraits disponibles en ligne.

Avec les informations disponibles sur Internet, les réseaux sociaux ou issues de fuites de données (nom, numéro de téléphone ou certains éléments de votre situation), un escroc peut donc facilement se faire passer pour un de vos proches ou encore une société ou un organisme connu (caf, impôts, banquier, etc.) pour obtenir votre confiance.
Il devient beaucoup plus difficile de distinguer une demande légitime d'une tentative de fraude.

La voix ou l'image d'une personne ne constituent plus, à elles seules, une preuve de son identité. Ce qui doit notamment vous alerter, au-delà du caractère urgent, c'est l'incohérence entre la demande et la relation habituelle que vous entretenez avec l'interlocuteur.

Exemples : Vous reconnaissez la voix ou l'image d'une personne mais…

- la qualité audio ou vidéo vous paraît légèrement étrange, irrégulière ou artificielle ;
- sa demande ne correspond pas aux habitudes de la personne ou de l'organisme concerné ;
- vous ne disposez d'aucun moyen de vérifier ce qui vous est demandé ou l'interlocuteur refuse certaines vérifications ;
- il semble connaître de nombreuses informations personnelles vous concernant sans que vous sachiez comment il les a obtenues ;
- le message, crédible et parfaitement rédigé, vous pousse à agir rapidement…

Une fraude multicanale et séquencée : SMS, courriel, téléphone et application bancaire

Les fraudeurs combinent maintenant plusieurs moyens de communication pour renforcer leur crédibilité. Un même scénario peut ainsi associer un courriel, un SMS, un appel téléphonique ou une demande de validation dans une application, donnant l'impression que différentes sources confirment la même information rendant ainsi le scénario plus crédible.

Par exemple, vous pouvez recevoir :

- un courriel ;
- puis un SMS, ou message WhatsApp ;
- puis un appel téléphonique ;
- avant une demande de validation dans votre application bancaire.

Toutes ces sollicitations sont liées et font partie d'une même tentative de fraude.

Le fait qu'une information soit relayée par plusieurs canaux de communication ne garantit pas qu'elle soit authentique. Vérifiez toujours la situation en utilisant un numéro ou un moyen de contact que vous choisissez vous-même.

Comment reconnaître une tentative de fraude ?

Les signaux d'alerte les plus fréquents

Les fraudes bancaires peuvent avoir des formes, des canaux et des objectifs différents, (obtenir vos codes de sécurité, détourner un paiement, vous convaincre d'effectuer vous-même un virement…). Pourtant, derrière ces scénarios très variés, les fraudeurs utilisent souvent les mêmes méthodes.

Ils cherchent généralement à créer un sentiment d'urgence, à susciter la peur ou à inspirer confiance afin de vous pousser à agir rapidement sans prendre le temps de vérifier.

Soyez particulièrement vigilant dès que :

- la demande est :
  - urgente ;
  - alarmante, ou au contraire rassurante ;
  - inhabituelle ;
  - en rapport avec l'étranger ;
- elle concerne vos codes, mots de passe ou identifiants, une mesure de sécurité ;
- ou encore si vos informations personnelles sont particulièrement mises en avant.

Si vous n'êtes pas à l'origine de l'échange, prenez toujours le temps de vérifier par le canal de communication que vous utilisez habituellement avec votre interlocuteur.

Prévention : 8 bonnes pratiques

Si aucune solution ne permet d'éliminer totalement le risque de fraude, certains réflexes simples permettent de réduire les risques.

Je ne communique jamais mes codes.

Code confidentiel de votre carte, codes reçus par SMS, identifiants de connexion, mots de passe ou codes de validation : ces informations sont strictement personnelles.
Personne n'a à vous les demander, même votre banque.

Je ne valide que les opérations que j'initie moi-même.

Certaines opérations nécessitent une confirmation de votre part dans votre application bancaire ou au moyen d'un dispositif de sécurité.
Une validation doit uniquement servir à confirmer une action que vous avez vous-même décidée.

Je prends mon temps.

Les fraudeurs exigent très souvent une réaction rapide pour empêcher toute vérification (risque supposé sur votre compte, paiement présenté comme urgent, menace de blocage, problème à résoudre immédiatement…).

Je vérifie l'identité de mon interlocuteur.

L'usurpation d'identité est largement utilisée dans les fraudes.
Caf, impôts, banques, fournisseurs d'énergie ou d'Internet, entreprises de livraison de colis, etc., que ce soit par téléphone, SMS, courriel, message ou site Internet, l'apparence ne garantit pas l'identité réelle de l'interlocuteur.

Je contrôle les coordonnées bénéficiaires avant un virement.

Avant un 1er paiement ou un changement de coordonnées bancaires, vérifiez toujours les informations communiquées auprès du bénéficiaire par un canal que vous connaissez déjà.
Si la banque signale une non-concordance entre le nom du bénéficiaire que vous avez renseigné sur l'ordre de virement Sepa et le nom associé à l'IBAN, ne validez pas sous la pression. Suspendez l'opération pour effectuer les vérifications nécessaires.
Une concordance exacte réduit certains risques, mais ne garantit pas que la demande de paiement elle-même est légitime.

Je protège mes appareils et mes informations personnelles.

Ordinateur, tablette et téléphone… La sécurité de vos équipements participe à la protection de vos comptes. Effectuez les mises à jour, utilisez des mots de passe robustes, verrouillez vos appareils et téléchargez les applications depuis des sources officielles.
Limitez la diffusion de vos informations personnelles et vérifiez à qui vous les communiquez. Car nom, adresse, date de naissance, numéro de téléphone ou adresse électronique peuvent être utilisés pour personnaliser une tentative de fraude.
Vous ne devez pas permettre à des tiers d'accéder à vos appareils via des éléments de biométrie en ajoutant une empreinte ou un face ID qui ne vous appartient pas. Ils pourraient permettre la validation d'opération de paiement ensuite.

Je consulte régulièrement mes comptes pour réagir rapidement.

La régularité permet de détecter plus rapidement une anomalie ou une opération inhabituelle. Il est alors plus facile d'en limiter les conséquences.
Selon la situation, vous pouvez notamment contacter votre établissement bancaire, modifier vos accès, faire opposition, signaler les faits.

Je me tiens informé des alertes de sécurité.

Consultez régulièrement les informations et recommandations de sécurité diffusées par votre établissement bancaire. Elles permettent d'être alerté des nouvelles fraudes et des méthodes actuellement utilisées par les escrocs. Et restez aussi attentif aux messages de votre banque, tel que « une dépense importante arrive sur votre compte » par exemple.

Pour aller plus loin, retrouvez notre collection de guides Sécurité

Quelles sont les principales fraudes visant les comptes et les paiements ?

Les tentatives de fraude peuvent prendre des formes très différentes. Certaines cherchent à obtenir vos identifiants ou vos codes de sécurité. D'autres visent à détourner un paiement ou à vous convaincre de réaliser un virement. Comprendre les mécanismes utilisés et les objectifs poursuivis par les fraudeurs permet de mieux repérer les situations à risque et d'adopter les bons réflexes.

1. Ils cherchent à obtenir vos codes ou vos validations

Les messages et liens frauduleux : phishing, smishing et quishing

Le fraudeur cherche à vous attirer vers un site frauduleux (copie d'un site habituel ou connu) pour que vous y communiquiez des informations sensibles (données personnelles, identifiants, codes de sécurité) ou que vous y réalisiez une opération.

Il peut utiliser différents moyens pour vous adresser le lien frauduleux : courriel (phishing), SMS (smishing), QR code (quishing).

Le message peut invoquer de multiples prétextes pour vous faire cliquer sur le lien/scanner le QR code, par exemple :

- compte à mettre à jour pour éviter blocage ou suspension de service ;
- opération à confirmer ;
- colis à récupérer ;
- paiement refusé ;
- remboursement à percevoir ;
- document à consulter…

Exemple : vous recevez une carte présentée comme une nouvelle carte bancaire, accompagnée d'un QR code à scanner pour l'activer.

Les signaux d'alerte

- message inattendu ou inhabituel ;
- demandant une action via lien internet ou QR code à utiliser ;
- avec une adresse d'expéditeur inconnue ou inhabituelle.

Ce qu'il faut retenir

Ne cliquez jamais sur un lien ou un QR code reçu dans un message inattendu. Un acteur légitime vous encouragera toujours à vous connecter de vous- même directement sur son site à l'adresse habituelle.

Et si vous avez cliqué trop vite, ne communiquez jamais vos identifiants, vos mots de passe ou vos codes de sécurité.

Le faux conseiller bancaire (spoofing)

Un fraudeur vous contacte en se faisant passer pour un conseiller bancaire, un service de sécurité ou un service de lutte contre la fraude. Pour renforcer sa crédibilité, il utilise un numéro de téléphone qui semble correspondre à celui de votre établissement bancaire. Cette usurpation de numéro de téléphone s'appelle le spoofing.

Au cours de l'échange, le fraudeur affirme généralement qu'une opération suspecte est en cours sur votre compte ou que celui-ci est menacé. Il cherche ensuite à vous convaincre de :

- communiquer des informations de sécurité ;
- valider une opération (ajout de bénéficiaire ou virement) via votre dispositif de sécurité.

Exemple : Le fraudeur affirme qu'un paiement suspect est en cours ; il vous demande de l'annuler en « validant l'opération » notamment via un dispositif d'authentification. Or, ce type de dispositif est toujours utilisé pour autoriser une opération mais jamais pour l'annuler ou la bloquer.

Les signaux d'alerte

- appel inattendu d'un numéro semblant correspondre à celui de votre banque ;
- demande de validation/confirmation pour annuler une opération ;
- demande d'informations confidentielles ;
- pression pour agir immédiatement ;
- interlocuteur qui décourage toute vérification.

Ce qu'il faut retenir
Le numéro affiché lors d'un appel ne garantit pas l'identité réelle de votre interlocuteur. Ni votre banque, ni un service de sécurité ne vous demanderont de communiquer vos codes ou de valider une opération pour en annuler une autre.

Dans ce cas, raccrochez et contactez votre banque en utilisant ses coordonnées habituelles.

Le faux numéro d'opposition bancaire

Un SMS ou courriel vous informe d'un achat, d'un virement ou d'une autre opération bancaire que vous ne reconnaissez pas. Le message indique un numéro de téléphone à appeler rapidement pour empêcher le paiement.

En réalité, ce numéro ne correspond pas à un service officiel d'opposition. Un fraudeur s'y présente comme un conseiller d'un service de sécurité ou de lutte contre la fraude. Il cherche alors à vous convaincre de communiquer des informations personnelles ou bancaires, de lui transmettre un code de sécurité, de valider une opération dans votre application bancaire ou d'effectuer une prétendue manipulation destinée à protéger votre compte.

Exemple : un SMS annonce un paiement important et vous demande de confirmer que vous en êtes bien à l'origine. Et si ce n'est pas le cas, il vous invite à appeler un numéro pour faire opposition.

Les signaux d'alerte
- message signalant une opération anormale ;
- demandant d'appeler de manière urgente un numéro pour faire opposition ;
- interlocuteur demandant des codes, des informations confidentielles ou une validation ;
- pression pour agir immédiatement sans vérification auprès de votre banque.

Ce qu'il faut retenir
N'appelez jamais un numéro de téléphone indiqué dans un message inattendu. Vérifiez vos opérations dans votre espace bancaire en ligne puis contactez vous-même votre banque à ses coordonnées habituelles.

Le faux support technique

Vous êtes informé d'un prétendu problème informatique. Le fraudeur vous invite à installer un logiciel ou à lui permettre d'accéder à votre appareil.

Les signaux d'alerte

- apparition d'un message alarmant ;
- demande d'accès à distance ;
- proposition d'assistance immédiate.

Ce qu'il faut retenir

Votre banque ne vous contactera jamais pour faire un test technique ou de virement. Elle n'a pas besoin de vous pour cela. Ne donnez jamais à un tiers un accès à distance à votre appareil sans avoir vérifié son identité.

Le détournement de numéro de téléphone (SIM swapping)

Le fraudeur utilise vos informations personnelles et se fait passer pour le titulaire de votre ligne auprès de votre opérateur téléphonique. Il parvient ainsi à faire transférer votre numéro de téléphone mobile vers une nouvelle carte SIM qu'il contrôle. Il peut alors recevoir vos appels, SMS et codes de sécurité afin d'accéder à vos comptes ou de réaliser certaines opérations.

Les signaux d'alerte

- votre téléphone perd soudainement le réseau mobile sans raison apparente ;
- vous ne pouvez plus émettre ou recevoir d'appels et de SMS alors que votre appareil fonctionne normalement ;
- vous recevez des notifications inhabituelles concernant votre ligne téléphonique mobile ;
- vous constatez des demandes de réinitialisation de mots de passe que vous n'avez pas effectuées ;
- des opérations ou tentatives de connexion apparaissent sur vos comptes sans votre intervention.

Ce qu'il faut retenir

Si votre ligne cesse brusquement de fonctionner ou présente des anomalies, contactez rapidement votre opérateur téléphonique et surveillez les services utilisant votre numéro de téléphone pour l'authentification. Informez votre banque.

2. Ils cherchent à vous faire effectuer un paiement

L'usurpation d'identité d'un proche

Le piratage de compte de messagerie ou de numéro de téléphone permet à un fraudeur de se faire passer pour un membre de votre famille ou un proche pour solliciter une aide financière urgente.

Les signaux d'alerte

- changement soudain de numéro ou d'email ;
- demande d'argent urgente ;
- ton ou langage employé inhabituel ;
- impossibilité de joindre la personne.

Exemple : le message WhatsApp type « Maman c'est moi. J'ai perdu mon téléphone. J'ai besoin d'argent ».

Ce qu'il faut retenir

Un message avec une adresse d'expéditeur correcte ne garantit pas l'identité de la personne. Vérifiez toujours la demande par un autre moyen.

Le faux achat ou la fausse vente en ligne

Le fraudeur se présente comme vendeur (ou acheteur) et cherche à récupérer un paiement (ou des données bancaires) en dehors de la plateforme officielle.

Les signaux d'alerte

- demande inhabituelle ;
- procédure de paiement complexe/à l'étranger ;
- pression pour agir rapidement.

Ce qu'il faut retenir

Utilisez toujours les dispositifs de paiement proposés par la plateforme utilisée.

La fraude au RIB

Les coordonnées bancaires du bénéficiaire que vous souhaitez créditer sont modifiées à votre insu (ou à l'insu de votre bénéficiaire) afin que votre virement soit envoyé sur le compte du fraudeur.

Les signaux d'alerte

- changement inattendu de coordonnées ;
- demande de dernière minute ;
- nouvelle banque/nouveau compte.

Ce qu'il faut retenir

Le service de vérification du nom du bénéficiaire pour les ordres de virement Sepa peut permettre de détecter dans certains cas ce type de fraude mais il ne dispense pas de vérifier une demande inattendue de changement de coordonnées. Vérifiez les coordonnées bancaires par un canal différent avant tout premier virement.

Cette fraude se perfectionne encore. Les fraudeurs ne se contentent plus d'envoyer un simple changement de coordonnées bancaires. Ils détournent aussi désormais des boîtes mail et falsifient des documents.

Le faux chèque ou la remise de chèque frauduleuse

On vous remet un chèque en paiement, d'un montant supérieur à la somme convenue. Puis, on vous demande de reverser rapidement la différence. Seulement, le chèque est finalement rejeté (faux, falsifié, volé ou sans provision). En règle générale, un chèque est crédité sous réserve d'encaissement : s'il revient impayé, la somme d'abord créditée sera finalement débitée de votre compte. Cette situation vous porte préjudice si, entretemps, vous avez reversé tout ou partie du montant du chèque.

Les signaux d'alerte

- montant supérieur au montant convenu ;
- demande de remboursement rapide ;
- offre d'emploi impliquant l'encaissement d'un chèque ;
- demande de reverser une partie des fonds par virement ou par retrait d'espèces ;
- interlocuteur qui refuse un autre moyen de paiement.

Ce qu'il faut retenir

Méfiez-vous lorsqu'une personne vous demande de lui reverser tout ou partie d'une somme provenant d'un chèque que vous venez d'encaisser. Cela peut vous porter préjudice voire engager votre responsabilité (compte de « mule », cf. plus loin).

Le faux placement financier

On vous promet un rendement élevé avec peu ou pas de risque.
On vous demande un premier versement rapide pour en profiter.

Les signaux d'alerte

- promesse de gain rapide ;
- pression commerciale ;
- performance exceptionnelle garantie/absence de risque confirmé par de nombreux avis (faux).

Ce qu'il faut retenir

Des rendements élevés s'accompagnent généralement d'un niveau de risque élevé. Au moindre doute, utilisez le site Internet ou l'application AMF Protect épargne et consultez les listes noires de l'AMF (listes des sites, plateformes et entités non autorisés à proposer des placements en France).

Le faux crédit

On vous propose un crédit à des conditions particulièrement avantageuses à condition de payer des frais au préalable.

Les signaux d'alerte

- frais demandés avant tout versement ou tout contrat formel ;
- promesses excessives ;
- absence de vérifications habituelles.

Ce qu'il faut retenir

Soyez vigilant lorsqu'un paiement est demandé avant la mise à disposition des fonds. Au moindre doute, consultez les agréments (Regafi, Orias) et la liste noire de l'ACPR.

La fraude sentimentale

Grâce aux réseaux sociaux, aux applications de rencontre et à l'IA générative, certaines escroqueries sentimentales sont aujourd'hui très élaborées.

Une relation apparemment de confiance (notamment sur les réseaux sociaux) se tisse au fil du temps avec un tiers rencontré sur ce canal. La relation peut durer plusieurs semaines ou plusieurs mois avant qu'une demande d'argent n'apparaisse.

Les signaux d'alerte

- demande d'aide financière ;
- situations d'urgence répétées ;
- refus de rencontre réelle, relation exclusivement à distance.

Ce qu'il faut retenir

Les demandes d'argent répétées, notamment de personnes jamais rencontrées physiquement, doivent vous alerter.

Ils cherchent à détourner vos moyens de paiement

Le prélèvement frauduleux

Un prélèvement est présenté sur votre compte sans mandat valable, par un créancier que vous ne connaissez pas. Vos coordonnées bancaires peuvent avoir été dérobées/utilisées pour créer un mandat de prélèvement frauduleux. Deux cas sont alors possibles : le bénéficiaire est le fraudeur lui-même ou le fraudeur usurpe votre identité pour donner le mandat de prélèvement auprès d'un commerçant légitime.

Les signaux d'alerte

- nom de créancier inconnu/référence de mandat inhabituelle ;
- petit montant récurrent inexpliqué ;
- prélèvement faisant suite à la communication récente d'un RIB.

Ce qu'il faut retenir

Contrôlez régulièrement vos prélèvements et signalez rapidement toute opération que vous ne reconnaissez pas.

Le skimming

Un dispositif frauduleux installé sur un distributeur ou un terminal de paiement enregistre les données de votre carte.

Les signaux d'alerte

- équipement endommagé ;
- élément inhabituel, sur l'automate ou le terminal de paiement ;
- clavier ou lecteur modifié.

Ce qu'il faut retenir

Soyez attentif à l'état des équipements que vous utilisez et privilégiez les distributeurs dans les espaces fermés. Au moindre doute, différez l'opération ou utilisez un autre distributeur.

Le détournement du paiement mobile

Le fraudeur tente d'obtenir :
- les données de votre carte bancaire ;
- des informations personnelles ;
- un code de sécurité ou de validation ;
- une authentification réalisée depuis votre téléphone.

Ces informations peuvent ensuite être utilisées pour ajouter votre carte à un portefeuille de paiement mobile ou pour autoriser des opérations frauduleuses.

Les signaux d'alerte
- réception inattendue d'un code de validation ;
- demande de communiquer un code reçu par SMS ou dans une application ;
- demande présentée comme une opération de sécurité ;
- notification concernant l'ajout d'une carte ou l'enregistrement d'un nouvel appareil ;
- opération ou paiement que vous ne reconnaissez pas.

Ce qu'il faut retenir
Ne communiquez jamais un code de validation reçu sur votre téléphone et ne confirmez jamais l'ajout d'une carte ou d'un appareil que vous n'avez pas vous-même demandé.

Exemples :

- Après une tentative de phishing ou de smishing : Vous saisissez vos informations sur un site frauduleux ou communiquez des données qui permettent ensuite au fraudeur d'initier l'ajout de votre carte sur un autre appareil.
- Après le vol de certaines données personnelles : Le fraudeur utilise plusieurs informations vous concernant pour tenter de contourner les contrôles de sécurité et enregistrer votre moyen de paiement.

3. Ils cherchent à utiliser votre compte bancaire

La mule financière / le faux emploi

Vous êtes sollicité pour recevoir de l'argent via votre propre compte bancaire pour le reverser sur un autre, moyennant une rémunération. Un escroc blanchit ainsi l'argent provenant de trafic ou d'opérations illicites.

Le faux emploi est un scénario de recrutement. Le fraudeur publie une annonce ou contacte une personne en lui proposant :

- un emploi à domicile ;
- une activité de gestion administrative ;
- une mission de correspondant financier ;
- un poste d'agent de paiement ;
- une activité rémunérée sans qualification particulière.

La mission consiste ensuite à recevoir et transférer de l'argent. La personne devient alors une mule financière, parfois sans en avoir conscience.

Exemple : une annonce propose un travail simple et rémunéré à domicile. Votre mission consiste à recevoir des fonds sur votre compte bancaire puis à les transférer vers d'autres comptes, en conservant une commission.

Les signaux d'alerte

- promesse d'argent facile ;
- simple transfert demandé ;
- activité présentée « sans risque ».

Ce qu'il faut retenir

Accepter de faire transiter de l'argent par son compte bancaire peut avoir de graves conséquences, financières et judiciaires.

Réagir en cas de doute ou de fraude

Face à un message suspect, une demande inhabituelle ou une opération que vous ne reconnaissez pas, une réaction rapide et adaptée peut contribuer à limiter les conséquences d'une fraude. Voici les principales vérifications et démarches à effectuer selon la situation rencontrée.

Je vérifie avant d'agir

Les fraudeurs cherchent fréquemment à obtenir une réaction rapide. Avant d'agir, prenez donc quelques instants pour vérifier ce qui vous est réellement demandé et repérer une situation suspecte.

Vérifiez l'origine réelle de la demande

Un courriel, un SMS, un appel téléphonique ou un message peuvent sembler provenir d'un organisme connu, d'un professionnel ou même d'un proche. Toutefois, l'apparence d'un message, l'adresse utilisée ou le numéro affiché lors d'un appel ne permettent pas de garantir l'identité réelle de votre interlocuteur.

Si une demande vous paraît inhabituelle ou inattendue, **prenez le temps de la vérifier**. En cas de doute, interrompez l'échange et contactez vous-même la personne ou l'organisme concerné à partir de coordonnées que vous connaissez déjà.

Vérifiez l'opération que vous êtes sur le point d'autoriser

Avant toute validation dans votre application bancaire ou à l'aide d'un dispositif de sécurité, **lisez attentivement les informations affichées**.

Une validation a pour objectif d'autoriser une opération. Elle ne sert jamais à annuler un paiement, à bloquer une fraude ou à sécuriser un compte.

Si vous ne comprenez pas clairement l'objet de la demande qui apparaît sur votre écran, n'autorisez pas l'opération et prenez le temps d'effectuer les vérifications nécessaires.

Vérifiez les coordonnées du bénéficiaire avant un virement

Les fraudeurs cherchent parfois à modifier les coordonnées bancaires d'un bénéficiaire afin de détourner un paiement vers leur propre compte.

Avant un premier virement ou lorsqu'un changement de coordonnées bancaires vous est communiqué, prenez le temps de **vérifier les informations reçues**. En cas de doute, contactez directement le bénéficiaire à l'aide d'un moyen de contact que vous connaissez déjà.

Pour renforcer cette sécurité, votre banque vérifie la concordance entre le nom du bénéficiaire et l'IBAN du compte destinataire d'un virement Sepa. Cette vérification permet de détecter certaines erreurs de saisie ou incohérences avant la validation du virement.

Si une concordance partielle, une non-concordance ou une impossibilité de vérification est signalée, faites preuve d'une vigilance particulière. Ne corrigez pas le nom au hasard et/ou ne validez pas sous la pression. Contactez directement le bénéficiaire afin de vérifier les coordonnées bancaires communiquées.

ATTENTION Une concordance exacte entre le nom du bénéficiaire et le nom associé à l'IBAN ne garantit pas à elle seule que la demande de paiement est légitime. Assurez-vous également que vous connaissez le bénéficiaire et que vous comprenez parfaitement l'objet du paiement.

La vérification du nom du bénéficiaire constitue une sécurité supplémentaire mais elle ne dispense jamais de vérifier le bien-fondé de la demande de paiement.

J’ai reçu une demande suspecte (appel, message, etc.)

Recevoir un appel, un message via SMS, courriel ou réseau social, inhabituel ne signifie pas nécessairement qu’une fraude est en cours. Toutefois, lorsque le message vous paraît surprenant, urgent ou incohérent, il est préférable de prendre quelques instants pour vérifier la situation avant d’agir.

Les fraudeurs cherchent souvent à obtenir une réaction rapide afin d’empêcher toute réflexion ou vérification. Prendre du recul est souvent le moyen le plus efficace d’éviter une erreur.

Interrompez l’échange en cas de doute

Si un appel, un SMS ou un courriel vous semble suspect, vous n’avez aucune obligation de poursuivre une conversation ou de répondre immédiatement à un message.

Au téléphone, **raccrochez calmement**. Face à un courriel ou à un SMS, **ne cliquez pas sur les liens** et n’ouvrez pas les pièces jointes dont vous doutez.

Mettre fin à l’échange permet de retrouver du recul et d’éviter d’agir sous l’effet de la pression ou de l’émotion.

Vérifiez l’information par un canal connu

Lorsqu’une demande semble provenir d’un organisme, d’un professionnel ou d’un proche, effectuez vous-même les vérifications nécessaires.

Utilisez des coordonnées que vous connaissez déjà ou que vous avez trouvées par vos propres moyens. N’utilisez pas les liens, numéros de téléphone ou adresses indiqués dans le message reçu.

Exemple : si un interlocuteur affirme appeler au nom de votre établissement bancaire, raccrochez et contactez-le vous-même à partir des coordonnées habituelles.

Ne communiquez aucune information sensible

En cas de doute, ne transmettez jamais :
- vos identifiants de connexion ;
- vos mots de passe ;
- votre code confidentiel de carte bancaire ;
- un code reçu par SMS ;
- un code de validation affiché dans votre application bancaire.

Les fraudeurs utilisent régulièrement des prétextes liés à la sécurité pour tenter d'obtenir ces informations. Si une demande de ce type vous est adressée, considérez-la comme un signal d'alerte majeur.

Ne réalisez aucune opération sous la pression

Beaucoup d'escroqueries reposent sur un sentiment d'urgence : fraude prétendument en cours, compte à sécuriser immédiatement, paiement à effectuer sans attendre ou opération à confirmer dans les minutes qui suivent…

Avant de réaliser un paiement, un virement ou une validation, assurez-vous de comprendre parfaitement ce qui vous est demandé et les conséquences de votre action.

Une opération importante mérite toujours quelques instants de réflexion et de vérification.

Conservez les éléments utiles

Même si vous décidez de ne pas répondre à la sollicitation, il peut être utile de conserver certains éléments :
- SMS ou courriels reçus ;
- captures d'écran ;
- numéro utilisé lors de l'appel ;
- adresse mail de l'expéditeur;
- lien suspect reçu ;
- date et heure du contact.

Ces informations peuvent vous être utiles si vous souhaitez effectuer un signalement ou si des événements liés à cette tentative de fraude surviennent par la suite.

J’ai déjà cliqué ou communiqué une information ou validé une opération

Vous craignez que le mal soit fait et vous ne savez pas comment réagir ? Toutes les situations ne présentent pas le même niveau de risque et il est souvent possible d’agir rapidement pour limiter les conséquences.

L’essentiel est d’identifier ce qui s’est passé afin d’adopter les démarches adaptées. Plus vous **réagissez rapidement**, plus il est généralement possible de **réduire les risques**.

J’ai simplement reçu un message

À ce stade, si vous n’avez ni cliqué sur un lien, ni ouvert de pièce jointe, ni communiqué d’information, le risque est généralement limité. **Supprimez le message** et **restez vigilant** face à d’éventuelles sollicitations similaires.

Si le message prétend provenir d’un organisme connu, vérifiez directement auprès de celui-ci en utilisant ses coordonnées habituelles. Si l’origine frauduleuse du message est confirmée, bloquez ce correspondant.

J’ai cliqué sur un lien

Cliquer sur un lien ne signifie pas nécessairement qu’une fraude a été commise.

Si vous avez seulement consulté une page sans saisir d’information ni télécharger de fichier, les risques restent généralement limités. **Fermez la page** et évitez désormais toute interaction avec celle-ci.

En revanche, si vous avez téléchargé un fichier ou installé une application à la suite de ce clic, il est recommandé d'être particulièrement vigilant. Surveillez votre appareil et vos comptes dans les jours qui suivent. Il est recommandé de **lancer votre anti-virus**.

J'ai saisi un identifiant ou un mot de passe

Si vous avez renseigné un identifiant et/ou un mot de passe sur un site dont la fiabilité est douteuse, **modifiez immédiatement le mot de passe** concerné.

Si vous utilisez ce même mot de passe pour d'autres services, modifiez-le également sur ces espaces. L'utilisation de mots de passe différents pour chaque compte contribue à protéger vos autres espaces en ligne.

Pensez également à vérifier les connexions récentes ou les paramètres de sécurité lorsque le service concerné le permet.

J'ai communiqué un code reçu par SMS ou dans mon application mobile

Les codes reçus par SMS ou les demandes de validation dans une application bancaire servent généralement à autoriser une opération ou à renforcer la sécurité d'un accès.

Si vous n'êtes pas à l'origine de l'action concernée, **contactez rapidement votre établissement bancaire** afin d'évaluer la situation et de sécuriser vos accès si nécessaire.

Surveillez attentivement les opérations enregistrées sur vos comptes dans les heures et les jours qui suivent.

J'ai installé une application ou partagé mon écran

Certains fraudeurs demandent à visualiser ou à prendre le contrôle d'un appareil à distance en vous demandant d'installer un logiciel ou une application, présentés comme des outils de sécurité, de vérification ou d'assistance.

Si vous avez installé une application ou partagé l'écran de votre appareil dans un contexte suspect, **mettez fin à l'accès accordé**, désinstallez l'application concernée si nécessaire et sécurisez vos différents comptes.

J’ai validé un paiement (virement par ex.)

L’opération vient juste d’être validée/réalisée ? Une réaction rapide peut permettre d’engager certaines actions de sécurisation ou de vérification :

- **conservez les éléments** dont vous disposez : messages reçus, captures d’écran, références d’opérations ou échanges avec votre interlocuteur
- **contactez** immédiatement **votre établissement bancaire** afin de connaître les démarches envisageables selon la situation. En fonction des circonstances et des délais, elle peut tenter de récupérer les fonds (sauf si les fonds ont déjà été transférés vers un ou plusieurs compte tiers).

Je constate une opération suspecte sur mon compte

D'abord, vérifiez que ce n'est pas juste un oubli : recoupez date, montant et bénéficiaire. Si vous n'êtes vraiment pas à l'origine de cette opération (paiement carte, retrait, chèque, prélèvement ou virement), il est important d'agir rapidement afin de limiter les risques et d'éviter, si possible, de nouvelles opérations frauduleuses.

Faire opposition si nécessaire

Selon la situation, il peut être nécessaire de **faire opposition** à votre carte bancaire ou de **bloquer** les moyens de paiement susceptibles d'être concernés afin d'empêcher de nouvelles utilisations frauduleuses.

C'est indispensable par exemple en cas de perte ou de vol de votre carte ou lorsque vous pensez que ses données ont pu être compromises.

En cas de doute sur la nécessité d'une opposition/blocage, contactez rapidement votre établissement bancaire qui pourra vous orienter vers la solution la plus adaptée.

Contacter rapidement la banque

Votre **établissement bancaire** est votre **interlocuteur privilégié** dès lors qu'une opération paraît suspecte.

Décrivez précisément ce que vous avez constaté : nature de l'opération, montant concerné, date, circonstances éventuelles et actions déjà réalisées. Un signalement rapide facilite l'analyse de la situation et la mise en œuvre des mesures adaptées.

Demander le rappel ou la récupération des fonds lorsque cela est possible

Si un virement a été effectué vers un compte frauduleux, selon la nature de l'opération, les circonstances et les délais écoulés, certaines démarches peuvent parfois être engagées afin de **tenter de récupérer les fonds** ou d'en demander le retour.

Toutefois, cette récupération n'est pas toujours possible, notamment lorsque les sommes ont déjà été transférées vers d'autres comptes. Donc, plus la demande intervient rapidement, plus les possibilités d'action sont importantes.

Surveiller mes comptes et moyens de paiement

Après la découverte d'une opération suspecte, restez particulièrement vigilant dans les jours et les semaines qui suivent.

Consultez régulièrement **vos comptes** afin de détecter d'éventuelles nouvelles opérations inhabituelles. Vérifiez également vos bénéficiaires enregistrés, vos paramètres de sécurité ainsi que les moyens de paiement associés à votre compte.

Certaines fraudes peuvent donner lieu à plusieurs tentatives successives ou à de nouveaux prélèvements après une première opération.

Conserver tous les justificatifs

Tous les éléments liés à la situation vont faciliter vos démarches de contestation et de signalement :

- SMS ou courriels reçus ;
- captures d'écran ;
- références des opérations ;
- échanges avec l'interlocuteur concerné ;
- documents ou justificatifs utiles.

Mémos pratiques

En cas de fraude ou simple doute :

Arrêter → Contacter → Sécuriser → Conserver → Surveiller

1

J'interromps l'échange

Je ne clique sur aucun lien, je ne communique aucune information et je ne réalise aucune opération. Je raccroche ou j'interromps la conversation, même si mon interlocuteur insiste.

2

Je contacte ma banque

J'utilise les coordonnées habituelles de mon établissement bancaire afin de signaler rapidement la situation et connaître les démarches adaptées.

3

Je sécurise mes accès

Selon la situation, je fais opposition à ma carte bancaire, je modifie mes mots de passe, je vérifie les accès à mes comptes, je sécurise mes appareils si je les crois compromis.

4

Je conserve

Je conserve les SMS, courriels, captures d'écran, références d'opérations et tout autre élément susceptible d'être utile pour comprendre les faits ou effectuer un signalement.

5

Je surveille

Dans les jours et semaines suivants, je consulte régulièrement mes comptes, je vérifie les opérations enregistrées et je signale rapidement toute anomalie.

Tableau des situations fréquentes

Réagissez rapidement pour limiter les conséquences d'une fraude.

Conservez systématiquement les éléments utiles afin de faciliter vos démarches.

SITUATION	RÉACTION IMMÉDIATE
Vous constatez un paiement par carte bancaire que vous ne reconnaissez pas.	Signalez rapidement l'opération à votre établissement bancaire et faites opposition à votre carte si vous pensez que ses données ont été compromises.
Vous avez perdu votre carte bancaire ou elle a été volée.	Faites immédiatement opposition à votre carte bancaire et vérifiez les dernières opérations enregistrées. En cas de vol, portez plainte.
Les données de votre carte bancaire semblent avoir été utilisées à votre insu.	Faites opposition à votre carte, surveillez vos opérations récentes et signalez les paiements frauduleux.
Vous découvrez un prélèvement que vous n'avez pas autorisé.	Contestez rapidement le prélèvement, demandez le blocage des prélèvements futurs si nécessaire et conservez les références de l'opération.
Vous constatez une connexion ou une opération réalisée depuis votre espace bancaire sans votre intervention.	Contactez votre banque et modifiez immédiatement vos identifiants et mots de passe, vérifiez les bénéficiaires enregistrés et contrôlez l'ensemble des opérations récentes.

SITUATION	RÉACTION IMMÉDIATE
Vous avez communiqué des informations sensibles à la suite d'un courriel, courrier, SMS ou un appel frauduleux.	Changez immédiatement les accès concernés et surveillez vos comptes afin de détecter toute anomalie.
Vous avez communiqué un code reçu par SMS ou validé une demande dans votre application bancaire.	Réagissez sans attendre : contactez votre banque, vérifiez les opérations récentes et expliquez précisément les circonstances de la situation.
Vous avez effectué un virement après avoir été trompé par un fraudeur.	Demandez immédiatement à votre banque si une procédure de retour des fonds (« recall ») peut être engagée et conservez tous les échanges liés à la fraude.
Vous avez été victime d'une fraude au RIB et viré des fonds sur un compte frauduleux.	Conservez l'ensemble des documents relatifs au changement de coordonnées bancaires et signalez immédiatement la fraude à votre banque et portez plainte.
Vous avez remis un chèque qui s'est révélé faux, falsifié ou frauduleux.	Conservez le chèque ou sa copie, ainsi que les échanges et paiements avec son émetteur.
Vous avez reçu un faux chèque et reversé tout ou partie des fonds à un tiers.	Interrompez tout nouveau transfert d'argent et rassemblez l'ensemble des justificatifs relatifs à l'opération.
Un chèque que vous avez émis a été falsifié puis encaissé.	Signalez rapidement la falsification à votre banque et conservez les documents relatifs au chèque concerné.
Vous êtes en désaccord avec un professionnel après un achat ou une prestation.	Contactez d'abord le professionnel concerné. Il ne s'agit pas a priori d'une fraude bancaire mais d'un litige commercial.

Cette présentation est donnée à titre indicatif. Chaque situation doit être examinée individuellement.

Connaître ses droits et les démarches

Après une fraude ou une tentative de fraude, pouvez-vous être remboursé, quelles démarches entreprendre ou à qui signaler les faits ?

Voici les principales règles à connaître, les démarches qui peuvent être engagées et les interlocuteurs susceptibles de vous accompagner.

Puis-je être remboursé en cas de fraude ?

Être victime d'une fraude ne signifie pas être automatiquement remboursé. En effet, les possibilités de remboursement dépendent de nombreux éléments. Chaque situation est examinée individuellement.

Quels éléments fournir à ma banque ?

Le remboursement d'une fraude dépend toujours des circonstances dans lesquelles l'opération a été réalisée. Plus vous serez complet, plus vous faciliterez l'examen de votre situation. N'ayez surtout pas honte : tout le monde peut se faire avoir, même un professionnel ou expert.

- **Signalez** rapidement les faits.
- **Expliquez** précisément ce qui s'est passé, les circonstances de la fraude.
- **Indiquez** les informations éventuellement communiquées, les validations réalisées, les moyens de sécurité utilisés.
- **Précisez** les démarches effectuées après la découverte de la fraude.
- **Conservez** les preuves disponibles.
- **Transmettez** toutes les informations demandées par votre établissement bancaire.

Quels sont les délais à respecter ?

Les délais réglementaires de contestation peuvent être relativement longs (par ex. jusqu'à treize mois après le débit) mais il s'agit de dates butoirs. Dès que vous constatez une opération de paiement que vous n'avez pas autorisée, vous devez la signaler sans tarder à votre établissement bancaire. À défaut, vous pourriez perdre un éventuel droit au remboursement.

Des règles particulières peuvent d'ailleurs s'appliquer par exemple pour les prélèvements, selon que vous contestez le mandat lui-même ou les conditions du paiement.

Dans tous les cas, une réaction rapide facilite les vérifications et peut permettre de limiter les conséquences de la fraude.

Comment mon établissement bancaire analyse-t-il une contestation ?

Chaque banque analyse la situation au cas par cas pour décider et effectuer un remboursement (ou pas) dans un délai d'un jour ouvrable (J+1).

- Elle effectue une 1ère analyse de l'opération pour déterminer si celle-ci est **éligible à un remboursement**. S'il y a remboursement, la banque rétablit votre compte dans l'état où il serait si l'opération n'avait pas eu lieu.
- Elle peut être amenée à **approfondir ses recherches** : une reprise des fonds remboursés, est donc possible dans les 30 jours suivant (sauf situation exceptionnelle), en fonction du résultat de ses recherches.

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.

Pourquoi la distinction entre opération autorisée et non autorisée est-elle importante ?

Lorsqu'une opération est contestée, la banque va vérifier si vous avez **donné ou non votre consentement** à cette opération. Ce critère est essentiel dans le cadre de votre contestation et d'un éventuel remboursement.

- Une opération est généralement considérée comme autorisée lorsque vous avez donné votre accord pour qu'elle soit exécutée.
- À l'inverse, une opération est considérée comme non autorisée lorsque vous ne l'avez ni réalisée, ni validée.

En cas de doute sur le caractère autorisé, elle procède au remboursement de la transaction et au plus tard à J+1, sauf démonstration d'une négligence grave de votre part ou d'une faute intentionnelle.

Quel rôle joue l'authentification forte ?

De nombreuses opérations nécessitent aujourd'hui une **authentification** à l'aide d'un code reçu sur votre téléphone, d'une validation dans votre application bancaire ou d'un autre dispositif de sécurité.

Lorsqu'une authentification forte a été utilisée, elle constitue un élément d'analyse important dans le sens où elle tend à s'assurer que c'est bien vous qui a avez consenti à l'opération.

Toutefois, la présence d'une authentification forte ne permet pas, à elle seule, de conclure automatiquement que l'opération a nécessairement été autorisée ou qu'un remboursement est exclu.

Les circonstances dans lesquelles cette authentification a été obtenue ou utilisée sont également prises en compte. Chaque situation est examinée dans son contexte.

Que faire en cas de refus de remboursement ?

Si votre établissement bancaire estime qu'un remboursement ne peut pas être accordé, il vous indiquera les motifs de sa décision, par exemple soupçon de fraude du client lui-même.

Prenez le temps de lire attentivement ces explications et, si certains éléments vous paraissent incomplets ou difficiles à comprendre, demandez des précisions.

Conservez l'ensemble des documents relatifs à votre dossier de contestation : échanges, courriers, justificatifs et éléments transmis.

Si un désaccord persiste, vous pouvez effectuer une réclamation auprès de votre établissement bancaire afin que votre situation fasse l'objet d'un nouvel examen via le service dédié aux réclamations voire saisir ensuite le médiateur en cas de réponse défavorable/négative de votre banque.

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

Faut-il déposer plainte ?

Le **dépôt de plainte n'est pas obligatoire** pour entamer les démarches auprès de la banque et demander un remboursement lorsque vous avez été victime d'une escroquerie.

Cependant, il **peut être très utile** afin de signaler officiellement les faits, conserver une trace des événements et aider les autorités à identifier et interpeller les escrocs.

Pour faciliter vos démarches, conservez et transmettez tous les éléments utiles :

- SMS ou courriels reçus ;
- captures d'écran ;
- relevés d'opérations ;
- coordonnées utilisées par le fraudeur ;
- échanges intervenus avant la fraude, etc.

Vous pouvez déposer plainte auprès d'un commissariat de police ou d'une brigade de gendarmerie. Il est possible de vous rendre dans le service de votre choix, quel que soit le lieu où la fraude a été commise.

Certaines démarches peuvent également être réalisées en ligne ou débutées sur Internet. Selon la situation, vous pourrez être orienté vers un dispositif de signalement spécialisé, une plateforme de plainte en ligne ou vers les services de police ou de gendarmerie compétents.

Le dépôt de plainte ne remplace pas le signalement à votre établissement bancaire. Contactez votre banque en priorité afin de sécuriser vos moyens de paiement et engager les démarches nécessaires.

Pourquoi utiliser les plateformes de signalement ?

Plusieurs **plateformes publiques** permettent de **signaler des fraudes**, de transmettre des informations aux autorités compétentes ou d'identifier les démarches à effectuer après une tentative de fraude ou une escroquerie avérée.

Selon la nature de la fraude, plusieurs dispositifs publics peuvent être utilisés :

- **Perceval**, pour signaler l'utilisation frauduleuse des données de votre carte bancaire lors d'achats réalisés sans votre accord et si vous êtes toujours en possession de votre carte.
- **THÉSÉE**, pour certaines escroqueries commises sur Internet.
- **PHAROS**, pour signaler des contenus ou comportements illicites observés en ligne.
- **Cybermalveillance.gouv.fr,** pour obtenir des informations pratiques, des ressources pédagogiques et une assistance en cas d'incident numérique.
- **33700**, pour signaler un SMS ou un appel frauduleux.
- **Signal Spam**, pour signaler un courriel indésirable ou frauduleux.

Ces signalements permettent aux autorités et organismes concernés d'identifier les campagnes d'escroquerie en cours, de repérer les modes opératoires utilisés par les fraudeurs et de renforcer les actions de prévention.

Lorsqu'une opération de paiement est concernée, votre 1er réflexe doit rester de contacter votre établissement bancaire. Les plateformes de signalement constituent un complément utile pour signaler les faits et contribuer à la lutte contre les fraudes.

Conclusion

Plus que jamais, avec l'essor de l'IA et les fuites de données massives, personne n'est à l'abri d'une tentative d'escroquerie. Connaître les principales fraudes, savoir repérer les signaux d'alerte et réagir rapidement en cas de doute permet de mieux protéger vos comptes et vos moyens de paiement.

Face à une situation inhabituelle, prenez votre temps et contactez votre banque.

Pour aller plus loin

Pour les autres formes d'escroquerie (chantage en ligne, piratage de compte, rançongiciel, fraude sur les réseaux sociaux, etc.), consultez les ressources et recommandations proposées par cybermalveillance.gouv.fr.

Annexe – Tableau récapitulatif

Les principales fraudes : comment les identifier et réagir

SIGNAL D'ALERTE PRINCIPAL	MOYEN(S) CONCERNÉ(S)
Demande urgente de validation ou de code de sécurité	Téléphone, application bancaire, virement
Lien reçu dans un message inattendu	Courriel, SMS, espace bancaire
Message alarmant invitant à agir rapidement	SMS
QR code inattendu ou non sollicité	QR code
Demande de remettre sa carte bancaire à un tiers	Carte bancaire
Invitation à appeler un numéro pour faire opposition	SMS, courriel, téléphone

FRAUDE	RÉACTION IMMÉDIATE
Faux conseiller bancaire	Raccrocher et contacter soi-même son établissement bancaire
Phishing / Smishing	Ne pas cliquer et vérifier l'origine de la demande
Smishing	Ne pas répondre et ne communiquer aucune information
Quishing	Ne pas scanner et vérifier l'origine du document
Faux coursier	Refuser et conserver sa carte
Faux numéro d'opposition bancaire	Ne pas appeler ce numéro et contacter directement son établissement bancaire

SIGNAL D'ALERTE PRINCIPAL	MOYEN(S) CONCERNÉ(S)
Changement inattendu de coordonnées bancaires	Virement
Proposition de rendement élevé avec peu ou pas de risque	Virement
Demandes répétées d'argent dans le cadre d'une relation en ligne	Virement
Proposition d'argent facile ou de commission contre un simple transfert	Compte bancaire, virement
Demande d'argent urgente provenant d'un proche	Virement, paiement mobile
Réception inattendue d'un code de validation ou d'une demande d'ajout de carte	Paiement mobile, application bancaire
Vous reconnaissez une voix ou une image mais la demande paraît inhabituelle	Téléphone, messagerie, vidéo, visio

FRAUDE	RÉACTION IMMÉDIATE
Fraude au RIB	Vérifier auprès du bénéficiaire par un canal déjà connu
Faux placement financier	Vérifier l'identité de l'intermédiaire, les agréments et les listes noires avant tout versement
Fraude sentimentale	Suspendre tout paiement et prendre du recul
Mule financière	Refuser immédiatement
Usurpation d'identité d'un proche	Vérifier la demande par un autre moyen de contact
Détournement du paiement mobile	Ne pas valider et vérifier l'origine de la demande
Deepfake vocal ou vidéo	Vérifier la demande par un autre canal avant toute action

lesclesdelabanque.com

FÉDÉRATION
BANCAIRE
FRANÇAISE

